**ANNEX II**

of the Commission Implementing Decision on the Annual Action Programme 2017 for Article 5 of the Instrument contributing to Stability and Peace (IcSP)

### Action Document for Fighting Organised Crime

| 1. Title/basic act/ CRIS number | Fighting Organised Crime  
| CRIS number: IFS/2017/040125 financed under IcSP |
| 2. Zone benefiting from the action/location | Miscellaneous countries |
| 4. Sector of concentration/thematic area | Fight against organised crime | DEV. Aid: YES |
| 5. Amounts concerned | Total estimated cost: EUR 10 550 000  
| | Total amount of EU budget contribution EUR 10 250 000 |
| 6. Aid modality(ies) and implementation modality(ies) | Project Modality:  
| | Indirect management with the Council of Europe (Component 1: Cybercrime) and the United Nations Office on Drugs and Crime (Component 2: Small Arms and Light Weapons - SALW); Direct management with procurement of services (Component 3: Falsified Medicine) |
| 7 a) DAC code(s) | 15130 - Legal and judicial development (Component 1)  
| | 15240 - Reintegration and SALW control (Component 2)  
| | 15130 - Legal and judicial development (Component 3) |
| b) Main Delivery Channel | 10000 - Public Sector Institutions |
| 8. Markers (from CRIS DAC form) | General policy objective | Not targeted | Significant objective | Main objective |
| Participation development/good governance | | | |
| Aid to environment | X | | |
| Gender equality (including Women In Development) | X | | |
| Trade Development | X | | |
| Reproductive, Maternal, New born and child health | X | | |
| RIO Convention markers | Not targeted | Significant objective | Main objective |
| Biological diversity | X | | |
| Combat desertification | X | | |
| Climate change mitigation | X | | |
| Climate change adaptation | X | | |
| 9. Global Public Goods and Challenges (GPGC) thematic flags | Not applicable |
| 10. SDGs | Primarily SDG 16 "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels", and subsidiary SDG 3 "Ensure healthy lives and promote well-being for all at all ages". |
SUMMARY

All components in this Annex aim to address the fight against different angles of organised crime activities, as identified in the IcSP Strategy paper 2014-2020 and Multiannual Indicative Programme 2014-2017. The proposed approach for all Components is in line with the IcSP’s security orientation and programming principles, while it seeks to strengthen the internal-external security nexus in support of the implementation of the European Agenda on Security and at the same time contribute primarily to the progressive achievement of SDG 16 of Agenda 2030.

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

Component A: Cybercrime

The specific objective is 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 joint EU-Council of Europe project "Global Action on Cybercrime", in order to further consolidate its results and expend its coverage, it is proposed to implement this action in indirect management with the Council of Europe, in close cooperation with EU Member States that already serve as project partners (Estonia, France, Romania, United Kingdom) as well as the European Cybercrime Centre at Europol (EC3) and INTERPOL.

Component B: Small Arms and Light Weapons

The specific objective is to prevent and counter illicit manufacturing and trafficking in firearms, and their links to transnational organized and other serious crimes, and promoting the ratification and implementation of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organised Crime (UNTOC). Considering that United Nations Office on Drugs and Crime (UNODC) serves as a guardian of UNTOC and its Protocols, and the long-standing experience of is Global Firearms Programme, it is proposed to implement this action in indirect management with UNODC.

Component C: Falsified medicine

The specific objective is to empower and add value to the systems which are already in place for combatting the trafficking, identification and effective management of falsified medicines and medicinal products in Eastern and Central African region. It is proposed to implement this component in direct management through a service contract awarded to a consortium from EU Member States or EU Member States and EU agencies.
1 CONTEXT

1.1 Sector/Country/Regional context/Thematic area

Transnational organised crime is a multi-faceted phenomenon and manifests itself in different activities including drug trafficking, trafficking in human beings, in firearms, in falsified medicine, and money laundering. Over the years, serious and organised crime has evolved in a dynamic and ever evolving phenomenon. Although it is difficult to measure the exact size of illicit markets, evidence drawn from law enforcement activity across the world suggests they are very large in both scale and impact. Serious and organised crime has a significant impact on the growth of the legal economy and society as a whole. The investment of criminal proceeds and trade in illicit commodities is interlinked with tax avoidance and money laundering that strengthens criminal enterprises run by or associated with Organised Crime Groups (OCGs). Particularly in developing countries and in post-conflict situations, organised crime patronage networks serve as a source of instability that undermine positive changes in the area of stability, governance and socioeconomic development or even endanger post-conflict transitions. Together with corruption they have a devastating impact on the rule of law and hinder equal access to public services. Considering that organised crime requires a holistic criminal justice response, there are several broad cross-cutting issues that need to be taken into consideration, most notably the difficulties faced by women within the justice and security sectors, as well as the challenges for children, minorities and other vulnerable groups.

Component 1: Cybercrime

In many developing countries the use of information and telecommunication technologies (ICT) is rapidly spreading and a number of them are undertaking important efforts to benefit from the development prospects offered by ICT and expanding broadband services. One example is mobile payments which are most popular in Africa and facilitate economic transactions also in rural areas. However, these opportunities are exploited by – often organised – criminals as reflected in massive fraud schemes, computer intrusions, terrorist use of ICT, threats to critical information infrastructure and many other phenomena. Malware infection rates are considerably higher in developing and many exploits appear to be targeting vulnerabilities in computer systems located in developing countries. Different types of Internet fraud are widespread. Advance-fee fraud schemes are operated by criminal enterprises associated with West Africa and cause major losses around the world. A sizeable share of users of mobile payment services are reported to fall victims to cybercrime. Cybercrime affects the security of individuals and increasingly children in developing countries fall victim to online sexual violence, for example through live streaming of sexual abuse. Criminal enterprises exploit the Internet to trade in counterfeit medicines online with developing countries as primary targets for substandard, non-approved or counterfeit medicines. Many countries are not able to protect their critical information infrastructure against intentional attacks or non-intentional security incidents. Alarmingly, the fact that any crime may entail electronic evidence on a computer system has serious implications for criminal justice systems in that large computer forensic capabilities are required and in that all law enforcement officers, prosecutors and judges of a State need to be enabled to deal with electronic evidence. Measures to secure volatile electronic evidence and bring offenders to justice require efficient international cooperation.

Progress has been made in recent years with regard to international cooperation: the Council of Europe (CoE) Convention on Cybercrime ("Budapest Convention"), the only international treaty on Cybercrime, has played a major role in this respect. Many countries have begun to reform their legislation, and tools and good practices are available with regard to legislation,
the creation of high-tech crime units, law enforcement and judicial training, partnerships between public and private sector and international cooperation.

**Component 2: Small Arms and Light Weapons**

The illicit trafficking of small arms and light weapons (SALW) is part of the core business of organised crime groups. Alongside other forms of trafficking, such as drugs, it is a key source of revenue. SALW leverage other forms of criminality and are used for intimidation, coercion and gang violence, while terrorist networks are accessing weapons and explosives through organised crime networks and the black market. Moreover, most present day conflicts are fought with and the majority of deaths caused in conflict, particularly among the civilian population, are attributed to SALW which are the weapons of choice in civil wars. SALW availability is also linked to human rights violations ranging from killings and torture to sexual violence and forced recruitment by armed groups.

There is a clear link between armed violence and limited progress on development goals as conflict fuels poverty and impedes economic growth. Porous, uncontrolled borders and increased global trade create new opportunities for illicit trafficking in SALW, their ammunition and explosives. Although there are no reliable figures on the number of SALW in circulation globally, it is considered that the majority are in private hands. Much of the SALW originally come from licit trade but are diverted into illicit channels often as a result of weak governance, theft from national stockpiles, support to foreign armed groups or state-armed civilians. Linkages with organised crime and drug trafficking are frequent. Little is known, however, about the extent of arms flows within and between regions.

**Component 3: Falsified Medicine**

Falsified medicines are fake medicines that pass for real, safe and effective medicines. They might contain ingredients, including active ingredients, which are of bad quality or in the wrong dose – either too high or too low. Falsified medicines are a major and growing threat to public health and safety as they have not been properly evaluated to check their quality, safety and efficacy and they usually contain ingredients of bad quality, in the wrong dose or simply ineffective, and in some cases even toxic.

Their illicit production and trafficking, as that of their chemical precursors, affect massively the poorest and most vulnerable populations. Accessibility to medical treatments and medical products in many developing countries is a challenge in itself, making their populations particularly exposed and vulnerable to the dangers of falsified medicines. Approximately 100,000 deaths per year in Africa are due to the trade of falsified medicines according to the World Health Organisation. Patients in developing countries can turn to the illegal market due to the lower prices, without appropriately measuring the risks they incur. If there is an insufficient regulatory authority and no appropriate means for individuals to verify the authenticity of a medical product, the patient is also subject to purchasing illegitimate products without knowledge. The impact of falsified medicines is particularly serious on

---

1 Although there has not been a consensus on a globally accepted definition of falsified medicine, the EU's Directive 2011/62/EU states that a falsified medicinal product is "any medicinal product with a false representation of: (a) its identity, including its packaging and labelling, its name or its composition as regards any of the ingredients including excipients and the strength of those ingredients; (b) its source, including its manufacturer, its country of manufacturing, its country of origin or its marketing authorisation holder; or (c) its history, including the records and documents relating to the distribution channels used".
women, since they are often in charge of caring for sick family members, children and elderly people. Raising women’s awareness on this aspect of falsified medicine is therefore crucial.

The appeal of high financial gains, combined with the perceived low risk of detection and prosecution, and the leniency of the penalties (compared with other forms of illicit trafficking) make the production and trafficking in falsified medicines and medicinal products an attractive commodity to criminal groups.

1.1.1 Public Policy Assessment and EU Policy Framework

The 2016 "Global Strategy for the European Union’s Foreign and Security Policy" identifies security as a priority area of the EU's external engagement. In addition, as part of the relevant EU policy framework in the broader area of security, the EU’s dialogue and cooperation with non-EU countries is shaped by different documents, most importantly the 2003 European Security Strategy [European Council, 12 December 2003] and the external dimension of the 2015 European Agenda on Security [COM(2015) 185 final, 28.4.2015], while the 2016 Joint Communication "Elements for an EU-wide strategic framework to support security sector reform" [JOIN(2016) 31 final, 5.7.2016] highlights that "helping partner countries to reform their security systems supports the EU’s objectives of peace and stability, inclusive and sustainable development, state-building and democracy, the rule of law, human rights and the principles of international law". The external dimension of related internal policies complement this framework, with most notable example the EU policy cycle for organised and serious international crime (EMPACT).

More generally, the United Nations Transnational Organized Crime Convention (UNTOC) ratified by 182 States is the main international instrument to address organised crime, supplemented by its three Protocols which target specific areas and manifestations of organised crime: the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition.

The proposed action document is inspired by the Agenda 2030 and the sustainable development goal (SDG) 16 to "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels", and it shall also support the fulfilment of SDG 3 on healthy lives and the well-being for all at all ages and SDG 5 aimed to achieve gender equality and empower all women and girls. While organised crime affects men, women and children indiscriminately, historically women have been excluded from criminal justice institutions, and to address this challenge the proposed action document shall, inter alia, contribute to the involvement of women in relevant policy and governance decision-making processes in line with the EU Gender Action Plan ["Gender Equality and Women's Empowerment: Transforming the Lives of Girls and Women through EU External Relations (2016-2020)", SWD(2015) 182 final, 29.09.2015].

Component 1: Cybercrime

The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [JOIN(2013) 1 final, 07.02.2013] and the European Agenda on Security [COM(2015) 185 final, 28.4.2015] provide the overall strategic framework for the EU initiatives on cybercrime and cybersecurity more broadly. Cyber capacity building is a key component of the EU's Cybersecurity Strategy which notes the need to "Develop capacity building on cybersecurity and resilient information infrastructures in third countries", referenced also in the European
Agenda on Security that calls for "Enhancing cyber capacity building action under external assistance instruments". This engagement is very much linked to the EU's development cooperation commitments also in reflection of the 2030 Agenda for Sustainable Development (SDG 9a on resilient infrastructure and SDG 16.4 on combatting all forms of organised crime), as reiterated in the 2015 Council Conclusions on Cyber Diplomacy which, inter alia, encourage the EU and the its Member States to promote "sustainable cyber capacity building, when appropriate, together with international partners, as well as streamlining and prioritising funding, including by making full use of the relevant EU external financial instruments and programmes". More recently the same principles were reiterated in the discourse about mainstreaming digital solutions and technologies in EU development policies [Council Conclusions of 28/11/2016] which recognise that "international cooperation and assistance in cyber capacity building play an essential role in enabling States to secure information and communication technology and their peaceful use", while the Joint Communication on Countering Hybrid Threats [JOIN (2016)18, 06.04.2016] recognises that efforts to strengthen the cyber resilience of third countries can directly increase their abilities to protect their strategic assets and to be ready to respond to potential hybrid attacks.

**Component 2: Small Arms and Light Weapons**

The EU's response to the multifaceted SALW problem is anchored in the EU Strategy to Combat Illicit Accumulation and Trafficking of Small Arms and Light Weapons (SALW) and their Ammunition, adopted in 2005. The strategy sets down three principles underpinning the EU’s action in the field of small arms and light weapons – prevention, cooperation with partners and support to multilateralism. This complements and contributes to the implementation of the UN Programme of Action on the Illicit Trade in Small Arms and Light Weapons and the International Tracing Instrument by combining all the instruments and policies available to the EU for tackling all facets of the firearms issue. Internally, Member States and the Commission, on the basis of Europol's 2013 EU Serious and Organised Crime Threat Assessment, have made the disruption of illicit manufacturing and trafficking in firearms one of the EU's nine law enforcement priorities for 2014-17, while the 2015 EU action plan against illicit trafficking in and use of firearms and explosives [COM(2015) 624 final, 2.12.2015] identified priority actions to tackle this serious challenge.

**Component 3: Falsified Medicine**

The action is in line with the Council of Europe MEDICRIME Convention, which is the first binding legal instrument to criminalise the practice of falsifying medical products and provides a framework for international cooperation on prevention and victim protection. The action also covers the external dimension of the EU Directive 2011/62/EU on Falsified Medicines [OJ L174/74, 1 July 2011] and the Council Conclusions focusing on the role of law enforcement cooperation [3096th Justice and Home Affairs Council meeting, 9 and 10 June 2011]. The increasing importance of this organized crime activity is also reflected in the strategy against falsified medicines developed by UNODC following its new mandate given in 2011 by the UN Commission on Crime Prevention and Criminal Justice.

1.1.2 Stakeholder analysis

**Component 1: Cybercrime**

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

At EU level there are several layers of relevant stakeholders, including 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.

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

**Component 2: Small Arms and Light Weapons**

Key stakeholders will be the competent governmental authorities, including ministries, law enforcement services (police, border authorities), judicial and prosecutorial authorities. Within these organisations, key duty bearers, policy makers and implementers will be identified and engaged by the project.

**Component 3: Falsified Medicine**

The stakeholders involved will be the third country governments and their competent ministries (e.g. Ministry of Health, Trade, Economy, and Customs), border officials, the private sector, civil society, and end-users. The involvement of gender focal points and women associations will also be sought. In addition, the Eastern and Central Africa Centre of Excellence regional secretariat set up by the Commission in Nairobi will also play a coordination role. Synergies will be pursued with International Organizations and other actors implementing similar projects.

1.1.3 Priority areas for support/problem analysis

**Component 1: Cybercrime**

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

The main challenge throughout developing countries clearly is the capacity to apply legislation on cybercrime and electronic evidence in practice. In some States, specialised cybercrime units have been established within law enforcement services but their capacities, in particular with regard to computer forensics, are very limited. This is also true with regard to the cooperation between such units within regions and to their cooperation with cybercrime units in Europe and other regions. In most States, skills of prosecutors and judges to apply legislation and to prosecute and adjudicate cases of cybercrime or involving electronic evidence are close to non-existent. For this reason, most developing countries are not able to engage in international judicial cooperation on cybercrime and electronic evidence. The need for ensuring swifter cross-border access to evidence and information is a key challenge in
light of current and future technological developments. 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.

Most countries are not in a position to prepare and implement comprehensive strategies on cybercrime and cybersecurity that also meet human rights and rule of law requirements and that allow countries to exploit the development potential of ICT. A considerable number of developing countries has adopted legislation on cybercrime (examples include Benin, Botswana, Cameroon, Cote d’Ivoire, Dominica, Dominican Republic, Ghana, India, Kenya, Laos, Mauritius, Nigeria, Senegal, South Africa, Sri Lanka, Tanzania, Thailand, Tonga, Uganda) or is in the process of developing legislation (e.g. Cambodia, Indonesia, Madagascar, Mongolia, Morocco, Pakistan, Paraguay, Vietnam and others). While in some cases, legislation appears to be fully in line with international standards; in others a further strengthening of the legal framework is required, including in view of improving rule of law safeguards.

While the ever increasing reach of the internet and the spread of social media have enabled new means and efforts in addressing violence against women and girls, the same tools are also used to inflict harm on them. Cyber-violence against women and girls is emerging as a global problem with serious implications for societies and economies around the world. Cyber violence against women and girls (cyber-VAWG) is under-reported both in western countries with high internet penetration as well as in the Global South. This emerging trend requires a gender sensitive development of the response to cybercrime, not only at the stage of legislation but also in the investigation, prosecution and adjudication of crimes entailing cyber-VAWG. To this end, the Cybercrime Convention Committee established a new working group on "cyberbullying and other forms of online violence especially against women and children" in November 2016. The first report and recommendations are expected in late 2017, which could be taken up by the proposed action.

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 strong partnerships with third countries and through our cooperation promote the notion of open, free and secure cyberspace, as well as compliance with and ratification of existing substantive and procedural legislative standards and frameworks for international cooperation ("Budapest Convention").

Component 2: Small Arms and Light Weapons

With the financial support of the EU, UNODC’s Global Firearms Programme has supported the strengthening of national and regional firearms control regimes with a view to prevent and combat illicit manufacturing, diversion and trafficking in firearms and ammunition, and enhancing States’ capacities to detect, investigate and prosecute criminal organizations.

---

2 There are six broad categories that encompass forms of cyber-VAWG and fall under different elements of cybercrime or cyber-enabled crimes: hacking, impersonation, surveillance/tracking ("cyber-stalking"), cyber-harassment, use of the internet to lure potential victims into violent situations (ex. trafficking); and malicious distribution (ex. "revenge porn").
engaged in the illicit firearms business and related forms of organised crime. The new action will build on past and on-going activities, providing support in 4 key areas:

- legislative and policy developments;
- implementation support and capacity building in firearm management, record keeping, marking and collection campaigns, to the extent that it is not financed by ISFP-2016-AG-IBA-UNODC (standardized methodology for data collection and analysis to develop knowledge on trends and patterns of firearm trafficking and to foster data and information exchange and cooperation in tracing, and enhance the capacity to collect and analyse crime and firearms related data at national and international level);
- strengthening criminal justice responses for investigation and prosecution
- promotion of effective international cooperation, information exchange and south-south cooperation.

This component 2, shall have a global scope but it is proposes a flexible assistance model, focusing on core countries/sub-regions where the issue of illicit firearms trafficking presents a clear or emerging threat, and where tailored assistance is needed, and with the possibility of reaching out to the broader sub-regions, for more general support (raise awareness to promote accession and implementation of global instruments; promote international cooperation; support data collection and analysis). As such, the following priority regions have been identified:

- In Africa: Maghreb (Algeria, Tunisia, Morocco, where possible, Libya); East Africa (Kenya, Tanzania, Uganda); West Africa (as appropriate to complement ongoing actions); Central Africa (Central African Republic, DRC, Cameroon, and Northern Nigeria). All activities in Africa will be coordinated and organized in close cooperation and with the support of the African Union, with a view to address the SALW problem across Africa, connecting sub-regional efforts with trans-regional, continental and global responses.
- In Latin America: Central America (Guatemala-El Salvador-Honduras) and South America (Bolivia, Colombia, Ecuador, Paraguay).
- In Western Balkans: Albania, Kosovo, Serbia, Bosnia and Herzegovina, Montenegro and the Former Yugoslav Republic of Macedonia.

Component 3: Falsified Medicine

Falsified medicines are a major threat to global public health and safety. While no country is protected against this threat, the impact is particularly acute in the developing world. In developing countries, they have included medicines used to treat life-threatening conditions such as malaria, tuberculosis and HIV/AIDS.

Falsified medicines are manufactured and sold by criminal individuals and organizations, exploiting weak national legislation and enforcement. Criminals often avoid prosecution by bribing corrupt officials or taking advantage of regulatory loopholes - both in the letter and implementation of the law. Even when the legal and regulatory framework is sufficient, regulatory inspectors, customs and border patrol and law enforcement officials are often not adequately trained, equipped or authorized to identify falsified medicines, properly prepare a file for prosecution, or take immediate actions. Moreover, falsified medicines dealers are often treated with non-deterrent penalties, making trafficking in this field a low-risk business.

Actions to eliminate falsified medicines should not, however, undermine access to legitimate and lower-cost generic drugs. As a complex criminal activity involving regulatory offenses
and several economic, social, legal and criminological sectors, falsified medicines require multi-pronged, multi-sectoral solutions.

In Eastern and Central Africa countries, (Uganda Tanzania, Congo, Kenya), governments and private sector are fairly aware of the impact of trafficking of falsified medicines on public health but also in public finances. For instance, the Kenyan Association of Pharmaceutical Industry estimates that counterfeit pharmaceutical products account for approximately $13 billion annually in sales in the country. Moreover, the ineffectiveness of counterfeited pharmaceuticals weakened people's level of confidence in medicines, reviving alternative and "traditional" methods.

The region can therefore be considered overall sensitive to the falsified medicine related issues, and countries are active in improving medicine regulation overall. The Eastern African Community (of which Kenya, Tanzania, Uganda and Rwanda are members) has several initiatives related to Medicines Regulation. Among them is the African Regulatory Harmonization project, launched in 2009 and aiming to serve as a model for continent-wide medicines regulatory. This is important as the Eastern African Community has made strides towards harmonizing registration procedures, a reality that is excellent for medicines access but which will increase the movement of medicines across borders, including falsified medicines.

The regional approach granted by the Centre of Excellence Initiative will ensure the required cooperation among all the countries involved.

2 **RISKS AND ASSUMPTIONS**

<table>
<thead>
<tr>
<th>Risks</th>
<th>Risk level (H/M/L)</th>
<th>Mitigating measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political instability and insecurity in the beneficiary countries that will disrupt the projects activities.</td>
<td>M</td>
<td>Flexibility in projects activities to allow for varying levels of engagement and focus to avoid an overhaul of project implementation.</td>
</tr>
<tr>
<td>Lack of commitment by the beneficiary country authorities to cooperate.</td>
<td>M</td>
<td>Engagement will be pursued with those partners demonstrating clear political will and commitment to change management.</td>
</tr>
<tr>
<td>Corruption within the beneficiary structures.</td>
<td>H</td>
<td>Promotion of national inter-agency teams to mitigate the risk through internal checks and balances. Continuous monitoring and engagement at medium and high political level.</td>
</tr>
<tr>
<td>Frequent government restructuring, lack of clear delineation of duties and responsibilities between relevant agencies and changes to government agenda reducing strategic outlook on addressing migrant smuggling.</td>
<td>L</td>
<td>Risk assessments and strong involvement of implementers will mitigate this risk. In addition, for the selection of priority countries, engagement will be pursued only with those demonstrating clear political will and determination for change management.</td>
</tr>
<tr>
<td>Challenge to conduct needs assessment from both beneficiary and implementer perspective, and not only from one side.</td>
<td>M</td>
<td>Ensure a multi-stakeholder approach with frequent agreement/alignment between beneficiary and implementer/donor</td>
</tr>
<tr>
<td>Lack of willingness to commit to the rule of law and human rights aspects.</td>
<td>M</td>
<td>Development of a human rights risk mitigation project strategy, while closer engagement will be pursued with those partners demonstrating clear political will and determination for change management.</td>
</tr>
<tr>
<td>Weak institutional capacity and/or low political will to cooperate among</td>
<td>M</td>
<td>Through increased awareness, peer pressure for action and other means, this risk will be mitigated.</td>
</tr>
</tbody>
</table>
neighbours remain a constant challenge to effectively cooperate in addressing organised crime.

Lack of gender awareness, gender sensitivity, gender understanding increase existing gender inequality.  
M  Include gender analysis and gender desegregated data. Make sure there is gender balance among beneficiaries of the action.

Lack of synergies between this Action and other relevant capacity building programmes at national and regional level.  
M  Regular coordination with EU HQ services, EU Delegations and engaged EU MS and other donors in countries where the activities take place will be pursued. Coordination with ongoing and future activities undertaken by Eastern African Community and involving its member states should be ensured.

Assumptions

- The Governments of the beneficiary countries are committed to cooperate both at a national and regional level.
- All institutions involved in the Project are committed to the overall objective and purpose of the Action throughout the duration of the Implementation Phase and ready to develop a working cooperation agenda
- The responsiveness, financial and technical capacity of the beneficiary countries will not decline in the forthcoming years.
- Sufficient capacities at national and (sub-)regional levels can be mobilised for participation in the activities.

3  LESSONS LEARNT, COMPLEMENTARITY AND CROSS-CUTTING ISSUES

3.1  Lessons learnt

There are several common lessons learnt from past actions implemented in the framework of IcSP's fighting organised crime priority. Working at a regional and trans-regional level poses significant challenges given the multitude of countries and actors involved, with different levels of capacity and commitment, different regulatory frameworks and priorities, including sometimes inadequate or total lack of national legislation on some of the areas related to the fight against organised crime. It is therefore important to ensure resources are flexible enough to allow for adaption to the different needs and stages of readiness in each partner country/region. It is important to engage with authorities that demonstrate clear political will and provide for an environment ready to embrace such changes. In ensuring ownership, such support would allow capacity building in both policy making and operational levels. A demand-driven approach on the basis of a comprehensive needs assessment is therefore necessary. Projects focusing more on operational cooperation seem to bring results that are more promising; with importance of incorporating human rights safeguards in the design and implementation of such actions. The establishment of long term relationships between relevant EU agencies and counterparts in third countries, e.g. via mentoring, is considered crucial and can strengthen the link with the external aspects of internal security policy.

Challenges include tensions between countries and fragility can hamper regional cooperation and negatively impact the execution of activities. Moreover, capacity shortages and frequent staff rotation in beneficiary institutions and agencies may also limit progress or significant consolidation of results from external assistance actions.

Specifically on cybercrime (Component 1), in light of the experience that the EU and the Council of Europe have gained in the implementation of joint projects against cybercrime within Europe focusing mainly on the Budapest Convention and technical assistance for capacity building, some key lessons can be drawn. A recent results-oriented monitoring of the IcSP-funded Global Action on Cybercrime (GLACY) highlighted several best practices, including the creation on inter-agency national project teams across the criminal justice chain
that foster ownership, ensure alignment with national priorities and help an institutional change process; as well as the 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. Scalability of the support provided is ensured through the development of Train-the-Trainers modules. Moreover, the experience gained within the EU during the past decade, in particular with respect to the development of standardised and scalable training, co-operation and information sharing between specialised cybercrime units and other fields, is shared through the action's partnership with EC3 at Europol and its European Cybercrime Training and Education Group (ECTEG).

In the case of SALW (Component 2), an independent evaluation was concluded in 2016 for all IcSP-funded projects in the area of SALW which were deemed to have made a contribution to the broad SALW policy framework outlined in the 2005 EU Strategy on SALW. The evaluation demonstrated that the EU-funded programmes under IcSP were, by a long shot, the largest and most comprehensive SALW programmes implemented worldwide in recent years, highlighting the central role played by the EU in supporting the worldwide implementation of international agreements on SALW.

Previous support to the UNODC's Global Firearms Programme from IcSP has been evaluated as particularly fit to address the transnational dimension of the problem of illicit manufacturing of and trafficking in firearms by strengthening the capacities of individual countries and sub-regions to develop and put in place comprehensive firearms control regimes, and by enhancing the capacity of criminal justice practitioners. The evaluation highlighted that results are more likely to appear in the long term, with enhanced legal frameworks and cooperation as a result of the direct contacts facilitated between practitioners from West Africa and South America for example. The programme has left an important legacy as an innovative intervention, with a particular added value in the enactment of relevant legislation. In terms of sustainability, the evaluation noted that some activities such as marking, registration and destructions of firearms were seen positively by beneficiaries.

In the area of falsified medicine (Component 3) some lessons learnt can be drawn from the monitoring and results of a previous project implemented under the IcSP. Attention should be given to the other initiatives supported by the EU and other entities to build on their outputs and maximise the use of existing resources. Reinforcing the regional and inter-regional dimension is deemed to be a key factor for the achievement of the objectives of the programme. Strong presence of the implementers and the involvement of local experts have been also recommended.

3.2 Complementarity, synergy and donor coordination

A significant number of EU programmes are directly or indirectly relevant to capacity-building and law enforcement activities for fighting organised crime. Many of the actions under the current proposal build on past and on-going activities and will be complementary to other EU initiatives at national or regional level, EU member states activities, and actions from international organisations or donors. An overview of donor coordination (within the EU and with third actors) on each specific project within this broader area of support by the IcSP will be provided in the relevant project descriptions of each action.

Component 1: Cybercrime

There are strong complementarities and synergies with other EU-funded actions, particularly in the Western Balkans and Neighbourhood (namely: iPROCEEDS, Cyber@EaP, and CyberSouth under the remit of the European Commission's Directorate-General for
Neighbourhood and Enlargement Negotiations) 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, particular attention will be placed to foster cooperation with IcSP's project "Cyber Resilience for Development", as well as with future projects under geographical financial envelopes, such as the Pan-African Programme ("Accessing the Digital Dividend in Africa") and regional ACP programmes. At the EU level the inter-service group on cyber issues allows for a framework of such internal coordination. More generally, coordination with the EU Member States is ensured in the relevant Council Working Group, i.e. the Horizontal Working Party on Cyber Issues (HWP Cyber). Coordination in the different strategy frameworks is combined with political and technical dialogue and exchange of information with EU Member States. Moreover, the EU is a founding member of the Global Forum on Cyber Expertise (GFCE) launched by the Netherlands in 2015 and its participation to the Forum will allow for exchange of information avoid overlaps and even identify potential synergies with other donors. In addition, coordination takes place in the context of the respective EU Cyber Dialogues most notably with the United States, Japan, and Republic of Korea, as well as with exchanges with like-minded countries financing cyber capacity building such as Australia and Canada.

Coordination will be sought with international organisations and agencies on the ground such as the UNODC, the International Telecommunication Union (ITU), the World Bank, as well as with a number of regional organisations which are involved in measures on cybercrime and cybersecurity such as the African Union and the Regional Economic Communities in Africa, the Arab League, the Association of Southeast Asian Nations (ASEAN), the Organisation of American States (OAS), the Commonwealth of Nations and the Commonwealth Telecommunications Organisation (CTO), and the Secretariat of the Pacific Community. An overview of donor coordination on the specific Component within this broader area of support by the IcSP shall be provided in the detailed project description.

Component 2: Small Arms and Light Weapons

The Commission already finances some of UNODC's work on global data collection and analysis on firearms trafficking and fostering cooperation and information sharing in particular among countries along major trafficking routes to and from the EU. It is intended to maintain close cooperation and seek synergies with other programmes and organisations active in this field.

The project aims at supporting data collection and analysis on firearms trafficking at national, regional and global levels with a view to monitoring and mapping illicit firearms trafficking flows, fostering effective international cooperation in tracing and information sharing, and combating illicit trafficking and related crimes. The project seeks to establish a regular collection mechanism of statistical data and information on firearms seizures and trafficking based on an internationally agreed methodology and best practices (incl. efforts lead by INTERPOL and EUROPOL) and on previous data collection efforts by UNODC, such as the 2015 Firearms Study. The project also contributes to collect and produce statistical data to monitor target 16.4 of the 2030 Agenda for Sustainable Development, which calls for a reduction of illicit arms flows and combating all forms of organized crime. The actual content of component 2 of the Action will include a clear delineation between it and the work on

3 ISFP-2016-AG-IBA-UNODC
global data collection.

In Africa, the project shall work in cooperation with the Africa Union. Moreover, the project activities are aligned with the AU Strategy on the Control of Illicit Proliferation, Circulation and Trafficking of SALW as well as its implementation action plan. In addition, the project will seek cooperation with relevant sub-regional organizations such as the Economic Community of West African States (ECOWAS), the Economic Community of Central African States (ECCAS) and the Regional Centre on Small Arms in the Great Lakes Region, the Horn of Africa and Bordering States (RECSA) as well as with the future IGAD Peace and Stability Programme and also with the East African Community. In Latin America, the project will work in synergy with MERCOSUR’s (Southern Common Market) Secretariat and its Working Group on Firearms and Ammunition, with UNASUR’s (Union of South American States) Council on Safety, Justice, and Coordination of Action Against Transnational Organized Crime (DOT); with the Consultative Committee of the Inter-American Convention against the Illicit Manufacturing of and Trafficking in Firearms, Explosives, Ammunition and Other Related Materials (CIFTA); and with the Central American Programme on Small Arms and Light Weapons Control (CASAC). In South East Europe, the project will seek synergies with Organization for Security and Co-operation in Europe (OSCE) and the South Eastern and Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons (SEESAC).

In order to reinforce the regional dimension of the project and enlarge its scope, the project will also seek to join forces and establish synergies and partnerships with other organizations with a view of promoting joint implementation of specific project activities, and thus leverage existing resources, including the Counter-Terrorism Committee Executive Directorate (CTED), UN-HABITAT and the UN Office for Disarmament Affairs (UNODA), the UN Department of Peacekeeping Operations (DPKO) and with other currently ongoing actions as i-Arms and i-Trace projects.

Component 3: Falsified Medicine

Many of the actions under the current proposal build on past and on-going activities and will be complementary to other initiatives at national or regional level carried out by institutions like WHO AFRO, International Federation of Pharmaceutical Manufacturers & Associations (IFPMA) Africa Regulatory Network (ARN) and others which have done considerable work towards sensitizing population and stake holders and provide training and capacity building to prevent proliferation and use of falsified medicines. UNICRI has a focused programme against falsified medicines in the continent. INTERPOL and WHO (International Medical Products Anti-Counterfeiting Taskforce - IMPACT) have joined hands with regional partners to conduct successful operations targeted to intercept and seize large amounts of counterfeit/falsified medicines in various parts of Africa.

3.3 Cross-cutting issues

Actions in the area of fighting against organised crime cut across many different sectors and issues, ranging from human rights, gender equality, good governance and migration to criminal law and border management. The activities of the Components foreseen in this Action Document will be carried out in conformity with the principles of rule of law, good governance and internationally recognised human rights standards as well as taking into account further victim-related and gender issues.

Strengthening domestic security and prosecution capacity, whilst strongly integrating human rights, may help mitigate the risk of “cultures of impunity” becoming entrenched. In this light,
all assistance and training aspects must include precautionary measures to assure international human rights standards and norms are met. To ensure compliance of the proposed action with the obligations stipulated in Article 10 ("Human rights") of Regulation (EU) No 230/2014, a clear human rights perspective should be incorporated throughout the different stages of the project cycle (project design/formulation; monitoring of implementation; evaluation) on the basis of the operational guidance developed to this end by the European Commission (https://ec.europa.eu/europeaid/operational-human-rights-guidance-eu-external-cooperation-actions-addressing-terrorism-organised_en). Any potential flow-on risk on the respect of human rights should be constantly monitored and mitigating measures need to be foreseen.

Considering that the proposed action document is aimed at enhancing the capacities of partner countries to prevent and fight various manifestation of organised crime, the integration of a gender sensitive perspective throughout the project cycle and in accordance to the specificities of the crimes at hand (cybercrime, trafficking of SALW and falsified medicine) 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) supporting the legislative reforms that are gender-sensitive; (iii) promoting the balanced representation of women in the security sector; and (iv) fostering the increased participation of women in all operational activities related to the actions.

Involvement of civil society is also key for a holistic approach in addressing the organised crime phenomenon, while in providing technical assistance and capacity building, the issue of corruption should be carefully considered. To mitigate the challenges posed by endemic corruption, anti-corruption actions will be comprehensively integrated into all parts of the training and awareness raising activities.

In addition, throughout the implementation of the different Components, concerted efforts need to be made to make sure that equal access to the foreseen activities is granted to women officials/participants and that they are included in all the training, mentoring and other operational activities, as a means to increase effectiveness of the interventions. In a similar vein, beneficiary countries will be advised on their recruitment policies for staff and on development of standard operating procedures in line with gender equality principles and guidelines as to fair and non-discriminatory treatment.

Specifically on cybercrime (Component 1), it is relevant to highlight the cross-cutting aspects noted in the 2015 EU Council Conclusions on Cyber Diplomacy that reaffirm the need to “foster open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures”.

In the area of falsified medicine (Component 3) particular attention will be paid to ensure a holistic approach in linking support measures with broader national health initiatives.

4 DESCRIPTION OF THE ACTION

4.1 Objectives/results

The overall objective of Components 1, 2, and 3, in accordance with the IcSP Multi Annual Indicative programme 2014-17, is to prevent and fight organised crime, including the fight against cybercrime and the illicit trafficking in small arms and light weapons and falsified medicine.
This programme is relevant for the Agenda 2030. It contributes primarily to the progressive achievement of SDG Goal 16, but also promotes progress towards Goals 3 and 5. This does not imply a commitment by the countries benefiting from this programme.

**Component 1: Cybercrime**

The specific objective is 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.

The expected results/outputs are:

- **Output 1:** Increased awareness of decision makers on cybercrime threats and reviewed national criminal law frameworks and policies, in line with the Budapest Convention on Cybercrime, including rule of law and human rights safeguards.

- **Output 2:** Strengthened due-process compliant capacities and operational skills of police authorities to investigate cases of cybercrime and electronic evidence and engage in effective inter-agency, public-private and international cooperation.

- **Output 3:** Enhanced capacities of criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence in compliance with international human rights law.

- **Output 4:** Improved international co-operation against cybercrime.

By embedding capacity building on cybercrime and electronic evidence within the context of broader criminal justice reform, this Component is not only aimed at strengthening the rule of law and human rights in cyberspace and at enhancing cybersecurity but also at contributing to human development, poverty reduction and democratic governance.

**Component 2: Small Arms and Light Weapons**

The specific objective is to prevent and counter illicit manufacturing and trafficking in firearms, and their links to transnational organized and other serious crimes, and promoting the ratification and implementation of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime (UNTOC).

The expected results/outputs are:

- **Output 1:** Increased awareness of the firearms issue and its international responses, and adequate policy and legislative frameworks in place, in line with relevant international and regional instruments.

- **Output 2:** Increased capacities of countries and sub-regions to implement effective firearms control regimes in line with the Firearms Protocol and other relevant instruments, and to prevent, investigate and prosecute firearms trafficking and related offences through effective national response and international law enforcement and judicial cooperation.\(^4\)

---

\(^4\) Beyond the standardized methodology for international data collection and analysis to develop knowledge on trends and patterns of firearm trafficking and to foster data and information exchange and cooperation in tracing addressed under project ISFP-2016-AG-IBA-UNODC.
Output 3: Improved effective international cooperation and sharing of information and good practices among firearms and organized crime practitioners on the prevention and combat of firearms trafficking and related crimes, through regular contacts and use of specialized cooperation networks and platforms and taking advantage of existing initiatives.\(^5\)

Output 4: Improved capacity to monitor, analyse and identify synergies for firearms legislation and case-law with and amongst other forms of transnational organised crime, including cybercrime, money laundering, illicit drug trafficking and smuggling of migrants.\(^6\)

Component 3: Falsified Medicine

The specific objective is to empower and added value to the systems which are already in place for combatting the trafficking, identification and effective management of falsified medicines and medicinal products in Eastern and Central Africa region.

The expected results/outputs are:

- **Output 1**: Increased public and stakeholder awareness on falsified medicines and medicinal products risks
- **Output 2**: Improved legal framework and law enforcement for combatting falsified medicines and medicinal products illicit trafficking.
- **Output 3**: Enhanced technical capabilities to address the falsified medicines problem.
- **Output 4**: Improved interagency collaboration and cooperation among departments and agencies dealing with the fight against falsified medicines in each country.
- **Output 5**: Enhancement of international cooperation to tackle the trafficking, identification and effective management of falsified medicines in Eastern and Central Africa region.

4.2 Main activities

Component 1: Cybercrime

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

*Under Output 1*: (i) Review of domestic legislation; (ii) Engagement with national decision-makers and legislators; (iii) Support to domestic law drafting working groups; (iv) Training activities on conditions and safeguards as well as data protection; (v) National and regional meetings for awareness raising, strategic engagement, and sharing of good practices.

*Under Output 2*: (i) Review of institutional capacities for cybercrime investigations as well as computer forensics; (ii) Advice, sharing experience and study visits on the establishment or strengthening of specialised services; (iii) Support to law enforcement training (including training of trainers) and incorporation of the courses in the curricula of the training academies; (iv) Support to standard operating procedures for the use of electronic evidence; (v) Promotion of interagency co-operation amongst cybercrime units, financial investigators and financial intelligence units in the search, seizure and confiscation of online crime

\(^5\) Idem.

\(^6\) Idem.
proceeds; (vi) Promotion of public/private co-operation, in particular on law enforcement and service provider co-operation on access to electronic evidence.

Under Output 3: (i) Review of institutional capacities for cybercrime prosecutions as well as computer forensics; (ii) Advice, sharing experience and study visits on the establishment or strengthening of specialised services; (iii) Support to judicial training (including training of trainers) and incorporation of the courses in the curricula of the training academies; (iv) Support to standard operating procedures for the admissibility of electronic evidence.

Under Output 4: (i) Review of rules, procedures and institutional capacities for international cooperation on cybercrime and electronic evidence; (ii) Training and advice for 24/7 points of contact; (iii) Support to participation in international initiatives.

Component 2: Small Arms and Light Weapons

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

Under Output 1: (i) Awareness-raising activities and engagement with decision makers on the issue of firearms and its international responses, not addressed under project ISFP-2016-AG-IBA-UNODC; (ii) Support for the normative development of governing bodies on firearms, beyond the designation of national focal points to facilitate data collection and analysis under project ISFP-2016-AG-IBA-UNODC; (iii) Legislative assessments, gap analysis and support for the adoption of national / regional action plans for the implementation of UNTOC's Firearms Protocol; (iv) Provision of tailored legislative advice and legal drafting support.

Under Output 2: (i) Development of legislative and technical assistance tools on firearms; (ii) Specialised assistance and expert advice for the implementation of relevant firearms control measures to reduce proliferation, and to prevent their illicit trafficking (in particular in the area of marking, recording, confiscation and collection-storage; except if already covered by the technical assistance provided under project ISFP-2016-AG-IBA-UNODC); (iii) Training for firearms control authorities and criminal justice practitioners (law enforcement, investigation and prosecution services, customs, police and intelligence agencies) to enable them implement the technical requirements of the Firearms Protocol and to investigate and prosecute transnational trafficking in firearms cases and engage in effective international cooperation in judicial and law enforcement matters; (iv) Support to creation of channels of formal and informal communication, joint investigations and common case work practice.

Under Output 3: (i) Establishment of communities of practitioners on Firearms and Organised Crime Experts to support direct cooperation and coordination, exchange of good practices and experiences in firearms control and in the investigation and prosecution of firearms and organised crime related cases; (ii) Development of tools to facilitate the work of the community of practitioners.

Under Output 4: (i) Legal research on legislation and case law for firearms and other forms of transnational organised crime, including cybercrime, money laundering, illicit drug trafficking and smuggling of migrants; (ii) identification of shortcomings, analysis of challenges and proposal of common approaches in addressing the problems.

Component 3: Falsified Medicine

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

Under Output 1: (i) Training workshops to the key stakeholders involved in law-making; (ii) Technical seminars for law enforcement, customs, border control; (neighbouring country joint seminars should be envisaged for agents involved in cross-border activities; (iii) Technical
seminars for public and private sector health professionals (pharmacists, doctors, health students); (iv) Awareness raising events for general public.

Under Output 2: (i) Development of a model of minimum legislation and respective regulations to cover all critical aspects of production, import and export, transport and distribution, and point of sale; (ii) Identification of gaps and weak points in the existing legislation applied to falsified medicines for each partner country; (iii) Conference(s) held at a (sub-)regional level involving all partner countries on the promotion of accession to and implementation of the MEDICRIME Convention; (iv) Drafting and publication of a handbook providing quick normative references to serve as a reference document for the lawmakers.

Under Output 3: (i) Inventory of the chemical and pharmaceutical analysis laboratories operating in the Eastern and Central Africa region; (ii) Developing of tailored training curricula and compilation of best practices to be used during the train the trainer sessions; (iii) Joint training events (minimum 3 events per country) on evidence-base and intelligence-led investigative techniques; (iv) Train the trainer sessions at national quality control laboratories; (v) Training sessions for judges and prosecutors.

Under Output 4: (i) Provision of guidelines to identify and clearly define responsibilities amongst national services; (ii) Definition of a procedure of improved communication and coordination between various sectors involved (ministries, authorities, law enforcement, customs and border control); (iii) National workshops in each beneficiary country, involving mid-management agency representatives.

Under Output 5: (i) Organisation of information exchange meetings with the contact points/project leaders of projects running or completed in the region by other donors; (ii) Organisation of one regional conference, to include discussion of cross-border and trans-regional cooperation with relevant regional and international organisations.

4.3 Intervention logic

Component 1: Cybercrime

The rationale in the definition of the above-described result areas is based on the fact that these four dimensions (policy and legal frameworks, operational capacities of law enforcement and judiciary – i.e. across the criminal justice chain– and cooperation at inter-agency, public-private and international level) are the tenet of any basic conceptual framework in addressing cybercrime. A key element of engagement with the selected third countries includes the establishment of national coordination project teams (see section 5.6), involving relevant authorities and institutions, as well as partnering with national training academies wherever applicable in order to incorporate the training courses in their curricula as a basic element of sustainability.

Given that the available resources under the external financing possibilities for third countries are limited, there is a need to prioritise any future engagement. In order to identify priority countries, in line with the IcSP Regulation's requirement for a transregional focus and its stipulation that “Priority shall be given to trans-regional cooperation involving two or more third countries which have demonstrated a clear political will to address the problems arising” (Article 5a.i), a set of criteria has been developed on the basis of inter-service coordination between European Commission (Directorate General for International Cooperation and Development and Directorate General for Migration and Home Affairs), the European External Action Service and EC3 at Europol. These include: (i) Minimum existing consistent cybercrime legislation; (ii) Political commitment to engage (for example demonstrated through signature or requested accession to the Budapest Convention) with a
Rule of Law ambition; (iii) Strategic role in the (sub)region with the potential to act as a champion/influencer/regional hub and have a ripple effect; (iv) Readiness for international cooperation, including eagerness to engage at a South-South/Triangular cooperation context; (v) The level and nature of cybercrime, and in what extent they host criminal infrastructure (amount of attacks and prosecutions, number of bad hosting companies); (vi) High impact potential; (vii) Potential policy influence in line with EU policy priorities; (viii) No overlap with other donors/possible synergies.

The tailored approach based on a continuous assessment of developments globally will be translated into the identification of (i) hub countries that meet the above criteria and have a sufficient level of maturity to share experience with countries of their respective (sub-) regions, while they may receive support in any issue of relevance across all Result areas; (ii) priority countries that meet all or most of the above criteria but do not have sufficient capacities to serve as hubs, but will enjoy the full range of support across all Result areas; (iii) associate countries that either receive support in the preparation of cybercrime legislation (any country may request such assistance) or engage with the project in regional activities primarily with a view to be introduced to a broader cyber community of practice, or foster existing ties and serve as inspiration for national policy/legal reforms. Some of these countries may become priority countries later on.

**Component 2: Small Arms and Light Weapons**

In order to identify priority countries from the regions identified already under the problem analysis a set of criteria will be developed during the inception phase, in line with the IcSP Regulation's requirement for a transregional focus and its stipulation that “Priority shall be given to trans-regional cooperation involving two or more third countries which have demonstrated a clear political will to address the problems arising” (Article 5a.i). This component will have a flexible, phased approach with multi-level engagement: the priority countries shall encourage changes in and between their regions and start cooperation gradually around good practices. The gradual adoption of compatible methods and indicators by the different countries is aimed to foster progressive (trans-)regional cooperation. See Appendix for details on the intervention logic.

**Component 3: Falsified Medicine**

This component will be implemented through the CBRN Centres of Excellence initiative, in particular involving the Regional Secretariat based in Nairobi and covering the Eastern and Central Africa (ECA) region. The Centres of Excellence, set up in 2010, aims to establish a framework for internal coordination and regional cooperation between third countries and to capacitate them. It targets all risks whether of a criminal, natural or accidental origin. It also covers the whole spectrum of intervention from prevention, through preparedness to post-crisis response. The threat caused by the falsified medicines has a transnational nature and requires the sharing of best practices and the pooling of resources, the Initiative grants a strong regional dimension. In addition it follows a bottom-up approach implying piloting at country level so as to get as close as possible to the latter's needs and ensuring the prior endorsement of the objectives and activities proposed by the project. At an operational level the participating countries benefit from several regional capacity-building projects that they identify and develop together during regional round tables. The combating against falsified medicines has been identified by the ECA region as one of their priorities.

Eleven countries are part of the Eastern and Central Africa Centres of Excellence and each one has nominated National Focal Point (NFP) and established a National Team (NT)
involving representatives from each relevant ministry (i.e. Ministries of Health, Trade, Economy, and Customs) and competent national agencies.

5 IMPLEMENTATION

5.1 Financing agreement

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

5.2 Indicative implementation period

The indicative operational implementation period of this action, during which the activities described in section 4.1 will be carried out and the corresponding contracts and agreements implemented, is 72 months (48 of implementation of the activities) from the date of adoption by the Commission of this Action Document.

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

5.3 Implementation modalities

5.3.1 Indirect management with an international organisation

Component 1 may be implemented in indirect management with the Council of Europe in accordance with Article 58(1)(c) of Regulation (EU, Euratom) No 966/2012. This implementation entails strengthening the capacities of the third countries to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international co-operation in this area.

This implementation is justified because the Council of Europe has a unique expertise in the domains the proposed action intends to address and falls within the call of the 2013 EU Cyber Security Strategy to engage with international partners and organisations to support global capacity-building. Having more than 10 years of experience in cybercrime capacity building efforts, as well as being the guardian of the Budapest Convention on Cybercrime, the Council of Europe has the required know-how and capacity to undertake such initiatives in third countries. The Council of Europe would implement the project in partnership with INTERPOL, the EC3 at Europol, as well as EU Member States (currently in the "Global Action on Cybercrime extended – GLACY+" the project partners include the Estonian Ministry of Justice, the French Ministry of Interior, The Romanian Ministry of Justice, the National Police and the Chief Prosecutor's Office, and the UK National Crime Agency). The entrusted entity would carry out the following budget-implementation tasks: carrying out the necessary procurement and grant award procedures and awarding, signing and executing the resulting procurement and grant contracts (in line with the rules foreseen in the Special Conditions) for works, services, supplies and other benefits to be provided to the beneficiary countries.

Component 2 may be implemented in indirect management with the United Nations Office on Drugs and Crime (UNODC) in accordance with Article 58(1)(c) of Regulation (EU, Euratom) No 966/2012. This implementation entails technical assistance to be provided to third countries towards the ratification and effective implementation of the Protocol against the
Illicit Manufacturing of and Trafficking in Firearms, their parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organised Crime (UNTOC) of 2000. This implementation is justified because UNODC is the guardian of UNTOC and has a global mandate to support countries to ratify and implement its Firearms Protocol. Moreover, in 2014 the UN General Assembly requested UNODC to help to establish international networks and partnerships among Member States in the area of international cooperation in criminal matters [UN GA Resolution 69/193].

The entrusted entity would carry out the following budget-implementation tasks: carrying out the necessary procurement and grant award procedures and awarding, signing and executing the resulting procurement and grant contracts (in line with the rules foreseen in the Special Conditions) for works, services, supplies and other benefits to be provided to the beneficiary countries.

The entrusted international organisation, namely UNODC, is currently undergoing the ex-ante assessment in accordance with Article 61(1) of Regulation (EU, Euratom) No 966/2012. The Commission’s authorising officer responsible deems that, based on the compliance with the ex-ante assessment based on Regulation (EU, Euratom) No 1605/2002 and long-lasting problem-free cooperation, the international organisation can be entrusted with budget-implementation tasks under indirect management. UNODC is dependent of the UN Secretariat, as confirmed during the 5th FAFA working group in April 2008, and it is covered by the four pillars analysis performed for the UN Secretariat.

The selection of the abovementioned international organisations for Component 1 and 2 (Council of Europe and UNODC) is in line with the EU commitment to promote a "rules-based global order with multilateralism as its key principle" described in the EU's 2016 Global Strategy, and with the approach promoted in international fora like the Global Partnership for Effective Development Co-operation.

5.3.2. Procurement (direct management)

**Component 3:**

<table>
<thead>
<tr>
<th>Subject in generic terms, if possible</th>
<th>Type (works, supplies, services)</th>
<th>Indicative number of contracts</th>
<th>Indicative trimester of launch of the procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDISAFE - Combating falsified medicines in Eastern and Central Africa</td>
<td>Services</td>
<td>1</td>
<td>4th</td>
</tr>
</tbody>
</table>

5.4 Scope of geographical eligibility for procurement and grants

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

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

---

7 Final Report International Organisations – completion of compliance analysis with internationally accepted standards, 7 March 2008
5.5 Indicative budget

<table>
<thead>
<tr>
<th>Component</th>
<th>EU contribution (amount in EUR)</th>
<th>Indicative third party contribution, in currency identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1. Comp 1-Indirect management with CoE</td>
<td>3,000,000</td>
<td>300,000</td>
</tr>
<tr>
<td>5.3.1. Comp 2-Indirect management with UNODC</td>
<td>3,250,000</td>
<td>N.A</td>
</tr>
<tr>
<td>5.3.2. Comp 3-Procurement / direct management</td>
<td>4,000,000</td>
<td>N.A</td>
</tr>
<tr>
<td>5.8. Evaluation, 5.10 - Audit</td>
<td>will be covered by another decision</td>
<td>N.A.</td>
</tr>
<tr>
<td>5.10. Communication and visibility</td>
<td>It will be included under the individual contracts of the components</td>
<td>N.A.</td>
</tr>
<tr>
<td>Contingencies</td>
<td>0</td>
<td>N.A</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>10,250,000</strong></td>
<td><strong>300,000</strong></td>
</tr>
</tbody>
</table>

5.6 Organisational set-up and responsibilities

**Component 1: Cybercrime**

The implementation of this Action will be coordinated and led by the Council of Europe. An appropriate management structure will be established to ensure the coherence of the project. Activities under all result areas will commence with an assessment of capabilities and conclude with an assessment of progress made. The project 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.

Each priority country is to appoint a *project team* consisting of representatives of the main counterpart institutions of the project. Typically this would include: (i) the Ministry of Justice; (ii) the Office of the Prosecutor General (or a prosecution department specialised in high-tech crime); (iii) a cybercrime unit or the Ministry of Interior; (iv) the 24/7 cybercrime point of contact (if not a member of a cybercrime unit or prosecution department); (v) a judicial training institution; (vi) a law enforcement training institution. These representatives will be responsible for liaising between the Council of Europe's Project Management Unit and domestic authorities for the purposes of the planning and implementation of activities.

Moreover, in order to guarantee the global strategic orientation of the programme, the Contracting Authority together with the implementing partner will establish and co-chair a *Steering Committee.* The responsibilities of the Steering Committee will be: (i) To assess the effectiveness of the project strategy; (ii) To monitor progress made in project implementation and agree on corrective actions or measures to be taken to address emerging needs; (iii) To approve the work plans of the project; (iv) To approve ad-hoc support to a specific country; (v) To review progress reports and other documentation; (vi) To ensure the participation of all relevant stakeholders in project activities; (vii) To promote synergies with actions of bilateral and regional cooperation of the EU and its Member States and coordination with the programmes and projects financed by other donors.

The responsibilities of the implementing partner will include, *inter alia:*

In *relation to the inception phase of the Component:* (i) Undertaking a comprehensive needs-assessment and a stakeholder mapping of the beneficiary countries; (ii) Defining a working plan of activities jointly with the beneficiary institutions; (iii) Identifying the most appropriate bodies/experts/institutions for the transfer of their know-how; (iv) Designing a human rights risk mitigation strategy; (v) Formulating the communication and visibility strategy.
In relation to the implementation phase of the Component: (i) Undertaking the tasks of each activity by mobilising the appropriate and necessary expertise and promoting EU best practice; (ii) Organising events of strategic dimension at national, sub-regional, regional and international level; (iii) Setting up a system of indicators in order to follow up the activities and measure the results; (iv) Reinforcing the collaborative links of the beneficiary countries' relative institutions/bodies amongst themselves and with their counterparts in the EU; (v) Promoting the dissemination of good practices and results of the project; (vi) Ensuring operational coordination with other implementing agencies on the ground.

Component 2: Small Arms and Light Weapons

The implementation of this Action will be coordinated and led by the UNODC in close collaboration with regional or other organisations as AU for the part concerning Africa. Activities under all result areas will commence with an assessment of capabilities and conclude with an assessment of progress made.

In order to guarantee the global strategic orientation of the programme, the Contracting Authority together with the implementing partner will establish and co-chair a Steering Committee. The responsibilities of the Steering Committee will be: (i) To assess the effectiveness of the project strategy; (ii) To monitor progress made in project implementation and agree on corrective actions or measures to be taken to address emerging needs; (iii) To approve the work plans of the project; (iv) To review progress reports and other documentation; (v) To ensure the participation of all relevant stakeholders in project activities; (vi) To promote synergies with actions of bilateral and regional cooperation of the EU and its Member States and coordination with the programmes and projects financed by other donors.

Component 3: Falsified Medicine

This Component will be implemented in direct management through a service contract.

An appropriate management structure will be established to ensure the coherence of the project. The steering of the project will be ensured by a committee which is responsible for identifying priorities, guiding and advising on technical issues, and facilitating the coordination and communication among the participants. The Steering Committee will be composed by the European Commission representatives, the implementing partner representatives and representatives from the Centre of Excellence region whom will be invited on an ad hoc basis.

5.7 Performance monitoring and reporting

The day-to-day technical and financial monitoring of the implementation of these actions defined under Component 1, 2, 3, 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. Particular attention should be given from the outset to the logframe matrix which should be updated at the start of the implementation to include baseline data and corresponding indicators at a project global level and also priority country level with disaggregated data by gender. The reporting shall be laid out in such a way as to allow monitoring of the means envisaged and employed and of the
budget details for the action. The structure of the Monitoring and Evaluation system of each Component shall be elaborated on the basis of these parameters prior to the start of the implementation with clear indication of the reporting responsibilities and adequate allocation of human and financial resources to follow up. The final report, narrative and financial, will cover the entire period of the action implementation.

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

5.8 Evaluation

Having regard to the importance of the action, a final evaluation may be carried out for all components of this action via independent consultants.

For Components 1 and 3, having regard to their nature, a mid-term evaluation may also be carried out for each of them via independent consultants. They may be carried out for accountability and learning purposes at various levels (including for policy revision), taking into account in particular the fact that Component 1 refers to the only programme in the fight against cybercrime of this scale to date globally and has defined the EU's approach to capacity building in countering cybercrime; while for Component 3 the lessons drawn could allow the mirroring of the action in another region particularly in the context of the EU CBRN Centres of Excellence initiative.

5.9 Audit

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

The financing of the audit shall be covered by another measure constituting a financing decision.

5.10 Communication and visibility

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

This action shall contain communication and visibility measures which shall be based on a specific Communication and Visibility Plan of the Action, to be elaborated at the start of implementation and supported with the budget indicated in section 5.6 above.

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

The Communication and Visibility Manual for European Union External Action shall be used to establish the Communication and Visibility Plan of the Action and the appropriate contractual obligations.
APPENDIX - INDICATIVE LOGFRAME MATRIX (FOR PROJECT MODALITY)

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

<table>
<thead>
<tr>
<th>Results chain</th>
<th>Indicators</th>
<th>Baselines (incl. reference year)</th>
<th>Targets (incl. reference year)</th>
<th>Sources and means of verification</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall objective: Impact</td>
<td>To prevent and fight organised crime, including the fight against cybercrime and the illicit trafficking in small arms and light weapons and falsified medicine.</td>
<td>C1/C2/C3. Number of countries that adopt and implement constitutional, statutory and/or policy measures for addressing organised crime in relation to cybercrime, small arms/light weapons and falsified medicine (on the basis of SDG Indicator 16.10.2) C2. Proportion of seized small arms and light weapons that are recorded and traced, in accordance with international standards and legal instruments (SDG Indicator 16.4.2)</td>
<td>To be determined by the implementing partners in the preparatory phase, reflecting on the selected third countries' state of play (2018)</td>
<td>National progress reports on SDG Target 16a</td>
<td>Target countries will ensure sustainability and durability to the action by making available the necessary human, financial, and material resources</td>
</tr>
<tr>
<td>Specific objective(s): Outcome(s)</td>
<td>C1. Strengthened 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.</td>
<td>Number of countries signing the Budapest Convention or applying legislation in line with the Budapest Convention</td>
<td>To be determined by the implementing partner in the preparatory phase (depending on the priority countries)</td>
<td>To be determined by the implementing partner in the preparatory phase (depending on the priority countries)</td>
<td>Council of Europe Treaty Office (Budapest Convention) CoE Assessments and progress reviews carried out under the project.</td>
</tr>
</tbody>
</table>

When it is not possible to determine the outputs of an action at formulation stage, intermediary outcomes should be presented and the outputs defined during inception of the overall programme and its components. The indicative logframe matrix will evolve during the lifetime of the action: new lines will be added for including the activities as well as new columns for intermediary targets (milestones) for the output and outcome indicators whenever it is relevant for monitoring and reporting purposes. Note also that indicators should be disaggregated by sex whenever relevant.
### Outputs

<table>
<thead>
<tr>
<th>C2. Prevention of counter illicit manufacturing and trafficking in firearms, and their links to transnational organized and other serious crimes, and promoting the ratification and implementation of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime (UNTOC).</th>
<th>Number of countries complying with international standards on UNOTC Convention and its Protocols (as assessed by UNODC)</th>
<th>To be determined by the implementing partner in the preparatory phase</th>
<th>UNODC Assessments and progress reviews carried out under the project.</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3. Empowered systems for combatting the trafficking, identification and effective management of falsified medicines in Eastern and Central Africa region.</td>
<td>Increased compliance with international laws and regulations for combating the trafficking, identification and effective management of falsified medicines</td>
<td>To be determined by the implementing partners in the preparatory phase</td>
<td>Assessments and progress reviews carried out under the project.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C1.1. Increased awareness of decision makers on cybercrime threats and reviewed national criminal law frameworks and policies, in line with the Budapest Convention on Cybercrime, including rule of law and human rights safeguards</th>
<th>C1.1.1. Number of draft laws or amendments in line with the Budapest Convention C1.1.2. Number of cybercrime strategies and policies developed/amended in target countries including interagency cooperation and international cooperation.</th>
<th>To be determined by the implementing partner in the preparatory phase</th>
<th>To be determined by the implementing partner in the preparatory phase</th>
</tr>
</thead>
</table>
| C1.2. Strengthened due-process compliant capacities and operational skills of police authorities to investigate cases of cybercrime and electronic evidence and engage in | C1.2.1. Number of countries where cybercrime modules and good practice guides are incorporated in police training academies and competent | C1.1.1. National legislation (official journal) C1.1.2. National strategies (official journal); Project update reports C1.2.1/2/3 Project update reports; National government reports, including | Good cooperation amongst Ministries and Agencies.
Minimum existing trust for good cooperation amongst countries. Ability of the implementing partners to mobilise timely the right expertise for the roll out of activities. |
<table>
<thead>
<tr>
<th>Effective inter-agency, public-private and international cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1.3. Enhanced capacities of criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence in compliance with international human rights law</td>
</tr>
<tr>
<td>C1.4. Improved international co-operation against cybercrime</td>
</tr>
<tr>
<td>C2.1. Increased awareness of the firearms issue and its international responses, and adequate policy and legislative frameworks in place, in line with relevant international and regional instruments</td>
</tr>
<tr>
<td>C2.2. Increased capacities of countries and sub-regions to implement effective firearms control regimes in line with the Firearms Protocol and other relevant instruments, and to prevent, investigate and prosecute firearms trafficking and related offences through</td>
</tr>
<tr>
<td>C1.2. Number of (domestic and international) investigations on cybercrime carried out by cybercrime units in the target countries.</td>
</tr>
<tr>
<td>C1.2.3. Number of requests for data sent to / and replies received from service providers by criminal justice authorities.</td>
</tr>
<tr>
<td>C1.3.1. Number of countries where cybercrime modules and good practice guides are incorporated in judicial training academies.</td>
</tr>
<tr>
<td>C1.3.2. Number of domestic and international prosecutions and cases adjudicated on cybercrime in priority countries</td>
</tr>
<tr>
<td>C1.4. Number of international police-to-police requests.</td>
</tr>
<tr>
<td>C1.4. Number of requests handled by national 24/7 points of contact.</td>
</tr>
<tr>
<td>C2.1 Number of training courses developed and delivered by UNODC on SALW policy and legislation.</td>
</tr>
<tr>
<td>To be determined by the implementing partner in the preparatory phase</td>
</tr>
<tr>
<td>To be determined by the implementing partner in the preparatory phase</td>
</tr>
<tr>
<td>To be determined by the implementing partner in the preparatory phase</td>
</tr>
<tr>
<td>National reports on the implementation of National Cybersecurity Strategies; Statistical Office (NSO) progress reports; National Law Enforcement Reports; Press Releases</td>
</tr>
<tr>
<td>C1.3.1/2/3 Project update reports; National government reports, including National reports on the implementation of National Cybersecurity Strategies; Statistical Office (NSO) progress reports; National Law Enforcement Reports; Press Releases</td>
</tr>
<tr>
<td>C.1.4.1 Reports by cybercrime units and prosecution offices C.1.4.2 Reports by 24/7 contact points</td>
</tr>
<tr>
<td>Trained staff remain within their institutions beyond the capacity building exercises/duration of the project.</td>
</tr>
<tr>
<td>National governments actively seek the involvement of the private sector (Internet Service Providers for C1; Manufacturers for C2; Medical/drug industry for C3) and civil society.</td>
</tr>
<tr>
<td>Necessary equipment exists/is made available.</td>
</tr>
<tr>
<td>Translation and interpretation services for the roll out of activities do not create delays.</td>
</tr>
</tbody>
</table>
### Effective National Response and International Law Enforcement and Judicial Cooperation

| C2.3 | Improved effective international cooperation and sharing of information and good practices among firearms and organized crime practitioners on the prevention and combat of firearms trafficking and related crimes, through regular contacts and use of specialized cooperation networks and platforms and taking advantage of existing initiatives. |
| C2.4 | Improved capacity to monitor, analyse and identify synergies for firearms legislation and case-law with other forms of transnational organised crime, including cybercrime, money laundering, illicit drug trafficking and smuggling of migrants. |

### C2.3 Number of Intelligence Reports Disseminated by the UNODC Global Firearms Programme

| C3.1 | Increased public and stakeholder awareness on falsified medicines and medicinal products risks |
| C3.2 | Improved legal framework and law enforcement for combating falsified medicines and medicinal products illicit trafficking |
| C3.3 | Enhanced technical capabilities to address the falsified medicines problem. |

| C3.1.1 | Number of policy makers reached with the awareness campaigns on falsified medicines' risks |
| C3.1.2 | Number of community leaders identified and reached with the awareness campaigns on falsified medicines' risks |
| C3.2 | Number of proposals of minimum legislation and regulations that should be in place regarding falsified medicines introduced to the relevant Ministries according to the specificities of each partner country. |
| C3.3 | Number of public officials, prosecutors, medical staff and pharmaceutical inspectors from each country whom acquired adequate knowledge on techniques of investigation and detection of falsified medicines. |

<p>| To be determined by the implementing partners in the preparatory phase | Project progress reports |
| Entrance and exit levels tests of each training course. | Project progress reports | Entrance and exit levels tests of each training course. |</p>
<table>
<thead>
<tr>
<th>C3.3.</th>
<th>Improved interagency collaboration and cooperation among departments and agencies dealing with the fight against falsified medicines in each country.</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3.4.</td>
<td>Enhancement of the international cooperation to tackle the trafficking, identification and effective management of falsified medicines in Eastern and Central Africa region.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C3.4.</th>
<th>Number of elaborated guidelines presented to the relevant Ministry about the improved coordination and no overlap of mandates and responsibilities among departments and agencies dealing with the fight against falsified medicines in each country.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of people from different countries, regional and international organizations participating in a conference on cross-border and trans-regional cooperation.</td>
</tr>
</tbody>
</table>