EN

THIS ACTION IS FUNDED BY THE EUROPEAN UNION

ANNEX IV

of the Commission Implementing Decision on the 2021 annual action plan for the global threats part of the thematic programme on peace, stability and conflict prevention

Action Document for Critical Infrastructure Protection (CIP)

ANNUAL PLAN
This document constitutes the annual work programme in the sense of Article 110(2) of the Financial Regulation, and action plans in the sense of Article 23 of Regulation (EU) 2021/947 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe.

1. SYNOPSIS

1.1. Action Summary Table

1. Title **CRIS/OPSYS business reference** **Basic Act**	**Critical Infrastructure Protection (CIP)** OPSYS/CRIS[1] number: NDICI THREATS FPI/2021/43399 Financed under the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe) Regulation			
2. Team Europe Initiative	No			
3. Zone benefiting from the action	The action shall be carried out worldwide.			
4. Programming document	Peace, Stability and Conflict Prevention Thematic Programme 2021 – 2027			
5. Link with relevant MIP(s) objectives/expected results	Priority 7 - Addressing trans-regional and global threats to critical infrastructure Specific objective 1: Increased capacity to address trans-regional and global threats to cybersecurity Specific objective 3: Increased capacity to address global challenges related to maritime security			
PRIORITY AREAS AND SECTOR INFORMATION				
6. Priority Area(s), sectors	Global, trans-regional and emerging threats 152 - Conflict, Peace & Security			
7. Sustainable Development Goals (SDGs)	Main SDG: 16 (Promote Peace and end violence) Other significant SDGs and where appropriate, targets: 5 (Achieve gender equality and empower all women and girls), 9 (Industry, Innovation and Infrastructure)			
8 a) DAC code(s)	15130 – Legal and judicial development 15210 – Security system management and reform			
8 b) Main Delivery Channel	Public Sector Institutions – 10000 Council of Europe – 47138			
9. Targets	☐ Migration ☐ Climate ☐ Social inclusion and Human Development ☐ Gender ☐ Biodiversity ☐ Education ☒ Human Rights, Democracy and Governance			
10. Markers (from DAC form)	**General policy objective**	**Not targeted**	**Significant objective**	**Principal objective**
	Participation development/good governance	☐	☐	☒
	Aid to environment	☒	☐	☐

[1] Depending on the availability of OPSYS at the time of encoding, a provisional CRIS number may need to be provided.

	Gender equality and women's and girl's empowerment	☐	☒	☐
	Trade development	☐	☒	☐
	Reproductive, maternal, new-born and child health	☒	☐	☐
	Disaster Risk Reduction	☐	☒	☐
	Inclusion of persons with disabilities	☒	☐	☐
	Nutrition	☒	☐	☐
	RIO Convention markers	**Not targeted**	**Significant objective**	**Principal objective**
	Biological diversity	☒	☐	☐
	Combat desertification	☒	☐	☐
	Climate change mitigation	☒	☐	☐
	Climate change adaptation	☒	☐	☐
11. Internal markers and Tags:	**Policy objectives**	**Not targeted**	**Significant objective**	**Principal objective**
	Digitalisation Tags: digital connectivity digital governance digital entrepreneurship job creation digital skills/literacy digital services	☐	☐ ☐ ☐ ☐ ☐ ☐ ☐	☒ ☐ ☒ ☐ ☐ ☐ ☐
	Connectivity Tags: transport people2people energy digital connectivity	☐	☒ ☒ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
	Migration (methodology for tagging under development)	☒	☐	☐
	Reduction of Inequalities (methodology for marker and tagging under development)	☒	☐	☐
	Covid-19	☒	☐	☐
BUDGET INFORMATION				
12. Amounts concerned	Budget line(s) (article, item): BGUE-B2021-14.020230 – STABILITY AND PEACE - GLOBAL AND TRANSREGIONAL THREATS Total estimated cost: EUR 9 555 556 Total amount of EU budget contribution: EUR 9 000 000			
MANAGEMENT AND IMPLEMENTATION				
13. Type of financing	**Indirect management** with the Council of Europe and Expertise France			

1.2. Summary of the Action

The protection of critical infrastructure from a broad range of security and safety related threats is essential to safeguarding core societal and economic activities in various sectors, including transport, energy and health, and to facilitating global trade and cooperation, as also stressed in the 2020 EU Cybersecurity Strategy for Digital Decade or the EU Maritime Security Strategy and its revised Action Plan, among others. In a globalised world, major disruptions resulting from intentional or unintentional harm or damage caused to this infrastructure can have significant repercussions, including for the EU.

The **overall objective** of the action to strengthen the protection of critical infrastructure, namely related to **cyber and maritime security**.

Component 1 "Global Action Against Cybercrime Extended" (GLACY+) intends to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area, while ensuring compliance with international human rights standards and the rule of law. Building on the experience of the ongoing joint EU-Council of Europe project, this component of the action aims to further consolidate the results of GLACY+ and expand its coverage. To this end, an additional focus will be put on connecting the fight against cybercrime with cybersecurity; ensuring that policy-makers understand the need for international cooperation in fighting cybercrime and the benefits of the Budapest Convention on

Cybercrime; applying the forthcoming Second Additional Protocol to the Budapest Convention on Enhanced Co-operation and Disclosure of Electronic Evidence; and on addressing related challenges posed by COVID-19 and other emerging issues.

Component 2: "Critical Maritime Routes Indo-Pacific" (CRIMARIO II) intends to support partner countries in the Indian Ocean and Southeast Asia to adequately address maritime security and safety challenges in a comprehensive manner, through cross-sectorial, inter-agency and cross-regional approaches, with the view to secure the lines of communication at sea. The two Specific Objectives of this component focus on enhancing information exchange and analysis to support incident coordination and crisis management, notably through the promotion of the IORIS maritime coordination platform; and on strengthening inter-agency cooperation in maritime surveillance, policing, investigation and judicial matters. This component will focus on providing satellite services and other actionable data to CRIMARIO's main partners, especially regional information fusion and information sharing centres, in order to enhance their operational capacity in mitigating common maritime safety and security risks in their regions. Provision of much needed satellite products will also enhance the attractiveness of IORIS, thus contributing to develop a single information sharing environment in the Indo-Pacific.

All components will be implemented in full complementarity with bilateral and regional programmes and in coordination with EU Delegations as well as relevant geographical units in INTPA and NEAR.

2. RATIONALE

2.1. Context

Component 1: 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 4 billion by the start of 2018, 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 increasing reliance on information and communication technologies (ICT) in all spheres of life has strengthened further during the Covid-19 pandemic, and a growing number of connections between people, processes and data has already started the transformation of our societies. Governance structures and systems need to keep abreast of these rapid changes. However, the risks and challenges associated with efforts to improve access to ICT and the growing Internet penetration have been underestimated. The last decade in particular has seen a rapid growth in threats to cyberspace. Every day, cyber security incidents cause major economic damage to the global economy and security.

Around 75% of cyberattacks are caused by criminals who seek to exploit security weaknesses of the digital infrastructure and the ICT. The lack of consistent legal instruments in some countries offers safe havens for cyber criminals, enables them to store their resources as well as protects them from any international law enforcement / judicial attempts at prosecution. Moreover, the fact that any crime may entail electronic evidence held on an electronic device has serious implications for criminal justice systems. Therefore, these systems and law enforcement agencies need to be enabled to deal with electronic evidence.

Progress has been made in recent years and the Convention on Cybercrime ("Budapest Convention") has played a major role in this respect. Many countries have begun to reform their legislation, tools and practices by creating high-tech crime units, training law enforcement and judicial officials, fostering partnerships between public and private sectors and enhancing international cooperation.

A new, 2nd Additional Protocol to the Budapest Convention on enhanced cooperation and disclosure of electronic evidence is in preparation. It was approved by the Cybercrime Convention Committee (T-CY) in May 2021 and is expected to be opened for signature in spring 2022.

More needs to be done however as regards connecting cybersecurity and the fight against cybercrime; ensuring that policy makers understand the needs for international cooperation in fighting the cybercrime and the benefits of the Budapest Convention; applying the forthcoming Second Additional Protocol to the Budapest Convention; challenges posed by COVID-19 and other emerging issues.

The proposed action contributes to building resilience, enhancing rule of law and supporting the fight against organised crime.

Component 2: Critical Maritime Routes are the routes considered crucial to maritime trade, transport, fishing and other essential maritime activities. As maritime transport represents by far the largest proportion by volume of world trade and around 90% of Europe's global trade is transported by sea, the Indian Ocean, the Gulf of Guinea and the South East Asia are of strategic importance to Europe.

Component 2 concentrates on securing critical maritime routes in the Western Indian Ocean, South Asia and Southeast Asia. A number of maritime threats, such as kidnap for ransom, maritime terrorism, and illicit trafficking plague these regions. Illegal, unreported and unregulated (IUU) fishing is also a challenge.

The complex threat landscape (including in relation to the South China Sea dispute) has led to rising levels of national maritime security spending amongst countries in the region in recent years. Nevertheless, the capabilities of Asian countries remain insufficient. This growth in spending requires complementary efforts in the professionalisation of maritime law enforcement at the national level, as well as to address the numerous maritime security and safety threats that countries in the regions continue to face.

Maritime domain awareness capabilities are receiving investments but remain insufficient in most parts of the wider Indian Ocean. Surveillance and control have been falling behind the growing challenges linked to increased threats. Strengthening these capabilities by using IT technologies and by promoting a cross-sectorial, inter-agency and cross-regional approach would assist coastal nations in their efforts to build maritime domain awareness and a coordinated capacity to respond to security and safety incidents at sea.

In this regard, the CRIMARIO II was launched in 2020 expanding its geographical scope from the Western Indian Ocean to cover also South and Southeast Asia, and increasing its focus from maritime information exchange and coordination also to law enforcement cooperation. This top-up of CRIMARIO II will add a focus on providing satellite and other services to its main partners, especially information fusion and information sharing centres, in order to enhance their operational capacity in mitigating common maritime safety and security risks in their regions and thus enhancing maritime security and safety.

2.2. Problem Analysis

Short problem analysis:

Component 1: The main challenge to be addressed is the insufficient state capacity to apply legislation on cybercrime and electronic evidence in practice. An increased capacity of third countries to address cybercrime is therefore a significant factor in enhancing cooperation frameworks also with the EU, for example in receiving electronic evidence in real time from other jurisdictions or cyber incident reports that can result in the EU's strengthened resilience to cyber threats. Misuse of emerging technologies to commit cybercrimes is an undeniable reality. Criminal justice authorities need to be prepared to react to these threats expeditiously. While new technologies can serve to enhance efficient cybercrime investigations, criminal justice authorities need to be ready to understand and manage the ethical, legal and human rights aspects of these technologies. Therefore, knowledge about the use of new technologies should be increased.

Since reportedly around 75% of cyberattacks are carried out by criminals, collaboration between cybersecurity actors and criminal justice practitioners needs to be strengthened. In many countries, there is also often a disconnect between criminal justice authorities and practitioners who understand the benefits of the Budapest Convention in terms of strengthening of the rule of law, and the policy/political level which may be receptive to alternative narratives; therefore a dialogue should be strengthened between criminal justice practitioners and policy makers. The Second Additional Protocol aims to further enhance cooperation on cybercrime and the ability of the criminal justice authorities to obtain electronic evidence of a criminal offence for the purpose of specific criminal investigations or proceedings. More awareness raising on the procedures and tools made available by the Protocol and capacity building on the application and effective implementation of the Protocol is therefore needed in this regard. COVID-19 has also brought a number of challenges connected with conducting investigations, handling electronic evidence, and conducting trials from remote/online.

Component 2: There is a clear gap in some countries of the region: capacity within maritime administrations, law enforcement and coast guards in the Indian Ocean and Southeast Asia to address maritime security challenges remains insufficient in some cases. The regions are faced with a rising threat landscape characterised by complex and intertwined maritime security and safety challenges. Mitigating the threats requires especially improved capabilities in maritime domain awareness and inter-agency cooperation and functioning maritime law enforcement.

In this regard, CRIMARIO has developed IORIS, a tailor-made web-based platform to:

- coordinate maritime operations including real-time management of incidents at sea; and

- offer secure communications between users allowing each to control access rights for their respective designated areas;
- to be used at national (inter-agency) as well as regional (international) level.

The platform has been operational since 2018 and is currently used by a growing number of national and regional maritime actors and agencies in the Western Indian Ocean, Horn of Africa and the Red Sea, including the Regional Maritime Information Fusion Centre (RMIFC) in Madagascar and the Regional Center for Operations Coordination (RCOC) in Seychelles, as well as Operation EUNAVFOR Atalanta.

It is in this context that maritime coordination and information-sharing initiatives are the cornerstones upon which law enforcement capacity building, exercises and other forms of cooperation shall be hinged. CRIMARIO II therefore focuses on promoting the development of single information-sharing environment, through concept development and technologies. Key in all this is support to existing information fusion and information sharing centres, and linking them and promoting interoperability to facilitate exchange of information and coordination of operations.

The proposed reinforcement of CRIMARIO focuses on supporting maritime operation centers by providing actionable information.

Whenever a calamity occurs at sea, be it offshore such as an airliner crashing mid-ocean; or coastal, such as a tanker breaking up on a sensitive coral reef, or a tsunami wiping out coastal communities, operational planners involved in tasking first responders need to have immediate access to actionable information, which should be as close as possible to real-time. Moreover, operational planners should also be able to monitor, control and survey the maritime domain to ensure that actors are conforming to international laws and obligations, in order to prevent accidents, deter illicit activities and react promptly whenever necessary. When incidents occur, operational planners should have the tools at their disposition, to be able to coordinate interagency responses, sometimes immediately.

The EU has developed technologies which offer satellite imagery and derived services which support in addressing threats to maritime safety and security. However, the Copernicus Maritime Service operated by the European Maritime Safety Agency is not available for third countries as end-users. In this respect, CRIMARIO would seek to obtain these critical technologies from commercial sources and provide them to its main partners (especially regional information fusion and information sharing centers) through IORIS. This would enable the partners facing calamities, distress and enforcement situations to react in an expedited manner. The focus would be especially on purchasing satellite services capable of identifying “dark targets” (vessels which deliberately switch off their responders to be invisible to operation centers), as well as access to databases about vessels and cargo and other data products.

Such an initiative would strengthen operational capacities of the EU’s partners, regional maritime security as well as the EU’s ability to influence outcomes. It would also strengthen the attractiveness of IORIS as an incident management tool and would thus support the expansion of its use across the regions, contributing significantly to the development of the single information-sharing environment and to the return on the EU’s investment in the platform.

EU Fundamental Values

Component 1: GLACY+ is global and targets several regions and countries worldwide. All its activities and operations will contribute to, and be accounted for under, the general objectives of the von der Leyen Commission: "A stronger Europe in the world" and “Promoting our European way of life”. The action is based on the recognition of the growing inter-connection between internal and external security (EU’s Security Union Strategy 2020-2025).

By supporting the adherence of countries to the Budapest Convention on Cybercrime and its effective implementation, this component of the action enhances Rule of Law and criminal justice in the countries, and promotes international cooperation in fighting cybercrime, in compliance with international human rights standards.

Moreover, in light of the increasing global polarisation on issues like Internet freedom and cyber governance, with authoritarian countries advocating cyber sovereignty, raising trade barriers and suggesting new treaties that allow content control, a coordinated approach combining EU policy and operational toolbox is necessary. Capacity building of third countries in the area of cybercrime can play a key role in building stronger, open, free and secure cyberspace in full respect of the human rights and based on rule of law principles.

Component 2: CRIMARIO II targets three regions with about 25 coastal and island countries. All its activities and operations will contribute to, and be accounted for under, the general objectives of the von der Leyen Commission: "A stronger Europe in the world" and “Promoting our European way of life”.

The selection of partner countries and organisations takes into account their respect of the fundamental values of democracy, Human Rights and the Rule of Law.

Key cross-cutting issues

Human rights, rule of law, management/leadership, justice, law enforcement, capacity building.

Relevance and credibility of Partner Country's/Regional Policies and Strategies

Component 1: The overall political commitment of the partner countries is proved by the governments having committed to join the Budapest Convention and/or having adopted domestic legislation in line with this treaty. These countries are then also represented in the Cybercrime Convention Committee (T-CY) of the Council of Europe as members or observers, and thus subject to peer reviews. The continued involvement in this mechanism fosters their commitment and sustainability.

Component 2: CRIMARIO II targets three regions with about 25 coastal and island countries and a number of relevant international and regional organisations. The component partners with, and provides support to those countries and organisations which aim to enhance maritime security and safety in a coordinated and collaborative manner.

The IMO-promoted Djibouti Code of Conduct (DCoC), adopted in 2009 by 21 countries with an interest in the Western Indian Ocean and originally focusing on counter-piracy, now through the Jeddah Amendment (DCoC(J)) includes also other illicit maritime activities such as illicit trafficking and illegal, unreported and unregulated fishing. The IMO supports CRIMARIO in assisting the DCoC through the use of IORIS.

The Indian Ocean Commission (IOC) has been actively enhancing its capacities and building up maritime security architecture in the region through the RMIFC and RCOC regional maritime centers, benefitting from the EU support via the MASE Programme.

The Foreign Ministers of the ASEAN Regional Forum (ARF) agreed, through the 2010 Hanoi Plan of Action, to implement the ARF Vision Statement. Priority areas include: promoting compliance and adherence to relevant international legal instruments and regional arrangements; forging closer cooperation to enhance the safety and security of navigation (implementation of standards, best practices, data-sharing for small vessel registration on a national and (potentially) regional basis); promoting regional maritime security capacity-building through concrete activities (information sharing, exchanges of officials, table top exercises, joint training activities); and promoting cooperation (maritime security and safety, search and rescue, technological cooperation, combating maritime terrorism and national crimes like piracy, armed robbery against ships, hijacking, smuggling, trafficking in persons). The 2016 ARF ministerial conference determined that the EU and ASEAN have shared interests in maritime security, and that the EU as ARF Inter-Sessional Meeting co-chair would have until mid-2021 to help guide ASEAN's maritime security agenda.

EU added value

Component 1: The EU Member States were at the origin of the Budapest Convention. The EU has been therefore actively supporting accession to the Budapest Convention and its effective application, most notably through its partnership with the Council of Europe. Through the Convention's focus on Rule of Law and international cooperation in compliance with international human rights standards, the Convention enshrines the EU's fundamental values and the Union is thus well place to protect them.

The EU policy framework in the domain of cybersecurity / cybercrime capacity-building and cooperation is anchored in 2016 EU Global Strategy, the 2017 new European Consensus on Development, the 2020 EU Security Union Strategy and the 2020 EU Cybersecurity Strategy for Digital Decade. Specifically, it revolves around principles of security-development nexus (security as both a necessary and sufficient condition for development) and internal-external nexus (coherence between internal and external policy).

In May 2021, the Council adopted conclusions setting the 2022-2025 EU priorities for the fight against serious and organised crime through the European multi-disciplinary platform against criminal threats (EMPACT). On the basis of the 2021 EU serious and organised crime threat assessment, presented by Europol, Member States have identified 10 crime priorities, including cyber-attacks orchestrated by criminal offenders, and online child abuse.

Component 2: In line with the EU Global Strategy and the EU Maritime Security Strategy (EU MSS), the EU aims to act as a global maritime security provider.

Among its objectives, the EUMSS pursues its actions to ensure freedom, safety and security of navigation, and to ensure coherence between the activities of various organisations, notably in the fisheries, environment and transport fields. One of the main features of the revised Action Plan is the emphasis on the regional approach, which is considered fundamental to tailoring responses to security challenges in European sea basins and other key maritime

hotspots, such as the Eastern Indian Ocean. The regional focus is viewed as much more dynamic and productive, capable of promoting a more concerted effort among all interested countries, regardless of their level of development.

Moreover, the EU Global Strategy notes that in the Eastern Indian Ocean, the EU will help build maritime capacities and support an ASEAN-led regional security architecture. The EU-ASEAN High Level Dialogue aims to gather ideas and inputs on how and where ASEAN and the EU can cooperate on maritime security. Specifically, the Dialogue explores pathways for bilateral cooperation between EU and ASEAN Member States to improve maritime surveillance, information sharing, law enforcement at sea, and the development of efficient, secure and environmentally friendly ports.[2]

The EU's added value also consists in the fact that the EU is mostly seen as rather a neutral actor in these regions and thus is a credible, reliable partner to support strengthening maritime security, especially in Southeast Asia where there are maritime disputes between countries.

Complementarity with EU and other Donors/Partners

Component 1: There are strong complementarities and synergies with other EU-funded actions, particularly in the Western Balkans and Neighbourhood (namely CyberEast and CyberSouth under the remit of the DG NEAR) which are implemented by the Council of Europe and therefore operational coordination is ensured by the Council of Europe's Cybercrime Programme Office.

Considering the synergies between cybercrime and cybersecurity, attention is placed to ensure coordination with FPI.1's actions Cyber Resilience for Development (Cyber4D) and EU CyberNet.

At the EU level, the inter-service group on cyber issues allows for a framework of internal coordination. More generally, coordination with the EU Member States is ensured in the Horizontal Working Party on Cyber Issues.

Within the European Union, much experience has been gained during the past decade in particular with respect to the development of standardised and scalable training, cooperation and information sharing between specialised cybercrime units and other fields. Cooperation with the European Cybercrime Centre at Europol (EC3), including the European Cybercrime Training and Education Group (ECTEG) and the EU Cybercrime Task Force, as well as with relevant EU Member State agencies, will allow to share this experience with third countries.

This component of the action will also seek to find synergies and support other actions whereby a joint effort can maximise both parties delivery at lower costs. Coordination will be sought with international organisations and agencies on the ground.

Component 2: CRIMARIO has established itself as a well-known actor in the maritime security community in the Western Indian Ocean and is progressively more known in South and Southeast Asia. It continues to build a high level of credibility with the expertise provided to key actors and has succeeded to develop synergies and a permanent flow of information with other EU initiatives covering the Indian Ocean such as MASE (in January 2021, a joint Action plan was elaborated by Indian Ocean Commission/MASE and CRIMARIO), MSCHOA (Maritime Security Centre – Horn of Africa), CRIMSON (in communications and evaluation).

Potential for collaboration in the field of maritime domain awareness with the EDF-funded Red Sea Programme is currently being analysed.

In Asia, a close cooperation has been established with the "Enhancing Security Cooperation in and with Asia" project.

Strong links have been established with other partners, including the US, Japan, India and Singapore.

Identification of main stakeholders and corresponding institutional and/or organisational issues (mandates, potential roles, and capacities) to be covered by the action:

Component 1: The key stakeholders are third country governments including policy makers, legislators, competent ministries (ICT, Security, Justice, etc) and relevant national authorities (police/high-tech crime units/financial crime units, lawyer associations, cybersecurity public agencies and Computer Emergency Response Teams), the private sector (particularly internet/telecom service providers, financial sector), civil society (especially those dealing with digital rights), and end-users.

[2] The Bandari Seri Begawan Plan of Action responds to the decision of Foreign Ministers made at the 18th ASEAN-EU Ministerial Meeting in Madrid, on 26 May 2010. It aimed to bring cooperation to a higher level, by addressing regional and global challenges of shared concern over the coming five years (2013-2017). It covered a wide range of areas – political/security, economic/trade, sociocultural – reflecting the multifaceted character of ASEAN-EU relations. Articles 1.2.2, 1.2.8, 1.2.9, and 1.2.10 of the Plan of Action specifically referred to maritime security issues.

At EU level, relevant stakeholders include the European Cybercrime Centre at Europol (EC3), the European Union Agency for Network and Information Security (ENISA), EU Delegations, EU Member States' embassies and Cybersecurity Agencies, as well as EU experts, who will provide expertise and good practice.

Component 2: The key stakeholders are:

- Maritime Law Enforcement authorities/agencies of coastal and island states in the Indian Ocean and Southeast Asia
- International and regional organisations such as Indian Ocean Commission, International Maritime Organisation/Djibouti Code of Conduct, ASEAN, Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP)
- Information fusion and information sharing centers such as Regional Maritime Information Fusion Centre (RMIFC) in Madagascar, the Regional Center for Operations Coordination (RCOC) in Seychelles, Information Fusion Centre-Indian Ocean Region (IFC-IOR) in India, Information Fusion Centre in Singapore (Changi)
- Third countries active in the regions such as US, Japan, Australia
- European actors and entities: EU-funded actions such as MASE Programme, Red Sea Programme, Enhancing Security Cooperation in and with Asia (ESIWA)

3. DESCRIPTION OF THE ACTION

3.1. Objectives and Expected Outputs

The overall objective (Impact) is to contribute to improving maritime security and safety, and cyber security encouraging cross-sectorial, inter-agency and (inter-)regional approaches.

Component 1:

For ease of identification, the new outputs proposed by this Action Document are <u>underlined</u>.

The **Specific Objectives** (Outcomes) of this component are to

1 Promote the adoption and implementation of consistent cybercrime legislation, policies and strategies.
2 Strengthen the due-process compliant capacities and operational skills of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions.
3 Enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence in compliance with international human rights law and engage in international cooperation.

The **Outputs** to be delivered by this component contributing to the corresponding Specific Objectives (Outcomes) are:

Contributing to Outcome 1 (Specific Objective 1)

1.1 Cybercrime policies and strategies strengthened in priority countries, including partnership with private sector, and experience shared with further countries.
1.2 Policy dialogue and cooperation on cybercrime enhanced between priority countries and their regions, international and regional organisations, and synergies maximized with EU-funded (notably IcSP-funded) projects developed in project areas.
1.3 Legislation on cybercrime, electronic evidence and data protection strengthened in line with the Budapest Convention and its Protocols as well as rule of law and human rights standards in priority countries and reforms initiated in additional countries.
1.4 <u>Dialogue strengthened between criminal justice practitioners and policy makers and legislators on matters related to legislation and international cooperation on cybercrime and electronic evidence</u>
1.5 <u>Criminal justice capacities enhanced on emerging issues related to cybercrime and electronic evidence and their implication on legislation.</u>

Contributing to Outcome 2 (Specific Objective 2)

2.1 Assessments/cyber reviews (initial and final) of law enforcement capacities available for priority countries.
2.2 Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries.
2.3 Law enforcement training strategies available in priority countries, including access to and further dissemination of European Cybercrime Training and Education Group (ECTEG) training materials.

2.4 At least 1000 law enforcement officers trained in basic cybercrime investigations and computer forensics as well as related rule of law requirements.
2.5 International police-to-police cooperation on cybercrime and electronic evidence is more effective
2.6 Interagency co-operation strengthened amongst cybercrime units, financial investigators and financial intelligence units in the search, seizure and confiscation of online crime proceeds.

Contributing to Outcome 3 (Specific Objective 3)

3.1 Assessments of criminal justice capabilities available for priority countries.
3.2 Judicial training academies in priority countries are providing training on cybercrime and electronic evidence as part of their regular curricula and experience has been shared with other countries.
3.3 Institutions strengthened, and procedures improved for international judicial cooperation related to cybercrime and electronic evidence in up to 20 countries and experience shared with other countries.
3.4 Training centres, academic institutions and other entities providing criminal justice capacity building programs with a regional scope are strengthened, and training on cybercrime and electronic evidence is streamlined in the respective curricula.
3.5 Criminal justice response adapted to the new challenges of cybercrime investigations and handling of electronic evidence generated by COVID-19 pandemic.

Component 2:

The **Specific Objectives** of this component of the action are:

1. Enhance information exchange and analysis, to support incident coordination and crisis management.
2. Strengthen maritime surveillance, policing, investigation and judiciary.

The **Outputs** to be delivered by this component contributing to the corresponding Specific Objectives (Outcomes) are:

1.1 Information sharing mechanism established to promote a single information sharing environment in the Indo-Pacific. National institutional structures and procedures reviewed to improve the decision-making processes related to maritime governance.

2.1 Cooperation amongst law enforcement agencies and judiciary strengthened at national, international and regional level (not essentially only on maritime issues).

3.2. Indicative Activities

Component 1:

For ease of identification, the new activities proposed by this Action Document are underlined.

Output 1.1 Cybercrime policies and strategies strengthened in priority countries, including partnership with private sector, and experience shared with further countries

1. Organise an international conference on cybercrime and cybersecurity policies. This will serve as the launching event of the project.
2. Organise in-country visits to priority countries to carry out assessments of cybercrime and cybersecurity policies and strategies and related capacities. (It will not be necessary to carry out such assessments for countries already participating in the GLACY project).
3. Support regional/international meetings to share experience and disseminate good practices and develop a guide on cybercrime strategies, including an inventory of existing strategies.
4. Disseminate tools and provide advice – if necessary – on Computer Security Incident or Emergency Response Team (CSIRT/CERT) capacity building.
5. Provide country-specific advice on policies/strategies and relevant aspects of cybersecurity and data protection.
6. Carry out follow up assessments to determine progress made in all countries. (This will also help determine progress made in countries having participated in the GLACY project at some time after its completion).
7. Provide advice on information sharing mechanisms at national, regional and international levels in the area of cybercrime and other forms of public-private partnership.
8. Review and provide advice on legislation and policies on emerging cybercrime threats and issues.
9. Organise an international conference to review progress and agree on strategic priorities. This will serve as the closing event of the project.

10. Provide advice for priority countries on the mechanisms enhancing the interagency cooperation between criminal justice sector, national cyber security agencies and relevant private sector entities, with focus on the creation of information sharing and analysis centres (ISACs), including based on the ENISA ISAC Box toolkit.
11. Organize regional and international meetings on the mechanisms enhancing the interagency cooperation between criminal justice sector, national cyber security agencies and relevant private sector entities.

Output 1.2: Policy dialogue and cooperation on cybercrime enhanced between priority countries and their regions, international and regional organisations, and synergies maximized with EU-funded (notably IcSP-funded) projects developed in project areas.

1. Hold meetings on the policies and measures on cybercrime of relevant international and regional organisations.
2. Support meetings and activities carried out by regional and international organisations as well as special requests emanating from national authorities (through funding of speakers and participants and other means relevant to this action).
3. Support meetings and activities carried out in the context of other EU-funded initiatives and maximize synergies to attain common goals.

Examples of organisations are the African Union Commission, the Organisation of American States, ASEAN, Pacific Islands Law Officers Network (PILON), Indian Ocean Commission, ECOWAS, FOPREL and others.

Output 1.3 Legislation on cybercrime, electronic evidence and data protection strengthened in line with the Budapest Convention and its Protocols as well as rule of law and human rights standards in priority countries and reforms initiated in additional countries

1. Provide advice on cybercrime legislation in line with the Budapest Convention and its Protocols as well as rule of law and human rights, including data protection standards (to priority and any other country seeking assistance on legislation).
2. Document legislation and case law in an online tool.
3. Organise regional and international meetings in view of sharing good practices and promote harmonisation of legislation as well as rule of law and human rights safeguards.
4. Prepare report on global state of cybercrime legislation and present it in conferences
5. Prepare guidelines on managing human rights and rule of law risks within the context of capacity building on cybercrime and electronic evidence
6. Permanent contact with the countries project team to update on the status of the legislative developments
7. Strengthen data protection legislation, strategies, policies, through regional engagement and domestic follow-up
8. Review and provide advice on strengthening legislation on emerging cybercrime threats and issues
9. Organize regional and international meetings for promoting the tools and procedures on enhanced cooperation and disclosure of electronic evidence established in the Second Additional Protocol and to promote the signature and ratification of the Protocol.

Output 1.4 Dialogue strengthened between criminal justice practitioners and policy makers and legislators on matters related to legislation and international cooperation on cybercrime and electronic evidence

1. Organize in-country meetings as platform for dialogue between criminal justice authorities and policy makers and legislators on matters related to legislation on cybercrime and electronic evidence as well as international cooperation
2. Support participation of the hub and priority countries in the global debate on international legal frameworks on cybercrime and electronic evidence, also with reference to the negotiations of the future UN treaty on cybercrime
3. Organize regional and international meetings of relevant policy makers, legislators and relevant stakeholders to promote the implementation of the Budapest Convention on Cybercrime and support the participation in other relevant similar initiatives.

Output 1.5 Criminal justice capacities enhanced on emerging issues related to cybercrime and electronic evidence and their implication on legislation

1. Develop training modules on the dual role of the new technologies (artificial intelligence, privacy-enhancing technologies, cloud computing, blockchain and distributed ledger technologies etc): the leverage of emerging technologies to commit cybercrimes and new technologies as enhancer for more efficient and cost-effective cybercrime investigations including modules on ethical, legal and human rights aspects of new technologies in emerging cybercrime legislative issues
2. Deliver the training modules on new technologies in priority countries, also with participants from other countries/neighbouring countries

3. Prepare a research study on cybercrime victims, addressing the rights, remedies and reparation of the victims and reporting mechanisms and present in regional and international conferences.

Output 2.1 Assessments/cyber reviews (initial and final) of law enforcement capacities available for priority countries

1. Organise in-country visits to carry out assessments of law enforcement capacities (cyber reviews) and prepare initial situation reports for priority countries.
2. Carry out follow up assessments/cyber reviews to determine progress made and further action to be taken in all priority countries.

Output 2.2 Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries.

1. Meetings of heads of cybercrime units and/or criminal investigation departments (CID) to share experience under the project with other countries as well as relevant regional and international organisations.
2. Advice on the setting up and development of cybercrime and computer forensic units (structure, ISO standards, international good practice) with reference to the gap areas identified in assessments in priority countries.
3. In-country workshops and advice on interagency cooperation.
4. In-country workshops and advice on public/private sector cooperation in priority countries, including with multi-national service providers.

Output 2.3 Law enforcement training strategies available in priority countries, including access to and further dissemination of European Cybercrime Training and Education Group (ECTEG) training materials

1. International workshop for cybercrime units and law enforcement training institutions on training strategies (technical level) and access to ECTEG training materials (translated as necessary).
2. In-country meetings (technical level and decision makers) on cyber training strategies.

Output 2.4 At least 1000 law enforcement officers trained in basic cybercrime investigations and computer forensics as well as related rule of law requirements.

1. Select trainers from priority and hub countries and carry out train the trainers courses.
2. Deliver three ECTEG courses or non-ECTEG courses per priority country with participants also from other countries.
3. Develop guides and training tools on data protection requirements and support Data Protection Officers in National Central Bureaus INTERPOL in the delivery of training workshops.
4. Support ad-hoc internships and participation in training events in EU member States.

Output 2.5 International police-to-police cooperation on cybercrime and electronic evidence is more effective

1. Support setting up and strengthening of 24/7 points of contact for cybercrime and e-evidence
2. Joint training workshops for cybercrime units, prosecution, central authorities for mutual legal assistance
3. International workshops on cooperation with Internet service providers
4. Facilitate joint operational activities through regional working groups

Output 2.6 Interagency co-operation strengthened amongst cybercrime units, financial investigators and financial intelligence units in the search, seizure and confiscation of online crime proceeds.

1. Advisory missions on search, seizure and confiscation of online crime proceeds.
2. Introductory training module on cybercrime and financial investigations for cybercrime, financial investigation units, FIUs and specialised prosecutors.
3. Joint workshops (regional and national) aiming to develop cooperation among cybercrime units, financial investigators, FIUs and specialised prosecutors on specific/relevant requests/needs (e.g. virtual currencies, terrorist financing, smuggling of persons if not covered by other actions).
4. Joint training and implement domestic and regional case simulation exercises on cybercrime accompanied by financial investigations.

Output 3.1 Assessments of criminal justice capabilities available for priority countries

1. Organise in-country visits to carry out assessments on criminal justice capacities regarding cybercrime and electronic evidence and prepare initial situation reports. (It will not be necessary to carry out such assessments for countries already participating in the GLACY project).

2. Provide advice to priority countries on collection and reporting mechanisms aiming to develop and implement consistent policy and transparent criminal justice statistical systems. Other opportunities to support monitoring of performance of criminal justice capacities regarding cybercrime and electronic evidence can be explored.
3. Hold regional/international workshops on criminal justice statistics on cybercrime and electronic evidence and prepare a good practice study on this topic to serve as a guide for capacity building activities.
4. Carry out follow up assessments to determine progress made and further action to be taken.

Output 3.2 Judicial training academies in priority countries are providing training on cybercrime and electronic evidence as part of their regular curricula and experience has been shared with other countries

1. Organise meetings with representatives of training institutions of priority countries for sharing experience and reaching agreement on a training concept for prosecutors and judges.
2. Train-the-trainer courses of up to 20 priority countries. (Trainers in the other priority countries will already have been trained under the GLACY project).
3. Develop or adapt training materials for basic, advanced, and specialized modules for each country, including for online delivery.
4. Develop tools and strengthen networking capabilities to support the online engagement of the international community of judicial trainers on cybercrime and electronic evidence.
5. Support the delivery of basic and advanced courses in priority countries with participants from other countries.
6. Provide advice to ensure integration/mainstreaming of training modules in curricula of training institutions.
7. Organise regional meetings to share experience and provide advice to neighbouring countries.
8. Develop and deliver new module on Training Skills and Certification Programme for CoE Trainers on Cybercrime and Electronic Evidence, including for online delivery.

Output 3.3 Institutions strengthened, and procedures improved for international judicial cooperation related to cybercrime and electronic evidence in up to 20 countries and experience shared with other countries.

1. Carry out analyses and compile data on the functioning of the mutual legal assistance process related to cybercrime and electronic evidence.
2. Provide advice to countries on the streamlining of procedures for mutual legal assistance related to cybercrime and electronic evidence, including the tools and procedures available under the Second Additional Protocol.
3. Expand online tools to facilitate international judicial cooperation.
4. Provide training for authorities of priority and other countries involved in judicial cooperation.
5. Organise regional meetings to share experience and provide advice to neighbouring countries.

Output 3.4 Training centres, academic institutions and other entities providing criminal justice capacity building programs with a regional scope are strengthened, and training on cybercrime and electronic evidence is streamlined in the respective curricula.

1. Support regional centres to develop capacity building programs on cybercrime and electronic evidence, where possible through formal agreements and provisioning of grants
2. Provide advice to the regional centres on the streamlining of cybercrime and electronic evidence in the regional training curricula
3. Provide support to establish and maintain regional pools of trainers specialized in cybercrime and electronic evidence, through participation in dedicated training courses or other specific events
4. Fund internship and other training opportunities for criminal justice authorities of priority countries.

Output 3.5 Criminal justice response adapted to the new challenges of cybercrime investigations and handling of electronic evidence generated by COVID-19 pandemic

1. Provide advice on tools and procedures to conduct cybercrime investigations and handle electronic evidence within the restrictions imposed in connection with the COVID-19 pandemic
2. Organise regional meetings to share experience and provide advice to neighbouring countries.

Component 2:

This top-up will add the following activities related to Output 1.1:

1. Provision of satellite technologies and services with a view to identifying dark targets at sea
2. Provision of Satellite Automatic Identification System (SAT-AIS) information as a complement to / and for users that do not have access to SeaVision
3. Provision of access to databases with information about vessels, crew, cargo, history (essential for non-SeaVision data)

4. Enhancing interoperability amongst information fusion and information sharing centres, national maritime coordination and operations centres
5. Access to database for information concerning the protection of Blue Economy.

3.3. Mainstreaming

Environmental Protection & Climate Change

Component 2: Through assistance to addressing maritime pollution, this component of the action contributes to environmental protection.

Gender equality and empowerment of women and girls

Component 1: As per OECD Gender DAC codes identified in section 1.1, this component is labelled as G1. This implies that the component will ensure that gender equality entails equal rights for women and men, as well as the same visibility, empowerment, responsibility and participation, in all spheres of the different activities to be implemented. The criminal justice system is in many of the countries primarily a male domain and the majority of the professionals operating in this crime area are also essentially men. GLACY+ encourages the participation of women in national country coordination teams and in the project activities to be implemented both as recipients of the training packages offered by the project but also through the promotion of the participation of women in the cybercrime and electronic evidence system. The Equality Strategy of the Council of Europe 2018-2023 builds upon the vast legal and policy acquis of the Organization as regards gender equality, as well as the achievements of the first Council of Europe Gender Equality Strategy 2014-2017. It links them to both the current economic context and the political leverage within the Council of Europe, including the overarching priorities of the Organisation. The Strategy outlines the goals and priorities of the Council of Europe on gender equality for the years 2018-2023, identifying working methods and main partners, as well as the measures required to increase the visibility of results.

Component 2: Gender aspects are crucial as women are an important part of the maritime community in the Indo-Pacific. In Somalia the role of a mother is important to help combat piracy which is perpetrated by the youth. A lot of women work in the maritime law enforcement agencies, in the fisheries sector and shipping industry in South and Southeast Asia. Therefore, the integration of a gender-sensitive perspective throughout the project cycle and in accordance to the specificities of the crimes at hand shall make the actions more sustainable through: (i) ensuring that national authorities are aware of relevant women's human rights norms and standards and that they are trained to respect and protect these rights while performing their functions; (ii) promoting the balanced representation of women in the security sector; and (iii) fostering the increased participation of women in all operational activities related to the actions.

Human Rights and Democracy

Component 1: The component will address cybercrime as a specific global and trans-regional threat to human rights, the rule of law, and to the functioning of the democratic societies. The project promotes the adoption of comprehensive and effective legislation on cybercrime that meets human rights and rule of law requirements. The project will pay particular attention to rule of law and human rights conditions and safeguards governing law enforcement powers as well as data protection requirements.

Component 2: A human rights perspective should be mainstreamed especially in the activities under the Specific Objective 2.

Disability

As per OECD Disability DAC codes identified in section 1.1, the action is labelled as D0.

Conflict sensitivity, peace and resilience

By enhancing the protection of the critical infrastructure as regards cybersecurity and maritime security and safety, this action contributes to enhancing the resilience of the relevant countries to security threats.

Disaster Risk Reduction

Component 2: Through assistance to addressing maritime pollution, this component of the action contributes to disaster risk reduction.

3.4. Risks and Lessons Learnt

Component 1:	Risks	Likelihood (High/ Medium/ Low)	Impact (High/ Medium/ Low)	Mitigating measures
	Political instability and insecurity in beneficiary countries	Low	High	Flexibility in activities to allow for varying levels of engagement and focus to avoid an overhaul of project implementation.
	Lack of commitment by the beneficiary country authorities to cooperate.	Low	Medium	The overall political commitment has been ascertained in that priority countries have committed to join the Budapest Convention and/or have adopted domestic legislation in line with this treaty. These countries are thus also represented in the Cybercrime Convention Committee (T-CY) of the Council of Europe as members or observers, and thus subject to peer reviews. The continued involvement in this mechanism fosters commitment and sustainability
	Corruption within the beneficiary structures.	Low	High	Action to be designed featuring solid procedures ensuring the least possible exposure to corruption mechanisms. Provision of internal control procedures vis-à-vis the beneficiary authorities. Strong procurement and financial procedures and processes in place
	Inter-agency rivalry negatively affecting cooperation.	Low	Low	Mitigation procedures already in place: The Project Steering Committee can decide to suspend activities in a specific country
	Lack of willingness to commit to the rule of law and human rights.	Low	High	The overall political commitment has been ascertained in that priority countries have committed to join the Budapest Convention and/or have adopted domestic legislation in line with this treaty. These countries are thus also represented in the Cybercrime Convention Committee (T-CY) of the Council of Europe as members or observers, and thus subject to peer reviews. The continued involvement in this mechanism fosters commitment and sustainability
	Overlapping with other projects (especially county-specific)	Low	Medium	Close coordination with EU Delegations will be ensured. The project seeks to identify the opportunities to cooperate with similar or complementary projects
Component 2:	Difficulty to involve different administration / agencies that should be targeted by the action due to lack of information, lack of interest, competition amongst them. Slow 'political' process necessary for inter-agency initiatives.	High	High	Need for access to high-level country representative to include a decision maker in the processes. Maximise the use of EU political support, including the role of the EU Delegations.
	Due to the sensitivity of maritime information, authorities are not inclined to cooperate.	High	Medium	Activities will be flexible and adjusted to the willingness of each beneficiary country to receive support.
	Difficulties to foster international cooperation	High	Medium	Participatation in international events and a good visibility strategy to advocate for the project action.
	Overlaps with existing EU-funded projects at national and regional level and with projects from other donors	Medium	Medium	Constant assessment of the project environment within EU structures. Formal and informal coordination with other donors and implementing agencies.
	Changes in the priorities of partner countries	High	Medium	The project design introduces necessary level of flexibility to adapt to changes by focusing on particular topics and/or by involving stakeholders from a wide spectrum.
	Current COVID 19 situation and travel ban measures hamper the deployment of the experts in the	High	High	Project activities are planned essentially remotely. This necessitates adaptation of the content of the activity and

	regions and slow down the implementation.			will be organised in person if and when the situation so allows.
	Difficulty to identify a potential owner for IORIS and to transfer the ownership in due time.	High	High	Different possibilities have been identified to transfer ownership of IORIS. A dedicated activity was created to familiarise Asian partners with the system.
	Involvement in a political sensitivity or a maritime dispute.	Medium	Medium	Ensure that activities planned take into account political sensitivities. Avoid to be involved in maritime disputes.
	Duplication of info-exchange systems in the regions.	Medium	Medium	Work closely with information fusion centres to deconflict efforts by offering the IORIS to promote interagency coordination at the national level in Southeast Asia.
	Risk of fragmentation or dilution of the action in case of a too high number of beneficiaries	Medium	Medium	Sequence the project's implementation through a roling plan by region, finding the right balance between EU political priorities, interest and the needs of beneficiary countries to use IORIS in the long term.
	Unsustainability of the actions/tools put in place	High	High	Put in place low cost solutions and advocate to facilitate mutualisaiton of costs.

Lessons Learnt:

Component 1: In light of the experience that the EU and the Council of Europe have gained, some key lessons and best practices can be drawn:

- the creation of inter-agency national project teams across the criminal justice chain that foster ownership, ensure alignment with national priorities and help an institutional change process;
- cooperation with national judicial and law enforcement academies and incorporation of training modules in their curricula which enhances the efficiency of the action and its chances of sustainability;
- use of the new global set-up, generated by COVID-19 pandemic as leverage to spread key messages to a vast audience, reach out to new countries and enhance visibility, through global online events attracting an increasing global audience of criminal justice practitioners;
- ensure sustainability of judicial training on cybercrime through supporting an international network of national judicial trainers on cybercrime; scalability of the support provided is ensured through the development of Train-the-Trainers modules.
- co-operation and information sharing between specialised cybercrime units and other fields, is shared through the action's partnership with EC3 at Europol and its European Cybercrime Training and Education Group (ECTEG).

Component 2: The following lessons were learnt and best practices identified during CRIMARIO I and the inception phase of CRIMARIO II:

- CRIMARIO I has clearly contributed positively in a number of ways. It has directly and indirectly helped enhance the interest in and political will to address challenges to maritime security and safety in the Western Indian Ocean. Secondly, the EU is widely recognised to have filled a specific need through IORIS and the trainings, which are highly-valued in the region. The IORIS platform is unique in its ambition and construction, while trainings have in turn helped participants in their career mobility and advancement.
- However, in the first phase the project has faced some challenges, namely related to the overlap of objectives with the MASE programme. During CRIMARIO II, relationships with MASE and the Indian Ocean Commission have improved considerably, with the support of the EUD in Mauritius. As a result, an action plan of joint activities between CRIMARIO and MASE/Indian Ocean Commission has been agreed. To date, no practical implementation has yet taken place, however the EC and EUD in Mauritius work jointly towards encouraging practical cooperation.
- It is crucial to be introduced to a country by the EU Delegation and conduct a formal introductory meeting with relevant Ministries, before proceeding to cooperation at a technical level.
- Regional information fusion centers have demonstrated a willingness to be interoperable with one another.
- The Indian Ocean Commission has explicitly stated that it would appreciate CRIMARIO serving as an interface with EU institutions.
- There are clearly capability gaps when it comes to monitoring vessels conducting coercive activities in the outer extremities of Exclusive Economic Zones and the High Seas. This has necessitated the need of exploiting satellite technologies to identify dark targets.
- There is a deficiency of secure information-exchange platforms for interagency cooperation in a number of Southeast Asian countries.
- The Western Indian Ocean lacks a single information sharing environment which CRIMARIO aspires to address through the use of IORIS.

- The increase in coast guards to conduct maritime law enforcement duties in the region necessitates a high level of operational coordination and information-sharing
- For beneficiaries, maximising the advantages of increased technical capabilities also requires a robust enhancement of training and capacity building initiatives focussed on data analysis, processing and visualisation to provide enriched actionable information.

3.5. The Intervention Logic

The underlying intervention logic for **Component 1** is that

IF cybercrime policies and strategies are strengthened in up to 20 countries, including relevant aspects of cybersecurity and partnerships with private sector, and if experience is shared with further countries,

IF a policy dialogue and cooperation on cybercrime are enhanced between priority countries and their regions, international and regional organisations, and synergies are maximized with relevant EU-funded projects,

IF legislation on cybercrime electronic evidence and related data protection provisions are strengthened in line with the Budapest Convention and its Protocols as well as rule of law and human rights standards in priority countries and reforms are initiated in additional countries,

IF a dialogue is strengthened between criminal justice practitioners and policy makers and legislators on matters related to legislation and international cooperation on cybercrime and electronic evidence,

IF criminal justice capacities are enhanced on emerging issues related to cybercrime and electronic evidence and their implication on legislation,

THEN consistent cybercrime legislation, policies and strategies are promoted.

IF assessments/cyber reviews (initial and final) of law enforcement capacities are available for priority countries,

IF cybercrime and computer forensics units are strengthened in priority countries and experience is shared with other countries,

IF law enforcement training strategies are available in priority countries, including access to European Cybercrime Training and Education Group (ECTEG) training materials,

IF at least 1000 law enforcement officers are trained in basic cybercrime investigations and computer forensics as well as on related rule of law requirements,

IF international police-to-police cooperation on cybercrime and electronic evidence is more effective,

IF law enforcement training strategies are available in priority countries, including access to ECTEG training materials,

THEN the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions is strengthened.

IF assessments of criminal justice capabilities are available for priority countries,

IF judicial training academies in priority countries are providing training on cybercrime and electronic evidence as part of their regular curricula and experience has been shared with other countries,

IF institutions are strengthened and procedures improved for international judicial cooperation related to cybercrime and electronic evidence in at least 20 countries and experience is shared with other countries,

IF training centres, academic institutions and other entities providing criminal justice capacity building programmes with a regional scope are strengthened and training on cybercrime and electronic evidence is streamlined in the respective curricula,

IF criminal justice response is adapted to the new challenges of cybercrime investigations and handling of electronic evidence generated by COVID-19 pandemic,

THEN criminal justice authorities can apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.

The underlying intervention logic for **Component 2** is that

IF an information sharing mechanism is established to promote a single information sharing environment in the Indo-Pacific and national institutional structures and procedures are reviewed to improve the decision-making processes

related to maritime governance, **ASSUMING** that information fusion centers are willing to take an active role in developing the SHARE.IT interface initiative,

THEN information exchange and analysis are enhanced, to support incident coordination and crisis management.

IF cooperation amongst law enforcement agencies and judiciary is strengthened at national, international and regional level (not essentially only on maritime issues), **ASSUMING** that COVID allows the conduct of in-country courses,

THEN maritime surveillance, policing, investigation and judiciary are strengthened.

3.6. Logical Framework Matrix

Results	Results chain	Indicators	Baselines (values and years)	Targets (values and years)	Sources of data	Assumptions
Impact	Contribute to improving maritime security and safety, and cyber security encouraging cross-sectorial, inter-agency and (inter-) regional approaches.	1 Increased number of investigations, prosecutions and adjudications of domestic and international cases of cybercrime and other offences involving electronic evidence 2 Increased compliance with international standards on cybercrime and rule of law, including data protection standards 3 Regional Organisations view CRIMARIO as a facilitator of a single information sharing environment.	2022-023	DCoC, IOC, ASEAN and BIMSTEC	Beneficary Partners	*Not applicable*
COMPONENT 1:						
Outcome 1	To promote consistent cybercrime legislation, policies and strategies	- Increased availability and quality of legislation on cybercrime and electronic evidence in line with the Budapest Convention - Increased quantity and quality of cybercrime policies and strategies in priority countries			Assessments and progress reviews carried out under the project. Annual report on cybercrime legislation	
Output 1 related to Outcome 1	Cybercrime policies and strategies are strengthened in up to 20 countries, including relevant aspects of cybersecurity and partnerships with private sector, and experience is shared with further countries	- Cybercrime and cybersecurity policies and strategies prepared or improved in priority countries - Situation reports on cybercrime and cybersecurity policies and strategies for priority countries available Progress reports available for priority countries by month 96			Assessments and progress reviews carried out under the project. Project reports	Draft strategies or amendments are subsequently adopted.
Output 2 related to Outcome 1	Policy dialogue and cooperation on cybercrime enhanced between priority countries and their regions, international and regional organisations, and synergies maximized with relevant EU-funded projects	- Number of joint meetings with international and regional organisations - Number of activities by regional and international organisations supported by the project - Level of participation by other organisations in project activities - Number of joint activities organized with other EU-funded initiatives			Assessments and progress reviews carried out under the project. Project reports.	More consistent advice and support by regional and international organization will favour more consistent domestic policies/strategies.

Output 3 related to Outcome 1	Legislation on cybercrime electronic evidence and related data protection provisions are strengthened in line with the Budapest Convention and its Protocols as well as rule of law and human rights standards in priority countries and reforms initiated in additional countries.	- Amendments or draft laws available in up to 30 States in line with Budapest Convention and its Protocols and rule of law/human rights and data protection requirements - Accession to / ratification of Budapest Convention on Cybercrime by at least 15 States - Accession request by at least an additional 15 States - Enhanced online tool on cybercrime legislation and case law by month 48 - Global reports on cybercrime legislation by month 36, 60, 84			Assessments and progress reviews carried out under the project. Project reports.	Draft laws will be submitted to Parliament and adopted.
Output 4 related to Outcome 1	Dialogue strengthened between criminal justice practitioners and policy makers and legislators on matters related to legislation and international cooperation on cybercrime and electronic evidence	- Cybercrime laws in line with Budapest Convention adopted by at least 15 States - Increased participation of countries in the negotiations of the future UN treaty on cybercrime			Assessments and progress reviews carried out under the project. Project reports.	The relevance of the Budapest Convention as the international treaty on cybercrime and electronic evidence is promoted.
Output 5 related to Outcome 1	Criminal justice capacities enhanced on emerging issues related to cybercrime and electronic evidence and their implication on legislation	- Training on new technologies and use of new technologies in cybercrime cases developed - Up to 40 courses on new technologies delivered - Study on the victims' rights, remedies and reparation and reporting mechanisms by month 96			Assessments and progress reviews carried out under the project. Project reports.	Training will enhance skills of judges and prosecutors and thus lead to improved prosecutions and adjudications.
Outcome 2	To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions	- Increased number of domestic and international investigations on cybercrime and electronic evidence			Assessments and progress reviews carried out under the project.	Stronger law enforcement capacities will strengthen the application of legislation and international cooperation. Priority countries will encourage other countries to follow their example.
Output 1 related to Outcome 2	Assessments/cyber reviews (initial and final) of law enforcement capacities available for priority countries	- Assessment reports (cyber reviews) for priority countries available by month 15 and for additional countries by month 27 and month 54 - Progress reports available for priority countries by month 60			Assessments and progress reviews carried out under the project. Project reports.	Assessments will identify strengths and gaps and needs for capacity building.
Output 2 related to Outcome 2	Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries	- Improved structures, procedures and interagency cooperation of specialized units in priority countries			Assessments and progress reviews	Specialised units will play an essential role with regard to

		- Good practice guides available and disseminated			carried out under the project. Project reports.	overall law enforcement capacities.
Output 3 related to Outcome 2	Law enforcement training strategies available in priority countries, including access to ECTEG training materials	- National law enforcement training strategies prepared in priority countries by month 24 - Cybercrime units and training academies have access to ECTEG training materials (translated as necessary) by month 24			Assessments and progress reviews carried out under the project. Project reports.	Training strategies are implemented and ECTEG materials are made use of.
Output 4 related to Outcome 2	At least 1000 law enforcement officers trained in basic cybercrime investigations and computer forensics as well as related rule of law requirements	- At least 1000 law enforcement officers from priority and other countries are trained in at least one ECTEG course (updated and translated as necessary).			Assessments and progress reviews carried out under the project. Project reports.	Officers trained will apply their new skills.
Output 5 related to Outcome 2	International police-to-police cooperation on cybercrime and electronic evidence is more effective	- Increased number of police-to-police requests - Increased number of requests handled by 24/7 points of contact			Assessments and progress reviews carried out under the project. Project reports.	Training strategies are implemented and ECTEG materials are made use of.
Output 6 related to Outcome 2	Law enforcement training strategies available in priority countries, including access to ECTEG training materials	- National law enforcement training strategies prepared in priority countries by month 24 - Cybercrime units and training academies have access to ECTEG training materials (translated as necessary) by month 24			Assessments and progress reviews carried out under the project. Project reports.	Training strategies are implemented and ECTEG materials are made use of.
Outcome 3	To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation	- Increased number of prosecutions and cases adjudicated on cybercrime and electronic evidence in priority countries - Regional training centres established and delivering courses on cybercrime and electronic evidence relevant for this action.			Assessments and progress reviews carried out under the project.	Enhanced capacities of prosecutors and judges regarding cybercrime and electronic evidence will contribute to the rule of law, including the application of legislation as well as international cooperation.

						Priority countries will encourage other countries to follow their example.
Output 1 related to Outcome 3	Assessments of criminal justice capabilities available for priority countries	- Situation reports on cybercrime legislation for priority countries available by month 15 and for additional countries by month 27 - Progress reports available for up to 15 countries by month 60			Assessments and progress reviews carried out under the project. Project reports.	The assessments will prepare the ground for reforms and strengthening of criminal justice capacities.
Output 2 related to Outcome 3	Judicial training academies in priority countries are providing training on cybercrime and electronic evidence as part of their regular curricula and experience has been shared with other countries	- Training on cybercrime and electronic evidence is reflected in the regular curriculum of training institutions of priority countries - Basic, advanced and specialized training modules available in priority countries - At least 200 trainers trained - Up to 60 basic advanced and specialized courses delivered and 800 judges, prosecutors and other legal professionals trained			Assessments and progress reviews carried out under the project. Project reports.	Training will enhance skills of judges and prosecutors and thus lead to improved prosecutions and adjudications.
Output 3 related to Outcome 3	Institutions strengthened and procedures improved for international judicial cooperation related to cybercrime and electronic evidence in at least 20 countries and experience shared with other countries	- Draft amendments to procedures and rules for MLA in up to 20 countries by month 96 - At least 80 officers responsible for MLA trained - Enhanced online tool for international judicial cooperation available by month 15			Assessments and progress reviews carried out under the project. Project reports.	Draft amendments will be adopted and officers trained will apply their skills
Output 4 related to Outcome 3	Training centres, academic institutions and other entities providing criminal justice capacity building programs with a regional scope are strengthened and training on cybercrime and electronic evidence is streamlined in the respective curricula	- At least 5 Regional training centres supported to offer programs on cybercrime and electronic evidence in line with the Budapest Convention - At least 20 regional trainers trained - At least 20 non-priority countries attending regional training events			Assessments and progress reviews carried out under the project. Project reports.	It is assumed that regional centres will function in the project regions and/or that national training institutions will commit to act regionally.
Output 5 related to Outcome 3	Criminal justice response adapted to the new challenges of cybercrime investigations and handling of electronic evidence generated by COVID-19 pandemic	- New procedures to conduct cybercrime investigations and to handle electronic evidence in priority countries developed - Good practice available and disseminated			Assessments and progress reviews carried out under the project. Project reports.	The advice will prepare the ground for reforms and adaptation of cyberjustice

COMPONENT 2:						
Outcome 1	Information exchange and analysis enhanced, to support incident coordination and crisis management	- IORIS becomes the tool of choice to facilitate the exchange of information for at least 7 WIO partners including regional organisations - IORIS becomes the tool of choice to facilitate the exchange of information for at least 3 SA partners including regional organisations - IORIS becomes the tool of choice to facilitate the exchange of information for at least 2 SEA partners including regional organisations.	1.1 2021 1.2 2021 1.3 2022	- RCoC, RMIFC, Seychelles, Comoros, Kenya, Madagascar, Somalia - Maldives, Sri Lanka - The Philippines and Vietnam	Beneficary Partners	Regional Organsiations such as the IOC, ASEAN, BIMSTEC promote CRIMARIO in their respective areas of responsibility
Outcome 2	Maritime surveillance, policing, investigation and judiciary strengthened.	- CRIMARIO-organised exercises are viewed as an option to improve interagency coordination	2022 for SA countrie2023 for SEA countries	Maldives and Sri Lanka The Philippines, and Vietnam	Beneficary Partners	Partner countries welcome CRIMARIO efforts notwithstanding the presence of other strong actors
Output 1 related to Outcome 1	Information sharing mechanism established to promote a single information sharing environment in the Indo-Pacific. National institutional structures and procedures reviewed to improve the decision-making processes related to maritime governance.	- SHARE.IT is adopted in the Indo-Pacific	2022	The three information fusion centres in the Indo-Pacific plus Indonesia and the US	Beneficary Partners	Information fusion centres are willing to take an active role in developing the SHARE.IT interface initiative
Output 1 related to Outcome 2	Cooperation amongst law enforcement agencies and judiciary strengthened at national, international and regional level (not essentially only on maritime issues)	- Conduct of Maritime Law Enforecement Courses	2022	Min 3 countries in SEA start receiving direct support through maritime courses	Beneficary Partners	COVID allows the conduct of in-country courses

4. IMPLEMENTATION ARRANGEMENTS

4.1. Financing Agreement

In order to implement this action, it is not envisaged to conclude a financing agreement with the partner countries.

4.2. Indicative Implementation Period

The indicative operational implementation period of this action, during which the activities described in section 3 will be carried out and the corresponding contracts and agreements implemented, is 72 months from the date of adoption by the Commission of this Financing Decision.

Extensions of the implementation period may be agreed by the Commission's responsible authorising officer by amending this Financing Decision and the relevant contracts and agreements.

4.3. Implementation Modalities

The Commission will ensure that the EU appropriate rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures[3].

4.3.1. Indirect Management with a Member State Organisation and an international organisations

Component 1: This component of the action may be implemented in indirect management with the Council of Europe. This implementation entails carrying out all the activities as described in chapter 4.1 aiming to strengthen the capacities of countries worldwide to apply legislation on cybercrime and electronic evidence and enhance their ability for effective international cooperation in this area in compliance with international human rights standards and the rule of law. The envisaged entity has been selected using the following criteria: the Council of Europe has a unique expertise in the domains the proposed action intends to address. The CoE is the guardian of the Budapest Convention on Cybercrime, the main international legal instrument to fight cybercrime and as such possesses unique experience in providing effective and sustainable capacity building in this domain. Moreover, the CoE has been and efficient implementer of previous phases of the project.

Component 2: This component of the action may be implemented in indirect management with Expertise France.

The entity was selected by the Commission's services using in particular the following criteria: operational capacity, experience and value added. The implementation by this entity entails achieving all the activities as described in chapter 4.1 aiming to support partner countries in the Indian Ocean and Southeast Asia to adequately address maritime-related issues and maritime security challenges in a comprehensive manner, encouraging cross-sectorial and interregional approaches.The Member State organisation identified above, is currently undergoing an ex-ante assessment of its systems and procedures for all pillars under Article 154(4) of the Financial Regulation. This assessment is expected be finalised by 31 December 2021. In the meantime, contractual clauses will be included in the contribution agreement signed with the Expertise France. Supervisory measures could also be necessary depending on the results of the ex-ante assessment.

In case the envisaged entities would need to be replaced, the Commission's services may select a replacement entity using the same criteria.

4.3.2. Changes from indirect to direct management mode (and vice versa) due to exceptional circumstances

In the interest of the programme, or if the negotiations with the selected entities fail, all parts of this action may be implemented in direct management.

[3] www.sanctionsmap.eu. Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website it is the OJ version that prevails.

4.4. 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.

4.5. Indicative Budget

Indicative Budget components	EU contribution (amount in EUR)	Indicative third-party contribution (amount in EUR)
Component 1: Indirect management with an international organisation (Council of Europe) - cf. section 4.3.1	5 000 000	555 556
Component 2: Indirect management with a Member State Organisation (Expertise France) - cf. section 4.3.1	4 000 000	0
Evaluation – cf. section 5.2; **Audit** – cf. section 5.3	will be covered by another Decision	
Communication and visibility – cf. section 6	will be covered by another Decision	
Contingencies	N/A	
Totals	9 000 000	555 556

4.6. Organisational Set-up and Responsibilities

Component 1: The implementation of this component will be coordinated and led by the Council of Europe. An appropriate management structure will continue to exist based on the ongoing arrangement of GLACY+, to ensure the coherence of the project.

Component 2: The implementation of this component will be coordinated and led by the European Commission. CRIMARIO II's management structure will continue to be applied to ensure the coherence of the activities under this component.

Activities under all result areas will commence with an assessment of capabilities and conclude with an assessment of progress made. The component will support processes of reform by combining measures at policy levels with measures at the level of practitioners, and by combining activities at domestic levels with regional and international activities.

Moreover, in order to guarantee the necessary strategic orientation of the programme, the Contracting Authority together with the implementing partners will establish and co-chair a *Steering Committee* for each of the two components aiming to monitor progress made in implementation, approve the work plans of the respective components, approve ad-hoc support to a specific country, review progress reports and other documentation, ensure the participation of all relevant stakeholders in activities, promote synergies with actions of bilateral and regional cooperation of the EU and its Member States and coordination with actions financed by other donors.

4.7. Pre-conditions

N/A

5. PERFORMANCE MEASUREMENT

5.1. 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 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).

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).

5.2. Evaluation

In case an evaluation is not planned, the Commission may, during implementation, decide to undertake such an evaluation for duly justified reasons either on its own decision or on the initiative of the partner.

The Commission shall inform the implementing partner at least one month 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 may 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.

5.3. Audit and Verifications

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 audit or verification assignments for one or several contracts or agreements.

6. COMMUNICATION AND VISIBILITY

Communication and visibility is a contractual obligation for all entities implementing EU-funded external actions to advertise the European Union's support for their work to the relevant audiences.

To that end they must comply with the instructions given in the *Communication and Visibility Requirements* of 2018 (or any successor document), notably with regard to the use of the EU emblem and the elaboration of a dedicated communication and visibility plan, to be completed for every action at the start of implementation.

These obligations apply equally, regardless of whether the actions concerned are implemented by the Commission, the partner country (for instance, concerning the reforms supported through budget support), contractors, grant beneficiaries or entrusted entities. In each case, a reference to the relevant contractual obligations must be included in the respective financing agreement, procurement and grant contracts, and delegation agreements.

Communication and visibility measures may be funded from the amounts allocated to the action. For the purpose of enhancing the visibility of the EU and its contribution to this action, the Commission may sign or enter into joint declarations or statements, as part of its prerogative of budget implementation and to safeguard the financial interests of the Union. Visibility and communication measures should also promote transparency and accountability on the use of funds.

Effectiveness of communication activities on awareness about the action and its objectives as well as on EU funding of the action should be measured.

Implementing partners shall keep the Commission and concerned EU Delegation/Office fully informed of the planning and implementation of specific visibility and communication activities before work starts. Implementing partners will ensure adequate visibility of EU financing and will report on visibility and communication actions as well as the results of the overall action to the relevant monitoring committees.

APPENDIX 1 REPORTING IN OPSYS

An Intervention[4] (also generally called project/programme) is the operational entity associated to a coherent set of activities and results structured in a logical framework aiming at delivering development change or progress. Interventions are the most effective (hence optimal) entities for the operational follow-up by the Commission of its external development operations. As such, Interventions constitute the base unit for managing operational implementations, assessing performance, monitoring, evaluation, internal and external communication, reporting and aggregation.
Primary Interventions are those contracts or groups of contracts bearing reportable results and respecting the following business rule: 'a given contract can only contribute to one primary intervention and not more than one'. An individual contract that does not produce direct reportable results and cannot be logically grouped with other result reportable contracts is considered a 'support entities'. The addition of all primary interventions and support entities is equivalent to the full development portfolio of the Institution.

Primary Interventions are identified during the design of each action by the responsible service (Delegation or Headquarters operational Unit).
The level of the Primary Intervention is defined in the related Action Document and it is revisable; it can be a(n) (group of) action(s) or a (group of) contract(s).

Tick in the left side column one of the three possible options for the level of definition of the Primary Intervention(s) identified in this action.
In the case of 'Group of actions' level, add references to the present action and other action concerning the same Primary Intervention.
In the case of 'Contract level', add the reference to the corresponding budgetary items in point 4.6, Indicative Budget.

Option 1: Action level		
☐	Single action	Present action: all contracts in the present action
Option 2: Group of actions level		
☐	Group of actions	Actions reference (CRIS#/OPSYS#):
Option 3: Contract level		
☒	Single Contract 1	Contract with Council of Europe
☒	Single Contract 2	Contract with Expertise France
☐	Group of contracts 1	

[4] ARES (2021)4204912 - For the purpose of consistency between terms in OPSYS, DG INTPA, DG NEAR and FPI have harmonised 5 key terms, including 'action' and 'Intervention' where an 'action' is the content (or part of the content) of a Commission Financing Decision and 'Intervention' is a coherent set of activities and results which constitutes an effective level for the operational follow-up by the EC of its operations on the ground. See more on the concept of intervention.