Council of the European Union

Brussels, 10 December 2021
(OR. en)

14874/21

JAI 1390	**DROIPEN 155**
COSI 247	**COPEN 448**
ENFOPOL 503	**FREMP 294**
ENFOCUSTOM 192	**JAIEX 133**
IXIM 287	**CFSP/PESC 1223**
CT 171	**COPS 465**
CRIMORG 161	**HYBRID 79**
FRONT 434	**DISINFO 44**
ASIM 102	**TELECOM 458**
VISA 249	**DIGIT 186**
CYBER 327	**COMPET 899**
DATAPROTECT 284	**RECH 558**
CATS 79	

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	8 December 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2021) 799 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Third Progress Report on the implementation of the EU Security Union Strategy

Delegations will find attached document COM(2021) 799 final.

Encl.: COM(2021) 799 final

EUROPEAN
COMMISSION

Brussels, 8.12.2021
COM(2021) 799 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Third Progress Report on the implementation of the EU Security Union Strategy

I. Introduction

The Security Union aims to ensure that the EU plays its full role in ensuring the safety of citizens while respecting the values that define the European way of life. Implementation is progressing on all four strategic priorities set out in the Security Union Strategy[1]: (i) a future-proof security environment; (ii) tackling evolving threats; (iii) protecting Europeans from terrorism and organised crime; and (iv) a strong European security ecosystem.

The COVID-19 pandemic has accentuated key vulnerabilities, while threats and challenges to European security continue to evolve in response to changing technologies and international developments. The second Security Union report[2] charted the particular challenges for security presented by the COVID-19 pandemic.

This third report focuses on the developments of the past six months linked to the most significant emerging threats in this period. It highlights in particular the need to intensify cooperation not only within the EU, but also internationally, with a broad array of stakeholders and partners.

The Security Union Strategy is being taken forward in the context of threats that are increasingly cross-border and cross-sectoral. The digital world continues to be exploited for malicious ends. Cyber-attacks originating in or outside Europe, including ransomware, are ever more frequent, hitting core state functions, such as healthcare and crucial infrastructure, industries and public bodies, as well as individuals. Foreign information manipulation and interference activities are on the rise, and have in some cases gone hand in hand with cyber activities, in particular hack and leak operations. Organised crime of all kinds continues to operate cross-border, and an effective response relies on partnerships beyond the EU. International developments require vigilance in the context of potential radicalisation and terrorism, as well as hybrid attacks including, during this reporting period, at the EU's external border.

To address these increasingly sophisticated global and cross-border threats, the EU is stepping up not only its own response but also cooperation with international partners. This is a core theme of this report.

At the same time, work is intensifying to reinforce security in the Schengen area. Close cooperation between Member States is crucial to the overall security of the Schengen area. A substantial new package including measures to enhance police cooperation and the security of the Schengen area has been prepared by the Commission to provide further improvements in this regard.

EU agencies are fully involved in this work through their operational activities in support of Member States' national authorities, and by providing expertise, information and situational awareness on the most pressing threats.

Further details and updates on the full range of initiatives under the Security Union are presented in an Annex to this Communication.

---

1 COM(2020) 605.
2 COM (2021) 440.

II. A future-proof security environment

Digital infrastructures, technologies and online systems allow us to create business, consume products and enjoy services. However, this growing digitalisation of our environment also makes us more vulnerable to attack. The scale, frequency and sophistication of cybercrime and cyber attacks is increasing, according to both **Europol**'s Internet Organised Crime Threat Assessment published in November 2021[3], and the EU Agency for Cybersecurity (**ENISA**)'s annual Threat Landscape report of October 2021. Governments in Europe faced at least 198 cybersecurity incidents in the past year, making public administration the most heavily targeted sector. Highly-skilled and well-resourced malicious actors come from inside, but also from outside the EU, and exploit the borderless nature of the global, open internet and the jurisdictional gaps of current frameworks. Cyberattacks and cybercrime are often interlinked, as demonstrated by numerous incidents where criminals are targeting vulnerabilities to extort money, and are a constant threat that continues to evolve. Cybercriminals may simply be motivated by increasing opportunities for the monetisation of their activities, but other malicious state or non-state behaviours are motivated by more complex geopolitical and ideological considerations, in addition to financial gains. Data gathered by **ENISA** has shown that state-backed hackers also reached 'new levels of sophistication and impact' with attacks targeting public and private sector supply chains[4].

It is therefore particularly important to maintain a high level of ambition for EU action, both in terms of the level of security we seek to achieve, and the pace at which we work to achieve it. The European Council of October 2021[5] addressed the marked increase in malicious cyber activities. It reaffirmed the EU's commitment to an open, free, stable and secure cyberspace, and stressed the need for effective coordination and preparedness in the face of growing cybersecurity threats. It also emphasised the necessity to step up action in the fight against cybercrime, in particular ransomware attacks, and enhance cooperation with partner countries, including in multilateral fora.

3 Internet Organised Crime Threat Assessment, 11 November 2021.
4 ENISA Annual Threat Landscape Report, 27 October 2021.
5 Conclusions of European Council, 21-22 October 2021.

Some examples of recent cyber/ransomware incidents in the reporting period

- July: Some 500 supermarket stores in Sweden were forced to close due to a very aggressive cyberattack affecting organisations around the world.
- July: **Estonia** reported that a Tallinn-based hacker downloaded 286,438 ID photos from government databases, exposing a vulnerability in a platform managed by their Information System Authority.
- August: The Lazio region in **Italy** suffered a ransomware attack that disabled administrative IT systems, including the COVID-19 vaccination registration portal. New vaccination appointments could not be scheduled for several days after the attack.
- September: In **Germany,** a cyberattack was confirmed in which hackers were able to breach the server and file systems of Germany's Federal Statistical Office, which is led by the national election commissioner.
- September: In **the Netherlands**, a cyberattack hampered the launch of a COVID passport.
- October: A ransomware attack on a hospital in **Belgium** forced it to cancel all scheduled consultations.
- November: During the cyberattack on the European branch of Mediamarkt hackers demanded USD50 million in Bitcoin.

Addressing EU resilience internally

The Commission's 2020 proposals on the **protection and resilience of critical infrastructure**, both physical and digital, are currently under negotiation in the European Parliament and the Council. On 19 October 2021, the Parliament adopted its negotiating mandate for the draft Directive on critical entities resilience, and on 10 November 2021, for the draft Directive on measures to achieve a high common level of cybersecurity across the Union (NIS2 Directive). The Council reached a general approach on NIS2 on 3 December. This will open the door to a swift, coherent and ambitious conclusion of negotiations in 2022.

A key component to increase the EU's ability to react and recover promptly came with the Commission's Recommendation to set up a **Joint Cyber Unit** (JCU). The JCU would bring together Member States and relevant EU institutions, agencies and bodies to provide a structure for coordinated cooperation at operational level. It would help to connect the various players responsible for cybersecurity operations across the EU cybersecurity communities (resilience, law enforcement, cyber diplomacy, and cyber-defence). On 19 October, the Council agreed[6] to explore the potential of the JCU initiative complementing the Commission's Recommendation on a coordinated response to large-scale cybersecurity incidents and crises. A preparatory process has been initiated and several workshops have been organised by **ENISA** to discuss deliverables and next steps, as defined in the Commission's recommendation and taking into account the Slovenian's Presidency paper on the way forward for the JCU[7].

[6] Council Conclusions on exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, 12534/2021 https://data.consilium.europa.eu/doc/document/ST-12534-2021-INIT/en/pdf.

[7] The Slovenian Presidency also produced a discussion paper (13019/21) on the way forward for the JCU, outlining concrete steps in order to enhance common situational awareness within and among all relevant cyber communities.

In addition to these overarching proposals, sectoral legislation complements this work, taking into account specific vulnerabilities, and during the reporting period progress can be noted in the financial, health, maritime and energy sectors, and in protection of consumers.

Negotiations are progressing on the **Digital Operational Resilience Act for the financial sector**, which aims to enhance the overall digital operational resilience of financial institutions. The Council reached a General Approach on 24 November, while the European Parliament aims to adopt its negotiating mandate before the end of the year. Once adopted, these measures will provide the EU and its Member States with a strong and future-proof legislative framework to address these challenges more effectively, provided the level of ambition required is reflected in the final outcome of the negotiations.

The pandemic has served to underline the essential nature of the healthcare sector, and the need for a strong **health security** framework. The European Health Union proposals, aim at improving EU-level protection, prevention, preparedness and response against human health hazards and show the EU's ambition and determination to protect this vital sector. Agreement has already been reached on updating the mandates of key agencies, and should soon follow on cross-border health threats. The launch of the EU Health Emergency Preparedness and Response Authority (HERA) in September 2021 has also added a new dimension to this work, and will be supported by a new framework of emergency, time-limited measures to be triggered if required.

Cyber and hybrid threats in the maritime domain, targeting critical **maritime infrastructure,** such as ports, undersea cables and pipelines, energy platforms and maritime traffic choke points, can be extremely disruptive. The EU Maritime Security Strategy and its Action Plan[8] are currently being assessed for a possible update, through which evolving cyber and hybrid threats could be addressed more effectively.

In the recent Communication on 'Tackling rising **energy** prices: a toolbox for action and support'[9], the Commission announced its intention to undertake actions by the end of 2022 to adapt the resilience of the energy system to new threats such as cyber attacks or extreme weather events. These would include new rules on the cybersecurity of electricity, a recommendation on the resilience aspects of clean energy and a European Standing Group of operators and authorities on the resilience of energy infrastructure.

Security vulnerabilities are also present in many smart products and wireless devices. Children in particular may be exposed to security risks because of vulnerabilities of **electronic products,** such as connected toys and smartwatches. To tackle the issue, in October 2021, the Commission adopted a delegated act under the Radio-Equipment Directive to safeguard privacy and networks and to protect against fraud in connected electronic products[10]. This would impose requirements on manufacturers that would increase the level of cybersecurity of products placed on the EU market, and allow Member States to take corrective measures if unsecure products are found on the market.

[8] Report on the implementation of the revised EU Maritime Security Strategy Action Plan SWD(2020) 252.
[9] COM(2021)660.
[10] COM(2021) 7672.

Addressing EU resilience through international co-operation

Security threats are global in nature, and building robust international partnerships is essential to address them effectively. The EU and its Member States are therefore stepping up their action to prevent, deter and respond to state and non-state sponsored threat actors, including by efforts to attribute responsibility more clearly. In July 2021, the EU[11], the United States, NATO and other world powers released statements strongly denouncing malicious cyber activities and attributing the Microsoft Exchange server hack of early 2021 to the territory of China. This malicious cyber activity compromised more than 100 000 servers worldwide. On 24 September 2021, the High Representative issued a declaration on behalf of the EU[12] on respect for the EU's democratic processes, denouncing a number of malicious cyber activities, urging the Russian Federation to respect the norms of responsible state behaviour in cyberspace, and calling on all involved to end such activity immediately.

Discussions on global security challenges are gaining momentum at **multilateral** level. The **G7** Interior and Security Ministers' meeting in September 2021 discussed a range of issues from child sexual abuse material online, to ransomware, combatting terrorism and serious crime, and corruption. G7 partners shared converging positions and committed to increase information-sharing (including biometrics and biographic) while ensuring protection of personal data and fundamental rights.

The EU also took part in the **G20** Digital Ministers' meeting under the Italian Presidency in August. Ministers agreed a declaration[13] stressing the need to ensure data safety for the general public and businesses, and safeguard the security of the digital environment for all. They also agreed a set of G20 Principles for a Safe and Beneficial Digital Environment for Children were agreed.

The EU has been a strong supporter of multi-stakeholder cooperation, believing that it is essential to keep cyberspace open, stable and secure. In November 2021, in the context of the 2021 Paris Peace Forum, President von der Leyen announced the decision to support the **Paris Call for Trust and Security in Cyberspace**, joining the over 80 states, 700 companies, 350 civil society organizations committing to work together to face the challenges but also the opportunities cyberspace brings.

The EU also engages bilaterally with a number of third countries, including through regular Security and Cyber dialogues. The EU-US cooperation on security issues has gained momentum over the past months and is a key example of work with like-minded countries to advance the security agenda.

---

[11] Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory, 19 July 2021.

[12] Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes. 24 September 2021.

[13] https://www.g20.org/wp-content/uploads/2021/08/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdfhttps://www.g20.org/wp-content/uploads/2021/08/DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf.

EU-US cooperation on security issues

The EU-US Summit of 15 June 2021 underlined a renewed determination to address common challenges in the area of security jointly. A number of initiatives have followed:

- The **EU-US Trade and Technology (TTC) Council** held a first meeting on 29 September 2021. The related Pittsburgh Statement[14] underlined the importance of investment screening to address risks to national security, of cooperation in areas related to export control for trade in dual-use items, of expanding resilient and sustainable supply chains, as well as of tackling foreign information manipulation and interference. The TTC includes a working group dedicated to **Information and Communication Technology and Services, Security and Competitiveness**, which will work on issues like security, diversity, interoperability and resilience across the ICT supply chain, including sensitive and critical areas such as 5G, undersea cables, data centres, and cloud infrastructure.
- An **EU-US Cyber Dialogue** took place on 21 September 2021. There was agreement on the need to increase cooperation and coordination on the UN discussions pertaining to cyber, to prevent, deter and respond to malicious cyber activities and to engage effectively with other countries, notably on increasing global resilience.
- The EU participated in the White House **Counter Ransomware Initiative** in October 2021[15], along with senior experts and government representatives from 30 countries. Discussions covered network resilience, misuse of virtual currency to launder ransom payments, information exchange to support the investigation and prosecution of transnational ransomware criminals, and diplomatic efforts to support shared objectives to counter ransomware. An **EU-US working group on ransomware** with a focus on operational cooperation among law enforcement met for the first time on 25 October 2021.
- In the margins of the G20 meeting of October 2021, the EU discussed with the US and other participants near-term **supply chain disruptions** and paths to long-term resilience, with a view to avoiding shortages and maintain open markets[16].

In order to combat **cybercrime** effectively, efforts to improve cross-border access to electronic evidence for criminal investigations are being undertaken around the globe, at national, EU[17] and international levels. Compatible rules at international level are particularly important to avoid conflicts of law when cross-border access to electronic evidence is sought.

Major progress on this front has been achieved with the formal conclusion of the negotiations on the Second Additional Protocol to the Convention on Cybercrime (**Budapest Convention)** under the Council of Europe, with adoption of the text by the Committee of Ministers of the Council of Europe on 17 November 2021. The Commission adopted proposals to authorise

[14] EU-US Trade and Technology Council Inaugural Joint Statement (europa.eu).

[15] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting (October 2021)

[16] Chair's Statement on Principles for Supply Chain Resilience. 31 October 2021, White House

[17] The "e-evidence package" (COM (2018)225 and COM (2018)226), is still under negotiation by the European Parliament and Council. It would provide national law enforcement and judicial authorities in the EU with European Production Orders and European Preservation Orders to obtain digital evidence from service providers for criminal investigations, irrespective of the location of the establishment of the provider or the storage of the information in a swift manner and at the same time provide for strong safeguards.

Member States, in the interest of the Union, to swiftly sign and ratify the Protocol[18] and is now closely working with the European Parliament and the Council to enable Member States to sign and ratify as soon as possible. The Protocol provides tools for practitioners around the world to enhance cooperation on cybercrime and electronic evidence, and recognises that effective cross-border cooperation for criminal justice purposes benefits from strong safeguards for the protection of fundamental rights. The Protocol also includes safeguards for the protection of privacy and personal data.

In parallel, a new United Nations cybercrime convention is being prepared, which should be legally consistent with existing instruments, in particular the Budapest Convention. The Commission will ensure effective participation of the European Union in the negotiations starting in January 2022.

III. Tackling evolving threats

The most significant evolving threats observed during the reporting period concern **hybrid** threats and the continuous evolution of **technological developments**. The scale, changing nature and modus operandi of security and hybrid threats today are a constant challenge, with the variety of tools used by malicious actors expanding. Security challenges also increasingly arise from evolving technological developments that, while bringing new opportunities to society, are also often exploited by malicious actors and criminals.

In order to tackle evolving threats effectively, President von der Leyen[19] has stressed the need for a comprehensive approach based on a common threat assessment. The **Strategic Compass** presented by the High Representative in November 2021, and planned to be agreed by Member States in March 2022, will be a guiding document for the EU's security and defence policies. Based on the first-ever EU comprehensive Threat Analysis conducted in 2020, the Strategic Compass sets out the way forward to enhance the EU's strategic autonomy and to become a stronger global partner. It defines concrete objectives and deliverables for the next 5 to 10 years, on how to act quickly when facing crises, secure our citizens against fast-changing threats, invest in the capabilities we need, and partner with others to achieve common goals.

The experience of the COVID-19 pandemic has shown that **foreign information manipulation and interference** is a serious and growing security threat. It can jeopardise the values enshrined in the EU Treaties, in particular democratic institutions and processes, and undermine fundamental rights and freedoms. The EU is active in detecting, analysing and exposing foreign information manipulation and interference, and works closely with third countries and international partners (in particular the G7 and NATO) to build up capabilities. Following the European Democracy Action Plan[20], the European External Action Service is currently developing a toolbox for countering foreign information manipulation and interference, in close cooperation with the European Commission. The Commission presented on 25 November a number of initiatives to reinforce democracy and integrity of

[18] COM (2021) 718 and COM (2021) 719.
[19] State of the Union 2021, Address by President Ursula von der Leyen, 15 September 2021.
[20] COM (2020) 790.

elections. These include a proposal for a Regulation on transparency[21] of political advertising, and two proposals updating the Directives on the electoral rights of "mobile EU citizens"[22].

A striking development concerning hybrid attacks on the EU in the summer of 2021 was an attempt to destabilise the EU through the instrumentalisation of migrants at the EU external border.

The Belarus hybrid attack on the EU

- In summer 2021 Belarus faced sanctions after the forced landing of a passenger plane in May 2021. The regime reacted by facilitating arrivals of irregular migrants to the borders of Lithuania, Latvia and Poland, an action that shows a determined attempt to create a protracted crisis as part of a broader concerted effort to destabilise the EU.
- In addition to exposing migrants to significant personal risk, an important component of the Belarus action to instrumentalise migrants, has been information manipulation. The EU has been monitoring, analysing and exposing foreign information manipulation and interference and sharing its findings with Member States and international partners (NATO and G7) through the Rapid Alert System.
- The Joint Communication on 23 November on responding to the state-sponsored instrumentalisation of migrants at the EU external border[23] set out the robust and varied response of the EU to these events.
- This has included a range of measures including: EU financial support; operational assistance to the affected Member States by EU agencies **Frontex** and **EASO**; diplomatic outreach to countries of origin and transit to avoid their citizens falling into the trap; adoption of sanctions targeting those who facilitate illegal crossings at the external borders of the Union[24]. A draft Regulation has been proposed to restrict the activities of transport operators that facilitate trafficking or smuggling of people to the EU[25]. Extraordinary measures on asylum and returns have been proposed to help the affected Member States respond to the current crisis, in full respect for EU values and standards[26]. The proposed revision of the Schengen Borders Code will also complement this toolbox by defining instrumentalisation in the EU legal framework.

The implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats continues, as described in the fifth annual report[27]. Hybrid threat considerations are being mainstreamed into policy-making, as part of the impact assessment of upcoming EU policy initiatives, in the framework of the Better Regulation Toolbox. The network of Hybrid Points of Contact, which now includes policy officers from across Commission services, the European External Action Service and the European Defence Agency, has been reinforced.

---

21 COM (2021) 731.
22 COM(2021) 732 and COM(2021) 733.
23 JOIN(2021) 32.
24 Council Decision 2021/1990 amending Decision 2012/642/CFSP concerning restrictive measures in view of the situation in Belarus and Council Regulation 2021/1985 amending Regulation No 765/2006 concerning restrictive measures in respect of Belarus, *OJ L 405, 16.11.2021, p. 1–2 and 10.*
25 COM(2021) 753.
26 COM(2021) 752.
27 SWD(2021) 729.

Enhancing situational awareness and building resilience are also key to countering hybrid threats. The **Hybrid Fusion Cell** within the EU intelligence and Situation Centre (EU INTCEN) that operates under the European External Action Service, has produced over 100 written reports on hybrid threats, including six Hybrid Trends Analyses. In order to develop tools to assess the level of preparedness in sectors prone to hybrid threat interference, Commission services and the European External Action Service conducted a **first identification of sectoral baselines,** a first step to track progress in protecting Member States and EU institutions against hybrid threats.

Hybrid threats are also a focus of **EU-NATO cooperation**, based on the Warsaw and Brussels Joint Declarations of 2016 and 2018, that has further intensified during the COVID-19 pandemic[28]. In light of the continuously evolving threats faced by EU Member States and NATO Allies, negotiations are ongoing for a third EU-NATO Joint Declaration.

Chemical, biological, radiological and nuclear (CBRN) risks

Threats of biological, chemical and unknown origin can constitute cross-border threats to health, and be used as hybrid threats or for terrorist purposes. This will be part of the mandate of HERA, with continuous threat assessments, and promoting procurement and manufacturing of relevant medical countermeasures. The EU is also funding (€5 million from the Health Programme) a Joint Action specifically designed to strengthen preparedness and response to biological and chemical terror attacks[29].

Technological challenges

Technologies such as encryption or artificial intelligence may be exploited by malicious actors and criminals. Here, the challenge for policy makers in Europe and beyond, is to strike the right balance between the protection of individual rights and freedoms, ensuring cybersecurity, and ensuring that law enforcement authorities can do their job.

As highlighted in the third report of the Observatory Function on encryption[30], law enforcement and judicial authorities face many challenges to lawfully intercept communications and gather evidence for criminal investigations. In this year's Organised Crime Strategy, the Commission set out its intention to suggest a way forward in 2022 to address the issue of lawful and targeted access to **encrypted information** for criminal investigations and prosecutions. The Commission is conducting a mapping exercise of existing legislation, case law, operational practices and needs in the Member States, to acquire a more thorough understanding of the legal frameworks, current practices, and the needs of the law enforcement, judiciary, and cybersecurity communities.

Discussions on the Commission's proposal for an **Artificial Intelligence** Act have taken place in the Justice and Home Affairs and Telecoms Councils. The Slovenian Presidency has organised workshops, including dedicated workshops on law enforcement, to clarify the most

[28] See Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, 3 June 2021.

[29] The work undertaken by the JA TERROR this consortium will specifically focus on providing knowledge and information to all relevant sectors to support health preparedness and strengthen cross sectoral response (health, security and civil protection) to biological or chemical terror attacks. The group has stakeholders from 18 European countries, with 14 Member States, one EEA member, one candidate country, one potential candidate country and the United Kingdom. Given the shared objectives, HERA will also be working closely with this consortium.

[30] Third report of the observatory function on encryption. 02 July 2021.

complex issues. In June 2021, the European Data Protection Board and the European Data Protection Supervisor published a Joint Opinion on the Commission's proposal[31], calling for a general ban on any use of AI for remote biometric identification systems in public spaces. The European Parliament adopted a resolution on 6 October 2021[32] pointing to the risk of real-time remote biometric identification systems and algorithmic bias in AI applications, and emphasising that human supervision and strong legal powers are needed, especially in law enforcement or border-crossing contexts.

IV. Protecting Europeans from terrorism and organised crime

Terrorism

The Terrorism Situation and Trend Report published by Europol in June 2021[33] indicated that Member States considered that jihadist terrorism remained the greatest terrorist threat in the EU. The report confirms that the most frequent type of jihadism-inspired attacks in the EU, Switzerland and the UK, has been assaults in public places targeting civilians. All completed jihadist attacks in 2020 were committed by individuals acting alone. It also indicates that several suspects arrested in 2020 had online contact with followers of terrorist groups outside the EU. The self-proclaimed Islamic State terrorist group and the al-Qaeda network continued to incite lone-actor attacks in Western countries[34], showing how external and internal security are closely interlinked. In August, the Justice and Home Affairs Council stated that "the EU and its Member States will do their utmost to ensure that the situation in Afghanistan does not lead to new security threats for EU citizens"[35]. Steps have been taken to ensure that all available tools are used to respond to possible threats.

In light of the developments in Afghanistan, the EU Counter Terrorism Coordinator in coordination with the Commission, the European External Action Service, the Presidency and key EU Agencies, drew up **a Counter-Terrorism Action Plan on Afghanistan**[36]. The Action Plan sets out 23 recommendations in four areas: security checks – preventing infiltration; avoiding Afghanistan becoming a safe haven for terrorist groups; monitoring and countering propaganda and mobilisation (e.g. role of Radicalisation Awareness Network); and tackling organised crime as a source of terrorist financing. The Action Plan was welcomed by Member States at the Justice and Home Affairs Council on 8 October 2021. A first achievement has been a voluntary procedure for enhanced security checks on people coming from Afghanistan, which was endorsed by the EU Standing Committee on Internal Security on 22 November 2021. At a technical meeting with members of the Taliban declared interim Afghan government on 28 November 2021 in Doha[37], the EU urged Afghanistan to take determined action to fight all forms of terrorism.

---

31 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

32 European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters.

33 Europol EU Terrorism Situation & Trend Report (Te-Sat), 22 June 2021.

34 Europol EU Terrorism Situation & Trend Report (Te-Sat), 22 June 2021.

35 Statement on the situation in Afghanistan, 11385/21, 31 August 2021.

36 Afghanistan: Counter-Terrorism Action Plan, 29 September 2021.

37 This dialogue does not imply recognition by the EU of the interim government but is part of EU's operational engagement, in the interest of the EU and the Afghan people.

The Commission continues its work on the implementation of the Counter-Terrorism Agenda. **An evaluation of the Directive on combatting terrorism**[38] was adopted on 18 November 2021[39] with a generally positive assessment. However, there are issues limiting performance, for instance, difficulties in proving terrorist intent, or in some Member States, challenges around the classification of violent extreme right-wing acts as acts of terrorism.

Finally, obstacles to effective cooperation and coordination between Member States remain as regards **the protection and assistance provided to victims of terrorism**. The Commission is currently further assessing the transposition of the Directive into national law and has opened infringement procedures against 24 Member States since July 2021 for failing to adequately transpose the directive. The pilot project of EU Centre of expertise for victims of terrorism[40] has been assisting Member States and national victim support organisations in practical application of the EU rules on victims of terrorism. Results of this pilot project include the EU Handbook on victims of terrorism, national handbooks and more than 750 participants taking part in national training activities.

The Commission constantly supports Member State efforts to better protect public spaces. A second Digital Autumn School on the Protection of Public Spaces has been held and stakeholders are updated on best practice[41].

To better prevent terrorism, the fight against radicalisation, both offline and online, needs to continue. In October 2021, the **Radicalisation Awareness Network (RAN)** celebrated its 10th year of radicalisation prevention, with a conference focussing on the changing nature of the challenges in this field. Regarding the fight against online radicalisation, on 5 November 2021, **Europol,** in cooperation with the Commission, organised a tabletop exercise to test the implementation of the EU Crisis Protocol[42]. The exercise took place in the framework of the EU Internet Forum and examined cooperation between government authorities and the tech industry to contain the viral spread of terrorist and violent extremist content online.

Since the security of our partners and neighbours is essential to ensure Europe's own internal security, the European External Action Service and the Commission work closely with key third countries and international organisations, through regular **counter-terrorism dialogues** to enhance our cooperation on security and counter-terrorism issues. At the same time, a number of agreements are put in place to facilitate the exchange of information and of personal data which in turn enables a more operational cooperation via Europol.

Counter-terrorism dialogues with third countries/international organisations between July and December 2021

Central Asia High-level Political and Security dialogue (July 2021)
- New Zealand Joint Cooperation Committee, EU-NZ Strategic Dialogue (July 2021)
- Maldives Senior Officials meeting CT section (September 2021)

[38] Directive 2017/541 of 15 March 2017 on combating terrorism, OJ L 88/6, 15.3.2017.
[39] COM (2021)701 final.
[40] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights/eu-centre-expertise-victims-terrorism_en.
[41] See Newsletter on the Protection of Public Spaces: https://europa.eu/!jV87NK.
[42] The EU Crisis Protocol, adopted by the Justice and Home Affairs Ministers in October 2019, is a voluntary mechanism that allows EU Member States and online platforms to respond rapidly and in a coordinated manner to the dissemination of terrorist content online in the event of a terrorist attack, while ensuring strong data protection and fundamental rights safeguards.

- Bosnia and Herzegovina CT Dialogue (October 2021)
- Turkey CT Dialogue (25 November 2021)
- EU-NATO CT dialogue (15 November 2021)

Europol agreements with third countries on the exchange of personal data

- Europol agreement with New Zealand concluded on 28 September 2021
- First round of negotiations with Israel took place on 22 November 2021

Europol strategic cooperation agreements

- Europol signed a strategic cooperation agreement with Armenia on 16 September 2021

There is particularly intense co-operation on counter terrorism and the prevention of radicalisation with the Western Balkans, in the framework of the 2018 Joint Action Plan on Counter-Terrorism with the Western Balkans[43]. Work on the implementation of the six Implementing Arrangements with each Western Balkan partner continues at a steady pace. The EU-Western Balkans summit in Slovenia in October 2021 underlined the importance of taking resolute action to address terrorism and radicalisation, serious and organised crime, in particular trafficking of human beings, migrant smuggling, money laundering, drug cultivation and trafficking, as well as corruption, illegal firearms trafficking, cyber and hybrid threats.

On 20 July 2021, the Commission presented an ambitious package of legislative proposals to strengthen the **EU's anti-money laundering and countering the financing of terrorism (AML/CFT) rules**[44], including measures regarding crypto-assets to align with the latest international standards developed by the Financial Action Task Force (FATF). For instance, all Crypto-Asset Services Providers (CASPs) will be brought within the scope of EU anti-money laundering legislation, requiring them to report any suspicious transactions effected by their customers. The Commission also proposes to ban the provision of anonymous crypto-assets wallets by CASPs. The package is part of the Commission's commitment to protect individuals in the EU and the EU's financial system from terrorist financing. The aim is to improve the detection of suspicious transactions and activities, and close loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system.

New recent regulations on customs controls on cash entering and leaving the Union[45] and on the import of cultural goods[46] are now in the implementation phase[47] (partial implementation for the latter, pending the development of the related centralized IT system). Those

[43] In October 2018, the Commission and representatives of Albania, Bosnia and Herzegovina Kosovo*, Montenegro, North Macedonia, and Serbia, signed a .Joint Action Plan on Counter-Terrorism for the Western Balkans.

[44] COM(2021) 421 final, COM(2021) 420 final, COM(2021) 423 final, COM(2021) 422 final.

[45] Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union, OJ L 284, 12.11.2018, p. 6–21

[46] Regulation (EU) 2019/880 of 17 April 2019 on the introduction and the import of cultural goods, OJ L 151, 7.6.2019, p. 1–14

[47] COM Implementing Regulation 2021/1079 for the purposes of EP and Council Regulation 2019/880 on the introduction and the import of cultural goods (adopted by Commission on 24.06.2021) and COM Implementing Decision on the criteria for the common risk management framework on cash movements for the purposes of EP and Council Regulation 2018/1672 on controls on cash entering or leaving the Union (adoption expected in December 2021).

regulations will contribute to the fight against money laundering and to the protection of cultural heritage, but will also play a role in enhancing the fight against terrorism financing.

Organised crime

Crime trends observed by Europol during the COVID-19 pandemic show that, despite lockdowns and restrictions, serious and organised crime remain active, adapt, and exploit all circumstances to make a profit. While legal economies have weakened, the criminal economy has been getting stronger. International law enforcement cooperation shows on a daily basis the global scale of organised crime networks and the degree of connectivity among criminals. International engagement on countering organised crime, including further steps to develop partnerships and cooperation with countries in the immediate neighbourhood and beyond, is needed to address this transnational challenge.

The trade in **illicit drugs** remains the largest criminal market in the EU. The EU Drugs Action Plan 2021-2025 was adopted at the beginning of July, following the Strategy published in December 2020. EU National Drugs Coordinators met on 22 September to discuss prevention. The **European Monitoring Centre for Drugs and Drug Addiction** (EMCDDA) presented its latest analysis of the drug situation in Europe in the European Drug Report 2021 in June[48] and released a report in September highlighting the increasing production of methamphetamine in Afghanistan[49]. **Europol** is stepping up cooperation with the Iranian and Turkish authorities to enhance intelligence on drugs trafficking. According to Europol, the main heroin trafficking route inside the EU is still through the Balkans while cocaine trafficking most commonly takes place through container ports such as Antwerp or Rotterdam. Europol is building a new platform on drugs to update EU Member States on developments on a weekly basis.

Cooperation with international partners is key in the fight against drugs. Recent contacts have included an EU-US dialogue in September 2021, the EU-Western Balkans Dialogue on Drugs in October, and the EU-CELAC coordination and cooperation mechanism on drugs in June. An EU-Iran dialogue as well as an EU-Colombia dialogue on drugs are to be established.

The 2020-2025 EU action plan against **firearms trafficking**[50] makes clear that the full implementation of the Firearms Directive is a top priority. The Commission report of October 2021 assesses application of the Directive on control of the acquisition and possession of weapons[51], noting that the Firearms Directive improved the categories of firearms, their traceability, exchanges of information and administrative procedures. However, so far only 10 Member States have fully transposed the Directive. The report underlines that there is room for further progress in the legal control of acquisition, possession and movements of civilian weapons. The Commission will therefore conduct an impact assessment on the possible modifications to the Firearms Directive. There are around 35 million illegal firearms in the EU and many are smuggled across our borders. Cooperation with the Western Balkans is key. An EU-Western Balkans ministerial conference on firearms took place in September

[48] https://www.emcdda.europa.eu/publications/edr/trends-developments/2021_en.
[49] https://www.emcdda.europa.eu/publications/ad-hoc-publication/methamphetamine-from-afghanistan-signals-indicate-europe-should-be-better-prepared_en.
[50] COM (2020) 608 final.
[51] COM (2021) 647 final.

2021, which underlined the close cooperation between the EU and the Western Balkans against firearms trafficking, working within the European Multidisciplinary Platform Against Criminal Threats (**EMPACT**). Since the adoption of the Regional Roadmap for comprehensive Small Arms and Light Weapons in 2018, there has been steady progress by Western Balkan partners in the harmonisation of legal frameworks with EU and UN firearms rules, as well as an increase in operational cooperation and information exchange with the EU and its agencies.

Waste trafficking[52] is one of the most serious forms of environmental crime. Up to 30% of waste shipments worth are illegal, worth €9.5 billion annually. The Commission adopted the revised Regulation on waste shipments on 17 November 2021, which will further strengthen action against waste trafficking by setting up an EU Waste Shipment Enforcement Group, empowering the European Anti-Fraud Office OLAF to support transnational investigations by Member States on waste trafficking, and providing stronger rules on administrative penalties.

The **fight against corruption** is key to ensuring a strong rule of law and preserving citizens' trust in public institutions. The strong link between organised crime and corruption, as well as the risk of infiltration of the licit economy and public institutions are key challenges. The second Rule of Law report, published on 20 July 2021[53], highlighted that while EU Member States continue to be among the best performers globally in the fight against corruption, challenges remain, in particular as regards criminal investigations, prosecutions and the application of sanctions for corruption in some Member States. While many Member States took measures to strengthen the corruption prevention and integrity frameworks, including rules on conflicts of interests, lobbying transparency and revolving doors, the resources allocated to anti-corruption fall short in some Member States. Concerns about the effectiveness of investigations, prosecution and adjudication of high-level corruption cases persist in others.

It is also essential to prevent **fraud against the EU budget**. The European Parliament issued on 26 October two reports[54] noting with concern that the COVID-19 pandemic created new opportunities for fraudsters and organised crime, and drawing attention to the importance of preventive measures in anticipating and responding to the risks of corruption in crisis situations, as well the need for increased transparency in the Union's financial environment. In September 2021, less than four months since the start of its activities, the European Public Prosecutor Office (EPPO) has already achieved remarkable results, opening investigations into cases of alleged fraud for an estimated total of some €4.5 billion[55]. On 15 October 2021, Europol set up Operation Sentinel, a new EU-wide operation that will target fraud against funds being offered under the framework of the NextGenerationEU initiative. It involves EPPO, Eurojust, OLAF and 23 Member States. The activities will run for at least a year, and will focus on proactive intelligence sharing, information exchange, and supporting the

---

52 COM (2021) 709 final.

53 COM(2021) 700 final.

54 Report on "The evaluation of preventive measures for avoiding corruption, irregular spending and misuse of EU and national funds in case of emergency funds and crisis-related spending areas (2020/2222(INI)), and Report on "The impact of organised crime on own resources of the EU and on the misuse of EU funds with a particular focus on shared management" (2020/2221(INI))

55 'Estimated damages to EU budget in ongoing EPPO investigations: almost €4.5 billion' available at https://www.eppo.europa.eu/en/news/estimated-damages-eu-budget-ongoing-eppo-investigations-almost-eu45-billion.

coordination of operations to tackle fraud against the Recovery and Resilience Facility in particular.

Smuggling of migrants is a criminal activity that seeks to prey on the vulnerable. 50% of people-smugglers are poly-criminals, engaged in other forms of criminal activity. Preventing and fighting migrant smuggling is a key objective of the EU Security Union Strategy, the EU Strategy to tackle Organised Crime, the EU Strategy on Combatting Trafficking in Human Beings (2021-2025) and the New Pact on Migration and Asylum, that requires continuous international cooperation and coordination. Building on the progress made by the first EU action plan against migrant smuggling (2015-2020), the Commission, working together with the High Representative, has adopted a renewed EU action plan for the period 2021-2025[56].

Key themes of the EU action plan against migrant smuggling (2021-2025)

- Develop **Anti-Smuggling Operational Partnerships** with concrete tools as part of comprehensive, balanced, tailor-made and mutually beneficial migration partnerships, further building on trust and mutual cooperation.
- Improve the implementation of the legal frameworks for sanctioning smugglers and for the protection from exploitation.
- Strengthen judicial cooperation on migrant smuggling by inviting EU Member States to make more use of **Eurojust,** support cross-border investigations, through Joint Investigation Teams and make best use of the Focus Group of prosecutors on migrant smuggling.
- Respond to **evolving online practices** and tools that facilitate smuggling, through enhanced operational cooperation and information exchange between national authorities and EU agencies.
- Increase **research and data collection** for a better understanding of migration trends, the nature and span of criminal networks, the impact of anti-smuggling policies and the 'modus operandi' of criminal networks.

On 4-5 November 2021, **Eurojust** held its annual meeting on migrant smuggling, which also provided an opportunity to enhance cooperation on this with the Western Balkans and the South Partners Countries of the Mediterranean Basin, participating in EuroMed Justice. In the last six months of 2021, Eurojust also supported several large scale operations against migrant smuggling[57].

Following the **Strategy on Combatting Trafficking in Human Beings**[58], the Commission is carrying out an evaluation of the Anti-trafficking Directive[59] including a consideration of minimum EU rules that could criminalise the use of exploited services of trafficking victims. The 15th EU Anti-Trafficking Day took place on 18 October 2021, to raise awareness about

[56] COM(2021) 591.

[57] See for instance link to the Press Release: https://www.eurojust.europa.eu/people-smuggling-network-netherlands-and-hungary-dismantled.

[58] COM(2021) 171.

[59] Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims. , OJ L 101, 15.4.2011.

this crime. On the same day, the JHA Agencies' Network published a joint report[60] on the identification and protection of victims of human trafficking. In November 2021, **Europol** and **Frontex** coordinated supported a large-scale international action against trafficking in human beings. 29 countries, led by Austria and Romania, took part in the action days with more than 14 000 law enforcement officers targeting trafficking routes on roads and at airports, resulting in 212 arrests and the identification of a further 89 trafficking suspects.

The **sexual abuse of children** both online and offline is one of the most serious crimes, and an ongoing priority for the EU and its Member States. On 12 November 2021, Ministers of Home Affairs discussed policies and practices aimed at raising awareness of and preventing this offence, the tools needed for the successful investigation of this crime in full respect of fundamental rights of all users concerned, and ways to ensure protection of victims, with a strong emphasis on the rights of the child. The temporary legislation to ensure that online service providers can continue their voluntary practices to detect and report child sexual abuse online[61], and to remove child sexual abuse material from their systems, entered into force on 3 August 2021. The Commission continues to take forward the work on the implementation of the initiatives announced in the EU Strategy for a more effective fight against child sexual abuse and the EU Comprehensive Strategy on the Rights of the Child and is also preparing longer-term legislation to fight child sexual abuse online more effectively.

V. A strong European security ecosystem

Enhanced police cooperation across the EU, as well as strong external borders, are essential elements of an EU without internal border controls. Given the cross-border nature of fighting crime and enhancing security, Member States must increasingly rely on one another. However, obstacles remain for data exchange between law enforcement authorities in different EU Member States, which lead to blind spots that can be exploited by criminals and terrorists acting in more than one Member State[62]. To better support Member States, the Commission is presenting a package of measures on police cooperation.

The **Police Cooperation package** includes:

- **Proposal for a Directive on information exchange between law enforcement authorities of Member States**[63]: the objectives are (i) to facilitate equivalent access for law enforcement authorities to information available in another Member State, (ii) to ensure that all Member States have an effective functioning Single Point of Contact, (iii) to establish the secured information exchange network application of Europol (SIENA) as the default communication channel for law enforcement information exchanges between Member States.
- **Proposal for Council recommendation on operational police cooperation**[64]: the objectives are to enhance operational cross-border police co-operation through the

[60] Joint report of the JHA agencies' network on the identification and protection of victims of human trafficking | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu).
[61] COM (2020) 568.
[62] More than more than 70% of organised crime groups are present in more than three Member States according to the 2021 Europol SOCTA report.
[63] COM (2021) 782.
[64] COM (2021) 780.

adoption of common EU minimum standards for cooperation tools in areas such as cross border hot pursuits, joint patrols and joint operations.

- **Proposal for a Regulation on Prüm II**[65]: the objective is to revise the current Prüm framework on the automated exchange of data including by (i) adding the categories of police records and facial images, (ii) providing a technical solution (a central router) for more efficient automated exchange of data between law enforcement authorities, and (iii) ensuring that relevant data from Europol's database is available to Member States law enforcement authorities.

Europol is critical to police cooperation against terrorism and organised crime. Swift agreement on the proposal to amend the Europol regulation[66] would allow Europol to better support Member States in fighting organised crime and terrorism.

Cooperation at international level between law enforcement authorities is key to our internal security. The Council adopted a negotiation mandate for an agreement between the EU and **Interpol** in July. Negotiations should start in December 2021.

To further support Member States' investigations on counter terrorism and organised crime, as well as to facilitate judicial cooperation, the Commission adopted a **Digital Justice Package** on 1 December 2021.

The **Digital justice package** includes:

- **Proposal on Digital information exchange on cross-border terrorism cases**[67]: the objective is to improve the functioning of the Counter Terrorism Register set up in October 2019. It will enable **Eurojust** to fulfil a stronger, more proactive role in supporting coordination and cooperation between the national investigating and prosecuting authorities in relation to terrorist offences.
- **Proposal establishing a cooperation platform to support the functioning of Joint Investigation Teams (JITs)**[68]: the objective is to further increase the efficiency and effectiveness of JITs. It will enable secure electronic communication and exchange of information and evidence among the competent national authorities as well as Union bodies, offices and agencies involved in the respective JITs.
- **Proposal on the digitalisation of cross-border judicial cooperation and access to justice in civil, commercial and criminal matters**[69]: the proposal seeks to ensure effective access to justice of natural and legal persons, and to facilitate judicial cooperation between the Member States, by providing a legal basis for the use of modern digital technologies for communication in the context of cross-border judicial proceedings in civil, commercial and criminal matters.

Better synergies between security and defence, will enhance the effectiveness of our action to support Member States in these fields. The Commission has begun implementation of the Action Plan on **Synergies between Civil, Defence and Space industries**[70] adopted in February 2021**.** It is working with EU agencies, including in particular the European Defence

[65] COM (2021) 784.
[66] COM (2020) 796.
[67] COM(2021) 757.
[68] COM(2021) 756.
[69] COM(2021) 759.
[70] COM (2021) 70 final.

Agency, on fostering capability-driven approaches across security sectors, and on promoting synergies by improving coordination of EU programmes and instruments. In addition, the Commission is publishing a Staff Working Document on "Enhancing security through research and innovation". This document highlights on one hand the strategic role of security research in supporting the achievement of the different civil security policy objectives and, on the other, illustrates the measures being put in place to enable an optimal uptake of innovation from research in tools and services available to European and national security authorities.

As regards EU funding for security, the Work Programme of the Internal Security Fund for 2021-2022 was adopted on 26 November 2021. This will contribute to actions in a number of areas such as information exchange, cross-border cooperation, preventing and combating organised crime, terrorism and radicalisation offline as well as online. On 10 November 2021, the Commission adopted work programmes for the Digital Europe Programme. Among these, the work programme on cybersecurity, with funding amounting to EUR 269 million, will be implemented by the Commission on behalf of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) with the Network of National Coordination Centres[71]. This programme will see investments in building up advanced cybersecurity equipment, tools and data infrastructures. It will fund the development and best use of knowledge and skills related to cybersecurity, promote best practice and ensure wide deployment of state–of-the-art cybersecurity solutions across the European economy.

Speedy and full implementation of legislation that has been adopted, is key for the effectiveness of the Security Union. In its infringement decisions, the European Commission pursues legal action against Member States who do not comply with their obligations under EU law, including legislation under the Security Union. On 2 December, the Commission decided to launch proceedings[72] against various Member States for failing to transpose or implement certain elements of EU rules on combating terrorism, combating racism and xenophobia, the European Arrest Warrant, the exchange of criminal records information, and the fight against fraud to the Union's financial interests by means of criminal law.

The role of EU Agencies and bodies

EU Agencies and bodies have continued to play a crucial role in fostering cooperation and information exchange across the Union and fighting against crime. During the reporting period, many of their activities have focused on promptly answering the operational needs resulting from the Afghan crisis, but also other pressing security challenges, like hybrid threats, ransomware, and organised crime.

Examples of operational activities by EU agencies

- In October 2021, cooperation activities coordinated by **Europol** and **Eurojust** were central to targeting ransomware attacks against critical infrastructure and identifying a number of threat actors that affected over 1800 victims in 71 countries[73].
- In July 2021, **Europol** celebrated the fifth anniversary of the No More Ransom initiative, which helped more than 6 million companies and individuals to recover

[71] Until the ECCC has the capacity to implement its own budget, the European Commission will implement the actions under this Work Programme in direct management on behalf of the ECCC.

[72] https://ec.europa.eu/commission/presscorner/detail/en/INF_21_6201

[73] https://www.eurojust.europa.eu/12-targeted-involvement-ransomware-attacks-against-critical-infrastructure.

their files for free, preventing almost a billion euros from being paid to cyber criminals.

- **ENISA**'s role in the field of operational cooperation was consolidated with the goal of enabling the CSIRTs Network[74], CyCLONe[75] and all actors involved in the EU to collaborate and respond to large-scale attacks. By coordinating both the secretariats of the EU CyCLONe and the CSIRTs Network, ENISA aims to synchronise the technical and operational levels and all EU actors involved in the response.

Co-operation between agencies also plays an important role: for example with the agreement concluded on 22 November between **Frontex**, and the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom Security and Justice, (**eu-LISA**).

Most agencies are developing an external dimension to their activities. International cooperation and this external dimension are key to address the security challenges the agencies are mandated to focus on. The implementation of this external dimension is undertaken in close consultation and coordination with other external actors and programmes, including Common Security and Defence (CSDP) action, in order to avoid duplication, to enable cooperation and to enhance effectiveness.

Role of EU Agencies in responding to the situation in Afghanistan and the region

- The EU agencies ensure constant monitoring of the situation in Afghanistan and the region and contribute to the situational awareness and to a dynamic exchange of information on Afghanistan in the context of the EU Migration Preparedness and Crisis Management Network (Blueprint Network).
- On 31 August, the European Police Agency (**Europol**) issued a report on the potential impact of developments in Afghanistan affecting EU internal security, in the fields of terrorism, organised crime, migrant smuggling. Europol also started an internal working group of experts to monitor the crisis and to share relevant and reliable information.
- The European Asylum Support Office (**EASO**) published an updated Country of Origin Information Report on the security situation in Afghanistan and activated support activities regarding both the internal and external dimensions of the crisis.
- The European Border and Coast Guard Agency (**Frontex- ECBG**) has monitored the situation and coordinated joint operations of Member States with third countries with the aim of enhancing border security, operational cooperation and information exchange.

EU agencies and bodies, in addition to operational actions described in the report, have issued a large number of valuable reports and guidelines since the last Security Union progress report, which can be found listed in annex.

[74] The CSIRTs Network is a network composed of EU Member States' appointed Computer Security Incident Response Team (CSIRTs) and the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU).

[75] The Cyber Crisis Liaison Organisation Network.

VI. Conclusion

The EU continues to show it can adapt and rise to new challenges as they emerge, and this is very evident in the field of security. Whether supporting Member States in the face of new hybrid threats on the EU's external border, or working with international partners to present a co-ordinated response to the constantly evolving threats arising from new technologies, the EU is keeping up-to-date to protect its Member States. At the same time, more conventional security risks continue to be met with EU level solutions and preventive action.

Ensuring the security of Europe as a whole is a common responsibility, where every actor has to play its part, from the European Parliament and the Council adopting new fit-for-purpose and effective rules, to the timely implementation of EU legislation by Member States, and the operational work carried out on the ground by a variety of authorities, organisations and stakeholders. The Security Union will continue to coordinate a very wide diversity of tools and actors in the interests of EU citizens.