

Programming Fiche
ESTONIA

Internal Security Fund (ISF)

Future priorities

Specific objective 1 - to increase the exchange of information among and within the Union law enforcement and other competent authorities and other relevant Union bodies as well as with third countries and international organisations

Current priorities or types of actions in the National Programme that could be continued under this specific objective

The current actions that increase the interoperability of IT systems and linking of different services and information for law enforcement agencies should continue.

- Information exchange
- Police/border guards or interagency cooperation (customs, intelligence services)
- Training
- IT-systems, interoperability, data quality, communication systems
- Networks, centres of excellence, cooperation structures, joint actions and operations

Policy issues (in priority order) that should be addressed in the future under this specific objective

Money laundering is a major current issue in Estonia, it is being tackled by changing the banking laws (more detailed reporting by banks, etc.)

Preventing money laundering has become a priority for Estonia against the background of large money-laundering scandals. Estonia has strengthened its anti-money laundering framework and the proportion of non-resident deposits in the Estonian banking sector has significantly decreased. However, challenges remain. While the Estonian government introduced additional measures and guidelines on how to further strengthen the prevention in this area, a legislative initiative aiming at increasing the capacities of the anti-money laundering supervision has not yet been adopted by the Estonian Parliament. Attention should be paid to the effective implementation of these measures, once adopted.

Information Systems

- Ensure the full and uniform implementation of the Union acquis on security supporting information exchange, for example on Prüm, PNR, SIS II (police) or in relation to Europol data, including through the implementation of recommendations made to Member States stemming from the **Schengen evaluations on police cooperation**, and the resulting action plans from Member States.
- Set up and adapt national IT systems or devices in order to ensure the effective connection to security relevant Union information systems and communication networks, including their interoperability.
- Acquire, adjust or develop appropriate tools to address identified gaps in the EU information architecture; for instance with the objective of extending the access to Europol's secure operational network to all relevant competent authorities at the confidentiality level required by the nature of the cooperation, and enhancing connectivity infrastructure so that Europol products and services SIENA, EIS, QUEST could be rolled out beyond Europol National

Units, in particular to PCCCs (Police Customs Cooperation Centres), AROs and PIUs;

- Set up and adapt the relevant IT system to address relevant and future Union priorities (for example: single window approach for the collection of API and PNR data, adoption of artificial intelligence tools for the processing of PNR, development of communication networks for the exchange of PNR at EU level and the interoperability with and connection to the various European (and international) systems and databases relevant for the processing of PNR).
- Create a UMF-based workflow interface with national processing systems to allow automated information exchange and follow up to hits and making UMF as the European standard for data exchanges;
- Introduce/update EIS Data Loaders, incl. New Generation Data Loaders (based on UMF, with a possibility of providing data also for analysis);
- QUEST integration with national single search system with a view to facilitating access/searching Europol data, including the forthcoming pilot project on QUEST+ and automation of searching (QUEST) and hit-follow up processes (SIENA web service);
- Upgrade to SIENA CONFIDENTIAL especially (but not only) for CT Units;
- Support SIENA web service integration with national case management/messaging systems and in particular the integration into 24/7 SPOC where also SIRENE bureaux and INTERPOL NCB reside;
- Implement and upgrade the law enforcement access to European Search Portal (ESP) and the large-scale European Information Systems (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN), noting that it will be possible to make QUEST+ available via ESP (according to Interoperability Regulation);
- Upgrade MS' capabilities for Identity & Access Management, especially since Europol provides multi-level security (BPL, EU-REST and EU-CONF).

Cybercrime

- Develop capabilities to deal with encrypted evidence through the development and sharing of solutions and good practices through participation in Europol's network of points of encryption expertise¹.
- Foster the involvement of law enforcement in 5G standardization bodies and develop close cooperation between law enforcement and relevant technology providers/telecommunication operators, to enable timely implementation of lawful interception mechanisms in 5G networks.
- Ensure that systems are in place to gather statistical data on reporting, investigative and judicial phases of cybercrime, in conformity with Article 18 of Directive (EU) 2019/713 and Article 14 of Directive 2013/40/EU.
- Ensure that the necessary laws, regulations and administrative provisions are in force to comply with Directive 2013/40/EU on attacks against information systems.
- Ensure that the necessary laws, administrative provisions and technical processes are in place to allow for an effective fight against child sexual abuse. In particular, the necessary measures must be in place to enable the transmission of information concerning the existence of criminal convictions for any offences referred to in Articles 3-7 of the Directive 2011/93/EU on combating child sexual abuse and sexual exploitation, or of any disqualification from exercising activities involving regular and direct contact with children arising from such criminal convictions. The transmission must be carried out in accordance with the procedures set out in the Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States when

¹ Page 9 of https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

requested under Article 6 of that Framework Decision with the consent of the person concerned.

Organised Crime

- Ensure the full implementation of **Directive 2019/1153 on law enforcement access to financial information to combat serious crimes**. Pursuant to the Directive, Estonia has to provide the designated national competent authorities and the Asset Recovery Office with **direct access** to the centralised bank account registry by **1 August 2021**. At present, there is no operational registry or system in Estonia.
- Strengthen the operational capacity of the national Asset Recovery Offices, in particular by providing them with direct access to the relevant national databases.
- Improve the operational capacity to manage frozen and confiscated assets by, for example, setting up an Asset Management Office, or by strengthening the capabilities of the existing Asset Management Office, or equivalent mechanism.
- Set up or strengthen national databases for the registration of frozen assets

Anti-Corruption

- Facilitate and streamline the flow of information between institutional actors in Member States in order to facilitate the detection and investigation of complex corruption and economic crime cases.
- Provide access to all relevant public registries and databases to law enforcement authorities in charge of anticorruption to allow a speedier treatment of corruption cases.

Firearms

- Support the establishment of a national focal point on firearms to produce better analysis of all information available in the area of illicit firearms, ensure full participation in the exchange of information with Europol in the area of firearms trafficking, act as a repository for firearms-related intelligence both criminal and ballistic, and as a repository for all lost, stolen and recovered firearms.
- Increase cooperation in the fight against the threat of (imported) gas and alarm, and blank-firing weapons converted into firearms.

Migrant smuggling

- Ensure resources to further make use of opportunities offered by EU Agencies and partners participating in the EMPACT Policy Cycle

Suggestions for desired outcomes

- A more effective exchange of information between relevant authorities on anti-corruption issues, resulting in more cases investigated and prosecuted.
- Ensure the uniform application of the Union acquis on security supporting information exchange for example via Prüm, EU PNR and SIS II, including through the implementation of recommendations from quality control and evaluation mechanisms such as the Schengen evaluation mechanism and other quality control and evaluation mechanisms
- Increase the number of active users of EU and where relevant national security relevant information exchange tools, systems and databases added with support from the Fund, as compared to number of total users.
- Provide the competent authorities with swifter access to financial and other relevant information and, hence, improve the effectiveness of financial investigations into serious crimes, including money laundering.
- Address, if applicable, as a result of the European Semester, those country-specific

recommendations (CSRs) which concern key security policy priorities, in particular the fight against corruption and money laundering.

Specific objective 2 - to intensify cross-border joint operations among and within the Union law enforcement and other competent authorities in relation to serious and organised crime with a cross-border dimension

Current priorities or types of actions in the National Programme that could be continued under this specific objective

- Police or interagency cooperation (customs, border guards, intelligence services)
- Operational projects for preventing and combatting organised crime / cybercrime
- Training

Policy issues (in priority order) that should be addressed in the future under this specific objective

Law Enforcement Cooperation

- Increase law enforcement (joint) trainings, exercises, mutual learning, specialised exchange programmes and sharing of best practice including in and with third countries and other relevant actors, in cooperation with CEPOL and in line with the Strategic Training Needs Analysis when applicable.
- Facilitate and improve the use of joint investigation teams, joint patrols, joint operations, hot pursuits, discreet surveillance, etc. and other operational cooperation mechanisms in the context of the EU Policy Cycle (EMPACT), with special emphasis on cross-border operations
- Develop joint threat/risk analyses to better target joint operations or patrols, and the deployment of technologies such as ANPR, UAVs or mobile communication devices
- Develop training and awareness raising activities in order to enhance the capabilities of the personnel working in Passenger Information Units responsible for the processing of PNR data to conduct joint analysis and joint targeting activities
- Consider a more systematic collection of statistics of hot pursuits and cross-border surveillance with a view to establishing a better overview about its operational cross-border police cooperation requirements (SCHEVAL recommendation)

Child sexual abuse

- Enable efficient cross-border cooperation in the fight against child sexual abuse, including in investigations and the exchange of best practices. Cross-border cooperation should also be enabled at a global level, in coherence with Member States' commitments as part of the We Protect Global Alliance to End Child Sexual Exploitation Online.

Encryption

- Ensure that the network of points of expertise, bringing together experts from all EU Member States, continues to be strengthened through regular participation, contribution, collaboration, and sharing of solutions and good practices to help practitioners overcome the challenges posed by encryption during the course of criminal investigations².

² Page 9 of https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

J-CAT

- Support the existing participation, or establishing temporary or permanent participation in the Joint Cybercrime Action Taskforce, through the secondment of dedicated cybercrime liaisons officers at Europol

Fraud and counterfeiting of non-cash means of payment

- Create/reinforce dedicated points of contact for fraud and counterfeiting of non-cash means of payment, with a view to preparing the implementation of Article 14(1) of Directive (EU) 2019/713

Organised Crime

- Increase coordination and cooperation of law enforcement authorities and other competent authorities dealing with organised crime, for example through networks of specialised national units
- Provide financing for operational support in complex high profile investigations requiring highly specialised criminal expertise, in particular support to Member States' participation in Operational Task Forces (OTF) to identify High Value Targets (HVT) posing the highest risk to the internal security of the EU
- Increase exchange on EU crime statistics in harmonised manner with a possibility to create EU CRIM statistic data base (database on a number of phenomena could help us to define the threats and risks better)
- Extend assistance to state-of-the-art forensic expertise, for example deployment of digital forensic tactical advisers; large-scale technically demanding support on the ground; network acquisition/cloud forensics/live forensics, etc.

Trafficking in human beings

- Focus on preventing trafficking in human beings, by countering the impunity that fosters the crime, enhancing national and transnational efforts to step up investigations, prosecution and convictions of all perpetrators.

Anti-Corruption

- Facilitate operational cooperation and coordination among law enforcement authorities and other relevant authorities in and among the EU Member States and with relevant agencies and third country authorities for a more effective investigation of cross border corruption cases
- Facilitate information exchange and training on best practices in investigating cross-border corruption cases

Drugs

- Enhance operational cooperation between EU Member States and with EUROPOL and the EMCDDA to disrupt the illicit drugs markets. This should take into account that fentanyl and fentanyl analogues have emerged as significant threats on European drug markets, with the Baltic countries playing a key role in this. Fentanyl and fentanyl analogues are trafficked to the EU from Russia, supplying local markets in the Baltic States, and from China to consumers across the EU. Previously restricted to Estonia, there have been several localised outbreaks of fentanyl use in the EU resulting in a number of lethal overdoses in Member States.
- Focus on the current trends – including notably technological developments and the spread of synthetic opioids, including fentanils
- Improve monitoring and operational resources in cooperation with EUROPOL and the EMCDDA against drug trafficking and distribution using online platforms such as social media, websites, Darknet markets, including developing new responses to tackle the threat

posed by trafficking through postal and parcel deliveries, including through informal parcel delivery entities

- Better respond to a globalised drug market by strengthening partnerships between Member States' authorities, international organisations, third countries and with industry, as well as operational actions identified under EU dialogues on drugs with third countries.
- Contribute to a measurable reduction of the demand for drugs on what concerns prevention

Firearms

- Enhance operational cooperation to fight against firearms trafficking along firearms trafficking routes, notably by strengthening the operational cooperation among law enforcement authorities and improving knowledge, detection, investigation and prosecution in using dedicated investigative tools, in particular in relation to priority regions/countries for Estonia, which are likely to pose a threat to the EU's security and most likely to benefit from EU action.

Migrant smuggling

- Ensure resources to allow efficient cooperation between EU MS LEAs and Third Countries LEAs, including through JITs/COPs
- Establish list of trusted interpreters and translators at national/regional level to support investigative and judicial follow-up of cross-border crimes

Suggestions for desired outcomes

- An increased number of cross-border operations in the area of corruption, resulting in the long run in a decrease of the cross-border criminality related to corruption.
- Increase the number of joint operational actions supported by the Fund, including the participating Member States and authorities in relation to serious and organised crime with a cross-border dimension
- Increase the number of victims of crime assisted with the support of the Fund in relation to serious and organised crime with a cross-border dimension
- Address, if applicable, as a result of the European Semester, those country-specific recommendations (CSRs) which concern key security policy priorities, in particular the fight against corruption and money laundering.

Specific objective 3 - to support effort at strengthening the capabilities in relation to combatting and preventing crime including terrorism in particular through increased cooperation between public authorities, civil society and private partners across the Member States

Current priorities or types of actions in the National Programme that could be continued under this specific objective

- Information exchange
- Police or interagency cooperation (customs, border guards, intelligence services)
- Training
- Exchange of best practices, workshops, conferences, events, awareness raising campaigns, communication activities
- Development of technology / forensics techniques
- Protection and resilience of public spaces and other soft targets
- Protection and resilience of critical infrastructure
- Crisis management

Policy issues (in priority order) that should be addressed in the future under this specific objective

Law Enforcement Cooperation / Training

- To increase law enforcement (joint) trainings, exercises, mutual learning, specialised exchange programmes and sharing of best practice including in and with third countries and other relevant actors, in cooperation with CEPOL and in line with the Strategic Training Needs Analysis when applicable.
- To increase training, exchange of best practices (including the Unions agencies, such as CEPOL and Europol, as well as air carriers' industry and other relevant actors) on the development of PNR systems and the exchange of PNR data.
- To focus training projects on the following policy priorities under each crime area: open source intelligence, data collection, analysis and application; financial investigations, money flows, alternative banking, etc.; elements of cyber-investigations, darknet and e-evidence; document fraud; fundamental and human rights; crime prevention; respective areas of forensics; links between different crime areas; and English language, specific professional terminology.
- To support the development of CEPOL National Units with adequate resources to ensure Law Enforcement training reaches all relevant Law Enforcement bodies.
- To exploit synergies by pooling resources and knowledge among Member States and other relevant actors, including civil society through, for instance, the creation of joint centres of excellence, the development of joint risk assessments, or common operational support centres for jointly conducted operations.
- To increase analytical capacities especially from mobile devices (UFED).
- Ensure adequate multidisciplinary counter-crime structures to deal with increasing poly-criminal organised crime groups often posing a mafia style threat. This multidisciplinary nature should also go beyond solely law enforcement aspects to include cooperation with the private sector, third countries and be carried forward along the whole penal chain. The multidisciplinary approach should also be reflected in the provision of resources to guarantee timely data collection on criminal justice statistics collected by Eurostat (e.g. migrant smuggling), including cross-cutting collection from various authorities such as police, prosecution, courts, prisons

Prevention of radicalisation

- Countering online extremist and terrorist propaganda: Strengthen capabilities to detect and refer terrorist content and coordinate with Europol; support the development of alternative and counter narratives as well as strategic communications capabilities.
- Local and multi-agency approach: Support to local and regional administrations and initiatives, in particular to develop local prevent strategies, action plans, collaborations among relevant stakeholders (including civil society actors and communities) and other capacity building actions (e.g. by offering training and consultancy).
- Ideology and polarization: Work with communities (training and civic education for religious leaders,...), support local authorities to develop an action plan for dealing with presence of local extremist groups, support information and awareness raising campaigns on how to report hate speech and threats online and in local communities, encourage dialogue with media on a common understanding of responsible reporting on extremist violence and extremist groups.
- Addressing the issue of polarisation between communities (resilience, early prevention, democratic values, rule of law etc.) as well as on line resilience and programmes to counter on line misinformation (counter narratives).
- Addressing the issue of the right wing extremism (resilience, early prevention and promotion of democratic values).

Protection of citizens and infrastructure

- Protection of public spaces. The actions could cover: enhanced public-private cooperation; enhanced protection against threats posed by Unmanned Aerial Vehicles and other emerging threats; acquisition and use of detection equipment, including mobile, regarding chemical, biological, radiological, nuclear and explosives (CBRN-E) threats.
- CBRN-E: The actions could include 1) effective implementation and enforcement of the new Explosives precursors Regulation, including online mystery shopping; different tools to raise awareness in the supply chain of the obligations of the Regulation and evaluate their effectiveness; 2) pooling of resources and knowledge among Member States, sharing of good practices, and conducting trainings and exercises 3) measures to enhance the security of radioactive sources, including upgrade in physical protection and awareness raising activities.
- Addressing insider threat: The actions could include: background checks (in particular in aviation, but also in relation to protection of major public events and for personnel with access to CBRN materials).
- Critical Infrastructure Protection: The action could include 1) analysis of interdependencies, vulnerabilities and possible cascading effects on critical infrastructure networks, possibly in conjunction with neighbouring Member States. 2) Measures to improve cooperation and support to critical infrastructure operators, e.g. establishing mechanisms for regular dialogue between authorities and operators, facilitating the exchange of threat and incident information, providing training to operators' security staff, disseminating guidance or best practice on security standards, establishing common criteria for risk assessments, or conducting exercises to test critical infrastructure protection and resilience. 3) A review of the state of play and future trends in application of the Directive 2008/114 on European Critical Infrastructures (ECI) and especially of the part on identification of ECIs.

Combating terrorist financing

- Strengthen capabilities in relation to counter-terrorism financial investigations, improve capabilities to conduct financial investigations into cryptocurrencies or other virtual assets

Drugs

- Reduce vulnerabilities at borders by enhancing risk analysis and profiling, intelligence sharing and implementation of proven approaches at ports, airports and land crossing points
- Enhance forensic capacity at national level to determine and address the threats posed by innovations in drug production and trafficking methods

Encryption

- Support LE officers to allow their participation in the training courses developed by European Cybercrime Training and Education Group and (in most cases) delivered by CEPOL

Cybercrime

- Support LE officers to allow their participation in the training courses developed by ECTEG (European Cybercrime Training and Education Group) and (in most cases) delivered by CEPOL including the CEPOL Cybercrime Academy
- Reinforce/develop training programmes based on competencies described in the EU Training Competencies Framework and on the training priorities identified in the CEPOL Operational Training Needs Analysis (OTNA) on Cybercrime. Use of available materials (e.g. ECTEG courses) is recommended.
- Cyber-crime centre of excellence
- Ensure/develop/improve platforms for online reporting of crimes committed online, especially with regard to fraud and counterfeiting of non-cash means of payment
- Develop/set up entities able to assist victims of cybercrime and online fraud, especially with regard to identity theft, with a view to preparing the implementation of Directive (EU)

2019/713

- Enable the development and implementation of measures to prevent the sexual abuse and sexual exploitation of children, including through public-private partnerships and cooperation with civil society and academia. Of particular relevance are prevention programmes to prevent recidivism and programmes for persons who fear that they might sexually offend against children, and, in general, the measures referred to in Articles 21 to 24 of Directive 2011/93/EU on combatting child sexual abuse and sexual exploitation.

Organised Crime

- Strengthen capabilities in investigating organised crime with a focus on High Value Targets
- Increase application of administrative approach to tackle serious and organised crime and provide for legal framework to allow for better exchange of administrative information across borders
- Strengthen capacities to develop and make use of special investigative techniques relevant to the fight against organised crime.

Anti-Corruption

- Improve the management of the human resources in law enforcement agencies (transparency in recruitment procedures, including for top management positions, rotation of staff in sensitive posts, unification of ethics rules in a single code, “revolving doors” rules to prevent conflict of interest, etc).
- Implement the national anti-corruption strategy (2013-20120) and the related Action plan
- Enhance the capacity of the national authorities via training, specialised exchange programmes and sharing of good practices with a view to achieving a better prevention, detection and repression of corruption in the public and private sector
- Support civil society actions in the area of preventing and detecting corruption
- Facilitate improvement of national statistical data collections on the treatment of corruption cases in the criminal justice system in Member States

Trafficking in Human Beings (THB)

- The priorities related to the fight against THB include: preventing that trafficking in human beings happens; addressing the culture of impunity via national and transnational efforts to increase investigations, prosecution and convictions of traffickers; victims of trafficking in human beings should be treated as rights holders to effectively exercise their rights when it comes to their assistance, support and protection. For this their early identification is important.

Migrant smuggling

- Ensure adequate multidisciplinary counter-crime structures to deal with increasing poly-criminal organised crime groups often posing a mafia style threat. This multidisciplinary nature should also go beyond solely law enforcement aspects to include cooperation with the private sector, third countries and be carried forward along the whole penal chain.
- Assign the necessary resources at national level (e.g. specialised units) in order to enhance smooth cross-border cooperation with counterparts in other Union Member States
- Enhance cooperation with the private sector in the prevention and follow-up to cross-border crimes e.g. financial sector, social media outlet, courier service providers, information sharing with haulage sector / carriers, etc
- This should also be reflected in the provision of resources to ensure timely data collection on criminal justice statistics collected by Eurostat (e.g. migrant smuggling) – includes cross-cutting collection from various authorities such as police, prosecution, courts, prisons.
- Increase national capacities to detect document fraud (in particular at the air border).

- Vulnerabilities identified in the two latest cycles of vulnerability assessments carried out by the EBCGA require a focus on ensuring availability of sufficient number of appropriately trained staff (document experts), appropriate technical equipment to detect sophisticated document fraud and forensic expertise.
- Training activities in the area of migrant smuggling at national level for law enforcement and judiciary (including related to documentary fraud, financial and online investigations and cooperation with third countries). Through the CEPOL Strategic Training Needs Analysis, Member States identified training related to the Facilitation of Illegal Immigration as the highest priority out of 21 criminal areas. This combined with the more specific Training Needs Analysis focusing specifically on cross-border cooperation to address migrant smuggling, pointed to the following training priorities at national level focusing on law enforcement and judicial officials to:
 - Enhance English foreign language skills to allow cross-border cooperation, which is to be supplemented at European level by specific professional terminology training activities
 - Knowledge of opportunities working with non-EU countries
 - Awareness of the role of social media in migrant smuggling and the relevant procedures (take-down request of pages, or their preservation for investigative purposes).

Security Research

- Developing innovative methods or deploying new technologies in close cooperation with the European Network of Law Enforcement Technology Services (ENLETS): testing, validating and exploiting the outcome of Union funded security research projects in developing and procuring state of the art tools and instruments for LEAs

Suggestions for desired outcomes

- A more effective prevention and repression of corruption by implementing the actions foreseen in the national anti-corruption strategy and the related action plan and by improving the human resources policy for the law enforcement agencies.
- Increase the number of law enforcement officials that completed training, exercises, mutual learning or specialised exchange programmes on cross-border counter terrorism provided with the support of the Fund
- In Critical Infrastructure Protection (CIP) develop a strong capacity to conduct risk assessments and engage with private operators, especially in order to provide security advice.
- Address, if applicable, as a result of the European Semester, those country-specific recommendations (CSRs) which concern key security policy priorities, in particular the fight against corruption and money laundering.
- Improved capabilities to fight cybercrime, e.g. through training, the development or adaptation of tools, collaboration (between LEAs and with other stakeholders), and the use of capabilities available at Europol (which might require training and technical connections).

Other comments

External dimension

- Cooperation with third countries on anti-terrorism and anti-radicalisation activities, cooperation between law enforcement authorities in the fight against terrorism, drugs and criminality as well as operational cooperation to tackle trafficking in human beings and migrant smuggling. Where needed implementation could be envisaged via several channels e.g. ad hoc projects/programmes, liaison officers, special investigation teams.

Synergies with other Funds

Asylum and Migration Fund
<p>There could be complementarities between ISF and AMF on legal migration regarding actions related to the fight against trafficking in human beings and migrant smuggling, protection of victims of trafficking in human beings and prevention of and countering radicalisation.</p> <p>Financing of EURODAC/security part.</p>
Border Management and Visa Instrument
<p>Actions related to border surveillance systems which could also contribute to security purposes and for fighting cross border crime, terrorism, migrant smuggling and trafficking in human beings.</p> <ul style="list-style-type: none">• LEA access to EES and other border management systems• Solutions to fight serious and organised crime at the borders, e.g. container scanner to be used at the border to detect illegal trafficking, depending also on which type of equipment is funded under the new Customs Control Equipment Fund.• ICT platforms/situation rooms/crisis management/communication tools which need to incorporate intelligence from inside the national territory and info gathered at the borders.
Cohesion Funds (ESF+, ERDF, etc)
<p>European Social Fund+: actions to counter radicalisation, victim protection, drugs</p> <p>In the Multiannual Financial Framework 2014-2020, drug policy issues were addressed mainly by the anti-drugs chapter of the Justice Programme (mainly on what concerns drug demand/public health) and by the Internal Security Fund – Police (mainly on what concerns drug supply/law enforcement and security), in line with the two pillars of drugs policy: security and public health. It was decided that the successor of the current Justice programme will not address any drug policy topics. The future Internal Security Fund 2021-2027 will address mainly security aspects of drugs policy; however, the public health aspects of drugs policy are envisaged to be addressed by the successor of the current Health Programme – the European Social Fund Plus (ESF+), including on health services to patients in the area of drugs, harm reduction and prevention of drugs related deaths and research on the epidemiology aspects of the use and abuse of drugs. These measures focused on public health challenges related to illicit drug should be covered not only by the health strand of the ESF+, but also by the shared management/national programmes co-funded by ESF+.</p> <p>ESF+ may also support actions aimed at fostering active inclusion and promoting equal access to and completion of quality and inclusive education and training for disadvantaged groups and through improving access to employment of, in particular, long-term unemployed and inactive people. Victims of crime could benefit from measures aiming to improve access to long-term care.</p> <p>European Regional Development Fund: protection/design of public spaces, cybersecurity, actions to counter radicalisation, Critical Infrastructure</p> <p>ERDF could finance actions related to the protection of public spaces. ISF can finance small-scale projects, such as the innovative integration of security into the design of new buildings/public space and the purchase of closed circuit television systems, concrete bollards and other preventive equipment, such as cyber-attack resilient information and communications security systems. However, the ERDF is better placed for making such investments at regional and local level and contributing to infrastructure investments where security is a key element in the design of the public space.</p>

ERDF will also address cybersecurity concerns when promoting digitalisation of SMEs, large enterprises and promoting government ICT solutions and IT services (cyber threats and cybercrime) under ERDF specific objective *Reaping the benefits of digitisation for citizens, companies and governments* (PO1). Cyber threats are increasing. They can disrupt the supply of essential services (critical infrastructure) such as water, healthcare, electricity, mobile services or generate substantial financial losses, undermine user confidence and cause major damage to the economy. Cybercrime is one of the fastest growing forms of crime and the risks are increasing exponentially. Unless we substantially improve cybersecurity, the risk will increase in line with digital transformation.

ERDF can also address protection of critical infrastructure (e.g. transport infrastructure, power plants, data centres, security and safety at airports and of air traffic management systems etc) under i.a. specific objective *Developing smart energy systems* (PO2) or specific objective *Developing a sustainable, climate resilient, intelligent, secure and intermodal TEN-T* (PO3).

Under PO 5 ERDF can also address security in the urban and other areas through the following specific objectives *Fostering the integrated social, economic and environmental development, cultural heritage and security in urban areas* and *Fostering the integrated social, economic and environmental local development, cultural heritage and security, including for rural and coastal areas* (...). It can cover e.g. prevention of radicalisation under social integration measures and protection of public spaces.

External Instruments (NDICI and IPA)

The external actions will continue to be implemented in complementarity to the NDICI and IPA that are and will remain the primary tools to support the external dimension of the Union's migration and security policy. Member States through their national programmes are more adequate to promote and deliver on cooperation initiatives that complement and reinforce actions taken at the EU level. For example, when Member States have good bilateral relations with third countries, specific interests and expertise or networks in a given third country, or when the nature of a specific policy has a direct impact on the MS and might require bilateral cooperation.

Neighbourhood, Development and International Cooperation Instrument (NDICI): fighting THB and migrant smuggling, support to regional and international initiatives contributing to security, preventing and countering radicalisation

NDICI can support actions in third countries to address the root causes of irregular migration and forced displacement, and it can support security and migration management and governance. The ISF on the other hand will provide for an external dimension that will essentially represent an extension of the EU's security policies. It will focus on actions that serve primarily the EU's security related priorities.

NDICI will allow for making best use of geographic programmes, supplemented by the Global Challenges thematic programme and the rapid reaction response pillar. In the area of security, this includes for instance addressing political and economic exclusion and other long-term structural and root causes of conflict, insecurity and instability, supporting regional and international initiatives contributing to security, stability and peace and preventing and countering radicalisation leading to violent extremism and terrorism as well as fighting against any form of violence, corruption, organised crime and money laundering.

The Internal Security Fund will continue supporting cooperation with third countries on anti-terrorism and anti-radicalisation activities, cooperation of law enforcement authorities in the fight against terrorism as well as serious and organised crime, trafficking in human beings and migrant smuggling, including through joint investigation teams.

Instrument for Pre-Accession Assistance (IPA): fight against organised crime/corruption/ THB and migrant smuggling, strengthening law enforcement

The Instrument for Pre-Accession Assistance will support enlargement countries in preventing and tackling organised crime and corruption, and in strengthening their law enforcement and migration

management capabilities, including border management. It will support cooperation on migration, ensuring access to international protection, sharing relevant information, strengthening the development benefits of migration, facilitating legal and labour migration, enhancing border control and pursuing our effort in the fight against irregular migration, trafficking in human beings and migrant smuggling.

Other Funds

Digital Europe: cybersecurity

The Digital Europe Programme is about digital transformation of public services and businesses. Amongst several other issues it will address cybersecurity, as it is of key importance to ensure trust in digital products and services, especially given the wide spread of cyber-attacks. ISF will deal with cyber-dependent crimes, i.e. crimes that can be committed only through the use of information and communications technology devices and systems, and cyber-enabled crimes, i.e. traditional crimes, such as child sexual exploitation, which can be increased in scale or reach by the use of computers, computer networks or other forms of information and communications technology.

Horizon Europe: security related research projects leading to innovative technologies

There are complementarities between ISF and the Horizon Europe Programme. Actions related to innovative new technologies and security relevant research projects under the cluster "Inclusive and Secure Society" can be supported by ISF.

Customs Control Equipment Instrument: customs control equipment to be used also for police cooperation and fight against serious and cross border crime

Multi-purpose equipment, e.g. container scanner purchase, also other equipment could fall into the grey zone. Need to coordinate with TAXUD on gap assessment / needs. PCCCs.

EU civil protection mechanism: Exploit synergies regarding disaster risk management, prevention and preparedness.

EU Defence Fund: Multi-purpose equipment (e.g. UAVs)

SRSP: potential overlap/synergies in several areas such as radicalisation, money laundering, financial crime, OSINT to counter terrorism, disaster management, cybercrime, anti-corruption, etc.