Council of the European Union

Brussels, 30 July 2020
(OR. en)

10010/20

JAI 624	**DROIPEN 61**
COSI 121	**COPEN 215**
ENFOPOL 190	**FREMP 51**
ENFOCUSTOM 95	**JAIEX 72**
IXIM 79	**CFSP/PESC 644**
CT 61	**COPS 256**
CRIMORG 66	**HYBRID 20**
FRONT 207	**DISINFO 16**
ASIM 55	**TELECOM 121**
VISA 84	**DIGIT 63**
CYBER 140	**COMPET 347**
DATAPROTECT 71	**RECH 286**
CATS 56	

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	27 July 2020
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2020) 605 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy

Delegations will find attached document COM(2020) 605 final.

Encl.: COM(2020) 605 final

EUROPEAN
COMMISSION

Brussels, 24.7.2020
COM(2020) 605 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on the EU Security Union Strategy

I. Introduction

The Commission's Political Guidelines made clear that we can leave no stone unturned when it comes to protecting our citizens. Security is not only the basis for personal safety, it also protects fundamental rights and provides the foundation for confidence and dynamism in our economy, our society and our democracy. Europeans today face a security landscape in flux, impacted by evolving threats as well as other factors including climate change, demographic trends and political instability beyond our borders. Globalisation, free movement and the digital transformation continue to bring prosperity, make our lives easier, and spur innovation and growth. But alongside these benefits come inherent risks and costs. They can be manipulated by terrorism, organised crime, the drugs trade and human trafficking, all direct threats to citizens and our European way of life. Cyber-attacks and cybercrime continue to rise. Security threats are also becoming more complex: they feed on the ability to work cross-border and on inter-connectivity; they exploit the blurring of the boundaries between the physical and digital world; they exploit vulnerable groups, social and economic divergences. Attacks can come at a moment's notice and may leave little or no trace; both state and non-state actors can deploy a variety of hybrid threats[1]; and what happens outside the EU can have a critical impact on security inside the EU.

The COVID-19 crisis has also reshaped our notion of safety and security threats and corresponding policies. It has highlighted the need to guarantee security both in the physical and digital environments. It has underlined the importance of open strategic autonomy for our supply chains in terms of critical products, services, infrastructures and technologies. It has reinforced the need to engage every sector and every individual in a common effort to ensure that the EU is more prepared and resilient in the first place and has better tools to respond when needed.

Citizens cannot be protected only through Member States acting on their own. Building on our strengths to work together has never been more essential, and the EU has never had more potential to make a difference. It can lead by example, by enhancing its overall crisis management system and working within and outside its borders to contribute to global stability. While primary responsibility for security lies with Member States, recent years have brought an increasing understanding that the security of one Member State is the security of all. The EU can bring a multidisciplinary and integrated response, helping security actors in Member States with the tools and the information they need.[2]

The EU can also ensure that security policy remains grounded in our common European values – respecting and upholding the rule of law, equality[3] and fundamental rights and guaranteeing transparency, accountability and democratic control – to give policies the right foundation of trust. It can build an effective and genuine Security Union in which the rights and freedoms of individuals are well protected. Security and respect for fundamental rights are not conflicting aims, but consistent and complementary. Our values and fundamental rights must be the basis of security policies, ensuring the principles of necessity,

---

1 While definitions of hybrid threats vary, it aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives (while remaining below the threshold of formally declared warfare). See JOIN(2016) 18 (final).

2 For example through the services delivered by the EU's space programme such as Copernicus, providing Earth observation data and applications for border surveillance, maritime security, law enforcement, anti-piracy, drug-smuggling deterrence and emergency management.

3 A Union of Equality: Gender Equality Strategy 2020-2025, COM(2020) 152.

proportionality and legality, and with the right safeguards for accountability and judicial redress, while enabling an effective response to protect individuals, particularly the most vulnerable.

Significant legal, practical and support tools are already in place, but need to be both strengthened and better implemented. Much progress has been made to improve the exchange of information and intelligence cooperation with Member States and to close down the space in which terrorists and criminals operate. But fragmentation remains.

The work must also go beyond the EU's boundaries. Protecting the Union and its citizens is no longer only about ensuring security within the EU borders, but also about addressing the external dimension of security. The EU's approach to external security within the framework of the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP) will remain an essential component of EU efforts to enhance security within the EU. Cooperation with third countries and at global level to address common challenges is central to an effective and comprehensive response, with stability and security in the EU's neighbourhood critical to the EU's own security.

Building on the previous work of the European Parliament[4], Council[5] and the Commission[6], this new strategy shows that a genuine and effective Security Union needs to combine a strong core of instruments and policies to deliver security in practice with a recognition that security has implications for all parts of society and all public policies. The EU needs to ensure a secure environment for everyone, whatever their racial or ethnic origin, religion, belief, gender, age or sexual orientation.

This Strategy covers the period 2020-2025 and focuses on building capabilities and capacities to secure a future-proof security environment. It sets out a whole-of-society approach to security that can effectively respond to a rapidly-changing threat landscape in a coordinated manner. It defines strategic priorities and the corresponding actions to address digital and physical risks in an integrated manner across the whole Security Union ecosystem, concentrating on where the EU can bring further value. Its goal is to offer a security dividend to protect everyone in the EU.

II. A rapidly changing European security threat landscape

The safety, prosperity and well-being of citizens depend on being secure. The threats to that security depend on the extent to which their lives and livelihoods are vulnerable. The greater the vulnerability, the greater the risk that it can be exploited. Both vulnerabilities and threats are in a state of constant evolution, and the EU needs to adapt.

Our daily lives depend on a wide variety of services – such as energy, transport, and finance, as well as health. These rely on both physical and digital infrastructure, adding to the vulnerability and the potential for disruption. During the COVID-19 pandemic, new technologies have kept many businesses and public services running, whether keeping us connected through remote working or maintaining the logistics of supply chains. But this

[4] For example, the work of the European Parliament's TERR committee which reported in November 2018.

[5] From the Council Conclusions of June 2015 on a "renewed internal security strategy "to the more recent Council outcomes of December 2019.

[6] "Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union" COM(2016) 230 final, 20.4.2016. See the recent appraisal of the implementation of legislation in the internal security field: Implementation of Home Affairs legislation in the field of internal security - 2017-2020 (SWD(2020) 135).

has also opened the door to an extraordinary increase in malicious attacks, attempting to capitalise on the disruption of the pandemic and the shift to digital home working for criminal purposes.[7] Shortages of goods have created new openings for organised crime. The consequences could have been fatal, disrupting essential health services at a time of the most intense pressure.

The ever-increasing ways in which digital technologies benefit our lives has also made the **cybersecurity** of technologies an issue of strategic importance.[8] Homes, banks, financial services and enterprises (notably small and medium enterprises) are heavily affected by cyber-attacks. The potential damage is multiplied still further by the interdependence of physical and digital systems: any physical impact is bound to affect digital systems, while cyber-attacks on information systems and digital infrastructures can bring essential services to a halt.[9] The rise of the Internet of things and the increased use of artificial intelligence will bring new benefits as well as a new set of risks.

Our world relies on digital infrastructures, technologies and online systems, which allow us to create business, consume products and enjoy services. All rely on communicating and interaction. Online dependency has opened the door to a wave of **cybercrime**.[10] 'Cybercrime-as-a-service' and the underground cybercriminal economy give easy access to cybercrime products and services online. Criminals quickly adapt to use new technologies to their own ends. For example, counterfeit and falsified medicines have infiltrated the legitimate supply chain of pharmaceuticals.[11] The exponential growth of child sexual abuse material online[12] has shown the social consequences of changing patterns of crime. A recent survey showed that most people in the EU (55 %) are concerned about their data being accessed by criminals and fraudsters.[13]

The **global environment** also accentuates these threats. Assertive industrial policies by third countries, combined with the continued cyber-enabled theft of intellectual property, are changing the strategic paradigm for protecting and advancing European interests. This is accentuated by the rise of dual-use applications – making a strong civilian technology sector a strong asset for defence and security capability. Industrial espionage has a significant impact on the EU's economy, jobs and growth: cyber theft of trade secrets is estimated to cost the EU €60 billion[14]. This calls for a thorough reflection of how dependencies and the increased exposure to cyber threats affect the EU's capacity to protect individuals and businesses alike.

---

7 Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (April 2020).

8 Commission Recommendation on the Cybersecurity of 5G networks, C(2019) 2335; Communication on Secure 5G deployment in the EU - Implementing the EU toolbox, COM(2020) 50.

9 In March 2020 the Brno University Hospital in Czechia suffered a cyber attack which forced it to reroute patients and postpone surgery (Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis). Artificial intelligence may be misused for digital, political and physical attacks as well as surveillance. Internet of Things data collection can be used for the surveillance of individuals (smart watches, virtual assistants, etc.).

10 According to some projections, costs of data breaches will reach $5 trillion annually by 2024, up from $3 trillion in 2015 (Juniper Research, The Future of Cybercrime & Security).

11 One 2016 study (Legiscript) estimated that globally only 4% of internet pharmacies operate lawfully, with EU consumers top targets for the 30,000-35,000 illicit online pharmacies active online.

12 EU Strategy for a more effective fight against child sexual abuse, COM(2020) 607.

13 European Union Agency for Fundamental Rights (2020), Your rights matter: Security concerns and experiences, Fundamental Rights Survey, Luxembourg, Publications Office.

14 The scale and impact of industrial espionage and theft of trade secrets through cyber, 2018.

The COVID-19 crisis has also underlined how social divisions and uncertainties create a security vulnerability. This increases the potential for more sophisticated and **hybrid attacks** by state and non-state actors, with vulnerabilities exploited through a mix of cyber-attacks, damage to critical infrastructure[15], disinformation campaigns, and radicalisation of the political narrative.[16]

At the same time, more long-established threats continue to evolve. There was a downward trend in **terrorist attacks** in the EU in 2019. However, the threat to EU citizens of jihadist attacks from or inspired by Da'esh and al-Qaeda and their affiliates remains high.[17] In parallel, the threat of violent right wing extremism is also growing.[18] Attacks inspired by racism must be a cause for serious concern: the deadly anti-Semitic terror attacks in Halle were a reminder of the need to step up the response in line with the 2018 Council Declaration.[19] One in five people in the EU are very worried about a terrorist attack in the next 12 months.[20] The vast majority of recent terrorist attacks were "low tech" attacks, lone actors targeting individuals in public spaces, while terrorist propaganda online took on a new significance with the live streaming of the Christchurch attacks.[21] The threat posed by radicalised individuals remains high – potentially bolstered by returning foreign terrorist fighters and by extremists released from prison.[22]

The crisis has also shown how existing threats can evolve in new circumstances. **Organised crime** groups have exploited shortages of goods providing an opening to create new illicit markets. The trade in illicit drugs remains the largest criminal market in the EU, estimated at a minimum retail value of €30 billion per year in the EU.[23] Trafficking in human beings persists: estimates show an annual global profit for all forms of exploitation of almost €30 billion.[24] International trade in counterfeit pharmaceuticals reached €38.9 billion.[25] At the same time, low rates of confiscation allow criminals to continue expanding their criminal activities and infiltrating the legal economy.[26] Criminals and terrorists find it easier to access firearms, from the online market and through new technologies such as 3-D printing.[27] Use of Artificial Intelligence, new technologies and robotics will further increase the risk that criminals exploit the benefits of innovation for malicious ends[28].

---

15 Critical infrastructures are essential for vital societal functions, health, safety, security, economic or social well-being, whose disruption/destruction has a significant impact (Council Directive 2008/114/EC).

16 97% of EU citizens have been confronted to fake news, 38% on a daily basis. See JOIN (2020) 8 final.

17 A total of 119 completed, failed and foiled terrorist attacks were reported by 13 EU Member States, with ten deaths and 27 injuries (Europol, European Union Terrorism Situation and Trend Report, 2020).

18 2019 saw six right-wing terrorist attacks (one completed, one failed, four foiled: three Member States), compared to only one in 2018, with further deaths in cases not classified as terrorism (Europol, 2020).

19 See also the Council Declaration on the fight against antisemitism and the development of a common security approach to better protect Jewish communities and institutions in Europe.

20 EU Agency for Fundamental Rights: Your rights matter: Security concerns and experiences, 2020.

21 From July 2015 until the end of 2019, Europol found terrorist content on 361 platforms (Europol, 2020).

22 Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism, 2019.

23 EMCDDA and Europol EU Drugs Market Report 2019.

24 Europol's Report on Trafficking in Human Beings, Financial Business Model (2015).

25 EU Intellectual Property Office and OECD report on Trade in counterfeit pharmaceutical products

26 Report on Asset recovery and confiscation: Ensuring that crime does not pay, COM(2020) 217.

27 In 2017, firearms were used in 41% of all terrorist attacks (Europol, 2018).

28 In July 2020, French and Dutch law enforcement and judicial authorities, alongside Europol and Eurojust, presented the joint investigation to dismantle EncroChat, an encrypted phone network used by criminal networks involved in violent attacks, corruption, attempted murders and large-scale drug transports.

These threats cut across categories and strike different parts of society in different ways. They all represent a major threat to individuals and businesses and require a comprehensive and coherent response at EU level. When security vulnerabilities can come even from small inter-connected household items such as an internet connected fridge or coffee machine, we can no longer rely on traditional state actors alone to ensure our security. Economic operators must take greater responsibility for the cybersecurity of products and services they place on the market; while individuals too need to have at least a basic understanding of cybersecurity to be able to protect themselves.

III. An EU coordinated response for the whole of society

The EU has already shown how it can bring real added value. Since 2015, the Security Union brought new linkages in the way security policies are addressed at EU level. But more needs to be done to engage the whole of society, including governments at all levels, business in all sectors and individuals in all Member States. The increasing awareness of the risks of dependency[29] and the need for a strong European industrial strategy[30] point to an EU with a critical mass of industry, technology production and supply chain resilience. Strength also means full respect of fundamental rights and EU values: they are a prerequisite of legitimate, effective and sustainable security policies. This Security Union strategy sets out concrete work streams to take forward. It is built around the following common objectives:

- ***Building capabilities and capacities for early detection, prevention and rapid response to crises:*** Europe needs to be more resilient to prevent, protect and withstand future shocks. We need to build capabilities and capacities for early detection and rapid response to security crises through an integrated and coordinated approach, both globally and through sector-specific initiatives (such as for the financial, energy, judiciary, law enforcement, healthcare, maritime, transport sectors) and building on existing tools and initiatives.[31] The Commission will also come forward with proposals for a wide-ranging crisis management system within the EU, which could also be relevant for security.
- ***Focusing on results***: A performance-driven strategy needs to be based around careful threat and risk assessment to target our efforts to best effect. It needs to define and apply the right rules and the right tools. It needs reliable strategic intelligence as a basis for EU security policies. Where EU legislation is required, it needs to be followed up so that it is implemented in full, to avoid fragmentation and gaps left to be exploited. The effective implementation of this Strategy will also depend on securing appropriate funding in the next programming period 2021-2027, including for related EU agencies.
- ***Linking all players in the public and private sectors in a common effort:*** Key players in both the public and private sectors have been reluctant to share security-relevant information, whether for fear of compromising national security or competitiveness.[32]

---

[29] Risks of foreign dependence involve an increased exposure to potential threats, from exploitation of vulnerabilities of IT infrastructures compromising critical infrastructures (e.g. energy, transport, banking, health) or taking control of industrial control systems, to increased capacity for data theft or espionage.

[30] Commission Communication A New Industrial Strategy for Europe, COM(2020) 102.

[31] Such as Integrated Political Crisis Response (IPCR), the Emergency Response Coordination Centre, Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (C(2017) 6100), the EU operational protocol for countering hybrid threats (EU Playbook) SWD(2016) 227.

[32] Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450.

But we are most effective when all are harnessed to support each other. In the first place, this means a more intense cooperation between Member States, involving law enforcement, judicial and other public authorities, and with EU institutions and agencies, to build the understanding and exchange needed for common solutions. Cooperation with the private sector is also key, all the more so given that industry owns an important part of the digital and non-digital infrastructure central to fighting crime and terrorism effectively. Individuals themselves can also contribute, for example through building the skills and awareness to combat cybercrime or disinformation. Finally, this common effort must extend beyond our borders, building closer ties with like-minded partners.

IV. Protecting Everyone in the EU: Strategic priorities for the Security Union

The EU is uniquely well-placed to respond to these new global threats and challenges. The threat analysis above points to four inter-dependent strategic priorities to be taken forward at the EU level, in full respect of fundamental rights: (i) a future proof security environment, (ii) tackling evolving threats, (iii) protecting Europeans from terrorism and organised crime, (iv) a strong European security ecosystem.

1. A future-proof security environment

Critical infrastructure protection and resilience

Individuals rely on key infrastructures in their daily lives, to travel, to work, to benefit from essential public services such as hospitals, transport, energy supplies, or to exercise their democratic rights. If these infrastructures are not sufficiently protected and resilient, attacks can cause huge disruption – whether physical or digital – both in individual Member States and potentially across the entire EU.

The EU's existing framework for protection and resilience of critical infrastructures[33] has not kept pace with evolving risks. Increasing interdependencies mean that disruptions in one sector can have an immediate impact on operations in others: an attack on electricity production could knock out telecommunications, hospitals, banks or airports, while an attack on digital infrastructure could lead to disruptions in networks for power or finance. As our economy and society increasingly move ever more online, risks such as these grow all the more acute. The legislative framework needs to address this increased interconnectedness and interdependency, with robust critical infrastructure protection and resilience measures, both cyber and physical. Essential services, including those based on space infrastructures must be adequately protected against current and anticipated threats, but also be resilient. This implies the ability of a system to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events.

At the same time, Member States have exercised their margin of discretion by implementing existing legislation in different ways. The resulting fragmentation can undermine the internal market and make cross-border coordination more difficult – most obviously in border regions. Operators providing essential services in different Member States have to comply with different reporting regimes. The Commission is looking into whether **new**

[33] Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016; Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

frameworks for both physical and digital infrastructures could bring more consistency and a more coherent approach to ensuring the reliable provision of essential services. This framework needs to be accompanied by **sector-specific initiatives** to tackle the specific risks faced by critical infrastructures such as in transport, space, energy, finance and health[34]. Given the high dependence of the financial sector on IT services and its high vulnerability to cyber-attacks, a first step will be an initiative on the digital operational resilience for financial sectors. Due to the particular sensitivities and impact of the energy system, a dedicated initiative will support a stronger resilience of critical energy infrastructure against physical, cyber and hybrid threats, ensuring a level playing field for energy operators across borders.

Security-relevant effects of foreign direct investments likely to affect critical infrastructures or critical technologies will also be subject to the assessments carried out by EU Member States and the Commission under the new European framework for foreign direct investments screening.[35]

The EU can also build new tools to support the resilience of critical infrastructures. The global internet has so far shown a high level of resilience, in particular as regards the ability to support increased traffic volumes. However, we need to be prepared for possible future crises threatening the security, stability and resilience of the internet. Making sure that the internet remains up and running means being robust against cyber incidents and malicious online activities, and limiting dependency on infrastructures and services located outside Europe. This will require a combination of legislation, with the review of existing rules to ensure a high common level of security of network and information systems in the EU; increased investment in research and innovation; and looking at the deployment or hardening of core internet infrastructures and resources, notably the Domain Name System.[36]

A key element to protect key EU and national digital assets is to offer critical infrastructures a channel for secure communications. The Commission is working with Member States to put in place a certified secure end-to-end quantum infrastructure, terrestrial and space-based, in combination with the secure governmental satellite communications system laid out in the Space Programme regulation.[37]

Cybersecurity

The number of cyber-attacks continues to rise[38]. These attacks are more sophisticated than ever, come from a wide range of sources inside and outside the EU, and target areas of maximum vulnerability. State or state-backed actors are frequently involved, targeting key

---

[34] Given the fact that the health sector has been under strain particularly during the COVID-19 crisis, the Commission will also consider initiatives to strengthen the EU health security framework and responsible EU agencies to respond to serious cross-border health threats.

[35] With its entry into full application on 11 October 2020, Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, will equip the EU with a new cooperation mechanism on direct investments from outside of the EU which are likely to affect security or public order. Under the Regulation, Member States and the Commission will assess potential risks linked with such FDI and, where appropriate and relevant for more than one Member State, propose adequate means to mitigate those risks.

[36] A domain name system (DNS) is a hierarchical and decentralised naming system for computers, services, or other resources connected to the Internet or a private network. It translates domain names to the IP addresses needed for locating and identifying computer services and devices.

[37] Proposal for a Regulation establishing the space programme of the Union and the European Union Agency for the Space Programme. COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

digital infrastructures like major Cloud providers.[39] Cyber risks have emerged as a significant threat to the financial system as well. The International Monetary Fund has estimated the annual loss due to cyber-attacks at 9% of banks' net income globally, or around $100 billion.[40] The move to connected devices will bring great benefits for users: but with less data stored and processed in data centres, and more processed closer to the user 'at the edge'[41], cybersecurity will no longer be able to focus on protecting central points.[42]

In 2017, the EU put forward an approach to cybersecurity with resilience-building, rapid response and effective deterrence at its core.[43] The EU now needs to make sure that its cybersecurity capabilities keep pace with reality, to deliver both resilience and response. This calls for a real whole-of-society approach, with EU institutions, agencies and bodies, Member States, industry, academia and individuals giving cybersecurity the priority it needs.[44] This horizontal approach again needs to be complemented by sector-specific cybersecurity approaches for areas such as energy, financial services, transport or health. The next phase of the EU's work should be drawn together in a revised European Cybersecurity Strategy.

Exploring new and enhanced forms of cooperation between intelligence services, EU INTCEN, and other organisations involved in security should be part of efforts to enhance cybersecurity, as well as combatting terrorism, extremism, radicalism and hybrid threats.

Given the ongoing roll-out of the **5G infrastructure** across the EU and the potential dependence of many critical services on 5G networks, the consequences of systemic and widespread disruption would be particularly serious. The process put in place by the Commission's 2019 Recommendation on the Cybersecurity of 5G networks[45] has now led to specific Member State action on the key measures set out in a 5G toolbox.[46]

One of the most important long-term needs is to develop a culture of **cybersecurity by design**, with security built into products and services from the start. An important contribution to this will be the new cybersecurity certification framework under the Cybersecurity Act[47]. The framework is already under way, with two certification schemes already in preparation, and priorities for further schemes to be defined later this year. Cooperation between the EU Agency for Cybersecurity (ENISA), the data protection authorities and the European Data Protection Board[48] is of key importance in this area.

---

39 Distributed Denial of Service attacks remain a permanent threat: Major providers had to mitigate massive DDoS attacks such as an attack against Amazon Web services in February 2020.

40 https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

41 Edge computing is a distributed, open IT architecture that features decentralised processing power, enabling mobile computing and Internet of Things (IoT) technologies. In edge computing, data is processed by the device itself or by a local computer or server, rather than being transmitted to a data centre.

42 Communication on A European strategy for data, COM(2020) 66 final.

43 Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN (2017) 450.

44 The report "Cybersecurity – our digital Anchor" of the Joint Research Centre provides multidimensional insights into the growth of cybersecurity over the last 40 years.

45 Commission Recommendation on the Cybersecurity of 5G networks, COM(2019) 2335 final. The Recommendation foresees its review in the last quarter of 2020.

46 See Report by the NIS cooperation group on the implementation of the Toolbox, of 24 July 2020.

47 Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act).

48 Communication on Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM(2020) 264.

The Commission has already identified the need for a **Joint Cyber Unit** to provide structured and coordinated operational cooperation. This could include a mutual assistance mechanism in times of crisis at EU level. Building on the implementation of the Blueprint recommendation[49], the Joint Cyber Unit could build trust between the different actors in the European cybersecurity ecosystem and offer a key service to Member States. The Commission will launch discussions with relevant stakeholders (starting with Member States) and set out a clear process, milestones and timeline by the end of 2020.

Also important are common rules on information security and on cybersecurity for all EU institutions, bodies and agencies. The aim should be to create mandatory and high common standards for the secure exchange of information and the security of digital infrastructures and systems across all EU institutions, bodies and agencies. This new framework should underpin a strong and efficient operational cooperation on cybersecurity across the EU institutions, bodies and agencies, centred on the role of the Computer Emergency Response Team (CERT-EU) for the EU institutions, bodies and agencies.

Given its global nature, building and maintaining robust **international partnerships** is fundamental to further prevent, deter and respond to cyber-attacks. The framework for a joint EU diplomatic response to malicious cyber activities ("cyber diplomacy toolbox")[50] sets out measures under the Common Foreign and Security Policy, including restrictive measures (sanctions), which can be used against activities that harm its political, security and economic interests. The EU should also deepen its work through development and cooperation funds to provide capacity building to support partner states in strengthening their digital ecosystems, adopting national legislative reforms and adhering to international standards. This increases the resilience of the overall community and its ability to counter and respond effectively to cyber threats. This includes specific work to promote the EU standards and relevant legislation to increase the cybersecurity of partner countries in the neighbourhood.[51]

Protecting public spaces

Recent terrorist attacks have focused on **public spaces**, including places of worship and transport hubs, exploiting their open and accessible nature. The rise of terrorism triggered by political or ideologically motivated extremism has made this threat even more acute. This calls for both stronger physical protection of such places and adequate detection systems, without undermining citizens' freedoms.[52] The Commission will enhance public-private cooperation for the protection of public spaces, with funding, the exchange of experience and good practices, specific guidance[53] and recommendations.[54] Awareness raising, performance requirements and testing of detection equipment and enhancing background checks to address insider threats will also be part of the approach. An important aspect to reflect is the fact that minorities and vulnerable individuals can be disproportionately affected including persons targeted because of their religion or gender, and therefore require

---

[49] Commission Recommendation 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

[51] See the EU External Cyber Capacity Building Guidelines adopted in Council conclusions on 26 June 2018.

[52] Remote biometric identification systems deserve specific scrutiny. The Commission's initial views are outlined in the Commission White Paper of 19 February 2020 on Artificial Intelligence, COM(2020) 65.

[53] As for example the Guidance on selecting proper security barrier solutions for public space protection (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Guidance on good practices is given in SWD(2019) 140, including a section on public-private cooperation. Funding under ISF-Police has a special focus on enhancing the public-private cooperation.

particular attention. Regional and local public authorities have an important role to improve security of public spaces. The Commission is also helping foster cities' innovation in security in public spaces[55]. The launch of a new Urban Agenda[56] partnership on "security in public spaces" in November 2018 reflects the strong commitment of Member States, Commission and cities to better address threats to security in the urban space.

The market for **drones** continues to expand, with many valuable and legitimate uses. However, they also have the potential to be misused by criminals and terrorists, with public spaces under particular threat. Targets can include individuals, gatherings of people, critical infrastructure, law enforcement authorities, borders or public spaces. Knowledge about the use of drones in conflict could find its way back to Europe either directly (via returning Foreign Terrorist Fighters) or online. Rules already developed by the European Aviation Safety Agency are an important first step in areas including the registration of drone operators and the mandatory remote identification of drones. With drones becoming ever more widely available, more affordable and more capable, there is a need for additional action. This could include information sharing, guidance and good practice for use by all, including law enforcement, as well as more testing of drone countermeasures.[57] In addition, the privacy and data protection implications of the use of drones in public spaces should be further analysed and addressed.

Key actions
• Legislation on the protection and resilience of critical infrastructure • Revision of the Network Information Systems Directive • An initiative on the operational resilience of the financial sector • Protection and cybersecurity of critical energy infrastructure and network code on cybersecurity for cross-border electricity flows • A European Cybersecurity Strategy • Next steps towards the creation of a Joint Cyber Unit • Common rules on information security and cybersecurity for EU institutions, bodies and Agencies • Stepped up cooperation for the protection of public spaces, including places of worship • Sharing of best practices on addressing misuse of drone

2. Tackling evolving threats

Cybercrime

Technology brings new opportunities for society. It also offers new tools for the judiciary and for law enforcement. But at the same time, it opens doors for criminals. Malware, the theft of personal or business data by hacking, and the shutting off of digital activity causing financial or reputational damage, are all on the rise. The resilient environment created by strong cybersecurity is the first defence. Law enforcement authorities need to be able to

[55] Three cities (Piraeus in Greece, Tampere in Finland and Turin in Italy) will be testing new solutions as part of the Urban Innovative Actions, co-funded by the European Regional Development Fund (ERDF).

[56] The Urban Agenda for the EU represents a new multi-level working method promoting cooperation between Member States, cities, the European Commission and other stakeholders to stimulate growth, livability and innovation in the cities of Europe and to identify and successfully tackle social challenges.

[57] A multi-year testing programme to support Member States in developing a common methodology and test platform in this area was recently established.

work in the sphere of digital investigations with clear rules to investigate and prosecute crimes and affording victims the necessary protection. This work should build on the Joint Cybercrime Action Task Force in Europol and the Law Enforcement Emergency response Protocol created to coordinate response to large-scale cyber-attacks. Effective mechanisms enabling public-private partnerships and cooperation are also key.

In parallel, the fight against cybercrime should become a strategic communication priority across the EU, to alert Europeans to the risks and to the preventive measures they could take. This should be part of a proactive approach. An essential step is also the full implementation of the current legal framework[58]: the Commission will be ready to use infringement procedures as appropriate, as well as keeping this framework under review to ensure it remains fit for purpose. The Commission will also explore, together with Europol and the EU Agency for Cybersecurity ENISA, the feasibility of an EU cybercrime-related rapid alert system that could ensure the flow of information and swift reactions when cybercrimes surge.

Cybercrime is a global challenge where effective international cooperation is necessary. The EU supports the Council of Europe's Budapest Convention on cybercrime, which is an effective, well-established framework that allows all countries to identify what systems and communication channels they need to put in place to be able to work effectively with each other.

Nearly half of EU citizens worry about data misuse[59] and **identity theft** is a major concern.[60] The fraudulent use of identity for financial gain is one aspect, but there can also be a major personal and psychological impact, with illegal postings made by the identity thief able to stay online for years. The Commission will explore possible practical measures to protect victims against all forms of identity theft, taking account of the upcoming European Digital Identity initiative.[61]

Tackling cybercrime means looking ahead. As society uses new technological developments to strengthen the economy and society, criminals can also look to exploit these tools to negative ends. For example, criminals can use artificial intelligence to detect and identify passwords or to simplify the creation of malware, to exploit images and audio that can be then used for identity theft or fraud.

Modern law enforcement

Law enforcement and justice practitioners need to adapt to new technology. Technological developments and emerging threats require law enforcement authorities to have access to new tools, acquire new skills and develop alternative investigative techniques. To complement legislative actions aiming at improving cross-border access to electronic evidence for criminal investigations, the EU can help law enforcement authorities to develop the necessary capacity to identify, secure and read the data needed to investigate crimes and to use that data as evidence in court. The Commission will explore measures to **enhance law enforcement capacity in digital investigations,** defining how to make the best use of research and development to create new tools for law enforcement; and how training can

---

58 Directive 2013/40/EU on attacks against information systems.

59 46% (Eurobarometer on Europeans' attitudes towards cyber security, January 2020).

60 The vast majority of respondents to the 2018 Eurobarometer 'Europeans' attitudes towards Internet security' (95%) saw identity theft as a serious crime, and seven in ten say that it is a very serious crime. The Eurobarometer published in January 2020 confirmed concerns about cybercrime, online fraud and identity theft: with two thirds of respondents concerned about banking fraud (67%) or identity theft (66%)

61 Communication of 19 February 2020 on Shaping Europe's Digital Future, COM(2020) 67.

offer the right skill set to law enforcement and the judiciary. This will also include providing stringent scientific evaluations and testing methods through the Commission's Joint Research Centre.

Common approaches can also ensure that **artificial intelligence, space capabilities, Big Data** and **High Performance Computing are integrated** into security policy in a way which is effective both in fighting crimes and in ensuring fundamental rights. Artificial intelligence could act as a powerful tool to fight crime, creating enormous investigative capabilities by analysing large amounts of information and identifying patterns and anomalies.[62] It can also provide concrete tools, such as to help identify online terrorist content, discover suspicious transactions in the sales of dangerous products or offer assistance to citizens in emergencies. Realising this potential means bringing together research, innovation and users of artificial intelligence with the right governance and technical infrastructure, actively involving the private sector and academia. It also means ensuring the highest standards of compliance with fundamental rights while ensuring an effective protection of citizens. In particular, decisions impacting individuals must be subject to human review and comply with the relevant applicable EU law.[63]

Electronic information and evidence is needed in about 85% of investigations into serious crimes, while 65% of the total requests go to providers based in another jurisdiction.[64] The fact that traditional physical traces have moved online further expands the gap between the law enforcement and criminals' capabilities. Putting in place clear rules for cross-border access to electronic evidence for criminal investigations is essential. This is why swift adoption by the European Parliament and Council of the e-evidence proposals is key to provide practitioners with an efficient tool. Cross-border access to e-evidence through multilateral and bilateral international negotiations is also key, to establish compatible rules at international level[65].

Access to digital evidence also depends on the availability of information. If the data is erased too quickly, important evidence may disappear, so that the possibility to identify and locate suspects and criminal networks (as well as victims) no longer exists. On the other hand, data retention schemes raise questions of protection of privacy. Depending on the outcome of the cases pending before the European Court of Justice, the Commission will assess the way forward on data retention.

Access to Internet domain name registration information ('WHOIS data')[66] is important for criminal investigations, cybersecurity and consumer protection. However, access to this information is becoming more difficult, pending the adoption of a new WHOIS policy by the Internet Corporation for Assigned Names and Numbers (ICANN). The Commission will continue to work with the ICANN and the multi-stakeholder community to ensure that legitimate access seekers, including law enforcement, can obtain efficient access to WHOIS data in line with EU and international data protection regulations. This will include

---

62 For example, in financial crimes.

63 This means compliance with existing legislation, including the General Data Protection Regulation (EU) 2016/679 as well as the Data Protection Law Enforcement Directive (EU) 2016/680 regulating the processing of personal data for detecting, preventing investigating and prosecuting criminal offences or the execution of criminal penalties.

64 Commission SWD(2018) 118 final.

65 In particular, the Second Additional Protocol to the Council of Europe 'Budapest' Convention on Cybercrime and an agreement between the EU and the United States on cross-border access to e-evidence.

66 Stored in databases maintained by 2.500 registry and registrar operators based all around the world.

assessing possible solutions, including whether legislation may be necessary to clarify rules for accessing such information.

Law enforcement and judicial authorities also need to be equipped to obtain the necessary data and evidence once the **5G architecture for mobile telecommunications** is fully deployed in the EU, in a way which respects the confidentiality of communications. The Commission will support an enhanced and coordinated approach when building international standards, defining best practices, process, and technical interoperability in key technological areas such as AI, internet of things or blockchain technologies.

Today, a substantial part of investigations against all forms of crime and terrorism involve **encrypted information**. Encryption is essential to the digital world, securing digital systems and transactions and also protecting a series of fundamental rights, including freedom of expression, privacy and data protection. However, if used for criminal purposes, it may also mask the identity of criminals and hide the content of their communications. The Commission will explore and support balanced technical, operational and legal solutions to the challenges and promote an approach which both maintains the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism.

Countering illegal content online

Bringing the security of the online and physical environments in line means continued steps in **countering illegal content online**. More and more, core threats to citizens such as terrorism, extremism or child sexual abuse rely on the digital environment: this calls for concrete action and a framework to ensure respect for fundamental rights. An essential first step is swiftly concluding the negotiations on the proposed legislation on terrorist content online[67] and ensuring its implementation. Strengthening voluntary cooperation between law enforcement and the private sector in the **EU Internet Forum** is also key to fight the misuse of the internet by terrorists, violent extremists and criminals. The EU Internet Referral Unit in Europol will continue to play a crucial role in monitoring the activity of terrorist groups online and the action taken by platforms,[68] as well as in further developing the **EU Crisis Protocol**[69]. In addition, the Commission will continue to engage with international partners including by participating in the **Global Internet Forum to Counter Terrorism** to tackle these challenges at global level. Work will continue to support the development of alternative and counter narratives through the Civil Society Empowerment Programme.[70]

To prevent and counter the spread of illegal hate speech online, the Commission launched in 2016 the Code of Conduct on countering illegal hate speech online, with a voluntary commitment by online platforms to remove hate speech content. The latest evaluation shows that companies assess 90% of flagged content within 24 hours and remove 71% of the content deemed to be illegal hate speech. However, the platforms need to improve further transparency and feedback to users and to ensure consistent evaluation of flagged content[71].

The EU Internet Forum will also facilitate exchanges on existing and developing technology to address the challenges related to child sexual abuse online. Tackling child sexual abuse online is at the heart of a new Strategy to step up the **fight against child sexual abuse**[72],

---

67 Proposal on preventing the dissemination of terrorist content online, COM(2018) 640, 12 September 2018.
68 Europol, November 2019.
69 A Europe that protects - EU Crisis Protocol: responding to terrorist content online. (October 2019).
70 Linked to the work of the Radicalisation Awareness Programme, see section IV.3 below.
71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf
72 EU Strategy for a more effective fight against child sexual abuse, COM(2020) 607.

which will seek to maximise the use of tools available at EU level to fight against these crimes. Companies must be able to continue their work to detect and remove child sexual abuse material online, and the damage caused by this material calls for a framework setting out clear and permanent obligations to tackle the problem. The Strategy will also announce that the Commission will also start preparing sector-specific legislation to tackle child sexual abuse online more effectively, in full respect of fundamental rights.

More generally, the forthcoming Digital Services Act will also clarify and upgrade the liability and safety rules for digital services and remove disincentives holding back actions to address illegal content, goods or services.

In addition, the Commission will continue to engage with international partners and with the **Global Internet Forum to Counter Terrorism**, including through the independent advisory committee, to discuss how to tackle these challenges at global level while preserving EU values and fundamental rights. New topics should also be addressed such as algorithms or online gaming.[73]

Hybrid threats

The scale and diversity of hybrid threats today is unprecedented. The COVID-19 crisis saw more proof of this, with several state and non-state actors seeking to instrumentalise the pandemic – in particular through manipulation of the information environment and challenging core infrastructures. This risks weakening social cohesion and undermining trust in EU institutions and Member States' governments.

The EU approach to hybrid threats is set out in the 2016 Joint Framework[74] and the 2018 Joint Communication on bolstering hybrid resilience.[75] Action at EU level is underpinned by a sizeable toolbox covering the internal-external nexus, based on a whole-of-society approach and on close cooperation with strategic partners, notably NATO and G7. A report on the implementation of the EU approach on hybrid threats is published together with this Strategy.[76] Based on the mapping[77] presented in parallel to this Strategy, the Commission services and the European External Action Service will create a **restricted online platform** for Member States' reference on counter-hybrid tools and measures at EU level.

Whereas responsibility for countering hybrid threats lies primarily with Member States – due to the intrinsic links with national security and defence policies – some vulnerabilities are common to all Member States and some threats extend across borders, such as targeting cross-border networks or infrastructure. The Commission and the High Representative will set out an EU approach to hybrid threats that integrates the external and internal dimension in a seamless flow and brings the national and EU-wide considerations together. This must cover the full spectrum of action – from early detection, analysis, awareness, building resilience and prevention through to crisis response and consequence management.

In addition to reinforced implementation, with hybrid threats in constant evolution, a particular focus will be to **mainstream hybrid considerations into policy making**, to keep up to speed with dynamic developments and to ensure that no potentially relevant initiative

---

[73] Terrorists are increasingly using the messaging system of gaming platforms for exchanges and young terrorists also re-play violent attacks in video games.

[74] Joint Framework on Countering Hybrid Threats – a European Union response, JOIN (2016) 18.

[75] Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, JOIN (2018) 16.

[76] SWD(2020) 153 Report on 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

[77] SWD(2020) 152 Mapping of the measures related to enhancing resilience and countering hybrid threats.

is overlooked. The effects of new initiatives will also be assessed through hybrid lenses, including initiatives in areas that have so far been outside the remit of the counter hybrid framework such as education, technology and research. This approach would benefit from the work done on the conceptualisation of hybrid threats, which provides a comprehensive view of the various tools that adversaries may use.[78] The aim should be to ensure that the decision-making process is underpinned by regular, comprehensive intelligence-based reporting on the evolution of hybrid threats. This will rely heavily on Member States' intelligence and on further enhancing intelligence cooperation with Member States' competent services through EU INTCEN.

To develop **situational awareness**, the Commission services and the European External Action Service will explore options to streamline information flows from different sources, including Member States, as well as EU agencies such as ENISA, Europol and Frontex. The EU Hybrid Fusion Cell will remain the EU focal point for hybrid threat assessments. **Building resilience** is central to preventing and protecting against hybrid threats. It is therefore crucial to systematically track and objectively measure progress in this area. A first step will be to identify sectoral hybrid resilience baselines for both Member States and EU institutions and bodies. Finally, to step up **hybrid crisis response preparedness,** the existing protocol should be reviewed, as defined in the 2016 EU Playbook[79], reflecting a broader review and strengthening of the EU crisis response system currently under consideration.[80] The aim is to maximise the effect of EU action by swiftly bringing together sectoral responses and ensuring seamless cooperation with our partners, NATO in the first place.

Key actions
• Ensuring that the cybercrime legislation is implemented and fit for purpose • A Strategy for a more effective fight against child sexual abuse • Proposals on the detection and removal of child sexual abuse material • An EU approach on Countering Hybrid Threats • Review of the EU operational protocol for countering hybrid threats (EU Playbook) • Assessment of how to enhance law enforcement capacity in digital investigations

3. Protecting Europeans from terrorism and organised crime

Terrorism and radicalisation

The terrorist threat in the EU remains high. Despite the decrease in the number of attacks overall, these can still have a devastating effect. Radicalisation can also more broadly polarise and destabilise social cohesion. Member States retain the primary responsibility in the fight against terrorism and radicalisation. However, the ever-increasing cross-border/cross sectorial dimension of the threat calls for further steps in EU cooperation and coordination. Effective implementation of EU counter-terrorism legislation, including

[78] The Landscape of Hybrid Threats: A conceptual Model, JRC117280, jointly developed by the Joint Research Centre and the Centre of Excellence for Countering Hybrid Threats.

[79] EU operational protocol for countering hybrid threats (EU Playbook), SWD(2016) 227.

[80] Following their video conference on 26 March 2020, the Members of the European Council adopted a Statement on EU actions in response to the COVID-19 outbreak, inviting the Commission to make proposals a more ambitious and wide-ranging crisis management system within the EU.

restrictive measures[81], is a priority. It remains an objective to extend the mandate of the European Public Prosecutor's Office to cross-border terrorist crimes.

Fighting terrorism starts with addressing the root causes. The polarisation of society, real or perceived discrimination and other psychological and sociological factors can reinforce people's vulnerability to radical discourse. In this context, tackling **radicalisation** goes hand in hand with fostering social cohesion at local, national and European level. Several impactful initiatives and policies have been developed in the last decade, in particular through the Radicalisation Awareness Network and the EU Cities against Radicalisation Initiative.[82] It is time now to consider actions to streamline EU policies, initiatives and funds to tackle radicalisation. Such actions can support the development of capabilities and skills, enhance cooperation, strengthen the evidence base and help evaluate progress, involving all relevant stakeholders, including first line practitioners, policy makers and academia.[83] Soft policies such as education, culture, youth and sports could contribute to the prevention of radicalisation, providing opportunities for at-risk youth and cohesion inside of the EU.[84] Priority areas include work on early detection and risk management, resilience building and disengagement, as well as rehabilitation and reintegration in society.

Terrorists have sought to acquire and to "weaponise" **chemical, biological, radiological and nuclear** (CBRN)[85] materials, as well as to develop the knowledge and capacity to use them.[86] The potential of CBRN attacks features prominently in terrorist propaganda. With the potential damage so high, particular attention is needed. Building on the approach used to regulate access to explosive precursors, the Commission will look into restricting access to certain dangerous chemicals that could be used to carry out attacks. The development of EU civil protection response (rescEU) capacities in the field in CBRN will also be key. Cooperation with third countries is also important to enhance a common culture of CBRN safety and security, making full use of the EU global CBRN Centres of Excellence. This cooperation will include national gap and risk assessments, support to national and regional CBRN action plans, exchanges of good practices and CBRN capacity building activities.

The EU has developed the most advanced legislation in the world to restrict access to **explosives precursors**[87] and detect suspicious transactions aiming to build improvised explosive devices. But the threat from home-made explosives remains high, used in multiple attacks throughout the EU.[88] The first step must be implementation of the rules, as well as ensuring that the online environment does not allow the by-passing of controls.

The effective prosecution of those who have committed terrorist crimes, including **Foreign Terrorist Fighters** currently in Syria and Iraq, is also an important element of counterterrorism policy. While these issues are primarily dealt with by Member States, EU

---

81 The Council adopted restrictive measures with respect to ISIL (Da'esh) and Al-Qaida, as well as specific restrictive measures directed against certain persons and entities with a view to combating terrorism. See the EU Sanctions Map (https://www.sanctionsmap.eu/#/main) for an overview of all restrictive measures.

82 The pilot initiative "EU Cities against Radicalisation" has the double objective to foster the exchange of expertise among EU cities and to gather feedback on how to best support local communities at EU level.

83 For example funding under the European Security Fund and the Citizenship programme.

84 EU actions such as the Erasmus+ Virtual Exchanges, e-twinning.

85 In the past two years there have been for instance several cases both in Europe (France, Germany, Italy) and elsewhere (Tunisia, Indonesia) involving biological agents (usually plant-based toxins).

86 The Council adopted restrictive measures against the proliferation and use of chemical weapons.

87 Chemicals that could be misused to manufacture homemade explosives. These are regulated in Regulation (EU) 2019/1148 2019 on the marketing and use of explosives precursors.

88 Some examples of such devastating attacks include attacks in Oslo (2011), Paris (2015), Brussels (2016), and Manchester (2017). An attack with a homemade explosive in Lyon (2019) wounded 13 people.

coordination and support can help Member States to address common challenges. The steps under way to fully implement border security legislation[89] and make full use of all relevant EU databases to share information on known suspects will be an important step. As well as identifying high-risk individuals, a reintegration and rehabilitation policy is needed. Cross-professional cooperation, including with prison and probation staff, will reinforce the judicial understanding of the processes of radicalisation to violent extremism and the judicial sector's approach to sentencing and alternatives to detention.

The challenge of foreign terrorist fighters is emblematic of the link between internal and **external security.** Cooperation on counterterrorism and preventing and countering radicalisation and violent extremism is central to security inside the EU.[90] Further steps to develop counterterrorism partnerships and cooperation with countries in the neighbourhood and beyond is needed, drawing on the expertise of the Network of EU Counter-Terrorism/Security Experts. The Joint Action Plan on Counter-terrorism for the Western Balkans is a good reference for such targeted cooperation. In particular, efforts should be made to support partner countries' capacity to identify and locate foreign terrorist fighters. The EU will also continue to promote multilateral cooperation, working with the leading global actors in this field, such as the United Nations, NATO, the Council of Europe, Interpol and the OSCE. It will also engage with the Global Counterterrorism Forum and the Global Coalition against Da'esh, as well as relevant civil society actors. The Union's external policy instruments, including development and cooperation, play also an important role when working with third countries to prevent terrorism and piracy. International cooperation is also essential to cut off all sources of **terrorism financing**, for example through the Financial Action Task Force.

Organised crime

Organised crime comes at a huge economic and personal cost. The economic loss due to organised crime and corruption has been estimated to represent between €218 and €282 billion annually.[91] More than 5,000 organised crime groups were under investigation in Europe in 2017 – a 50% rise compared to 2013.[92] Organised crime is increasingly operating cross-border including from the immediate neighbourhood of the EU, calling for intensified operational cooperation and information exchange with partners in the neighbourhood.

New challenges are emerging and taking crime online: the COVID-19 pandemic saw a huge rise in online scams on vulnerable groups, as well as health and sanitary products being targeted in thefts and burglaries.[93] The EU needs to step up its work against organised crime, including at international level, with more tools to dismantle organised crime's business model. Fighting organised crime also requires close cooperation with local and regional administrations as well as civil society, who are key partners in crime prevention as well as in providing assistance and support to victims, with a particular need amongst administrations in border regions. This work will be brought together in an **Agenda for tackling organised crime**.

---

89 Including the new mandate of the European Border and Coast Guard Agency (Frontex).

90 Council conclusions of 16 June 2020 underlined the need to protect EU citizens against terrorism and violent extremism, in all their forms and irrespective of their origin, and to further strengthen the EU's external counter-terrorism engagement and action in certain priority geographic and thematic areas.

91 In terms of Gross Domestic Product (GDP); Europol report: "Does crime still pay?" – Criminal asset recovery in the EU, 2016.

92 Europol, Serious and Organised Threat Assessments (SOCTA), 2013 and 2017.

93 Europol, 2020.

More than one third of the organised crime groups active in the EU are involved in the production, trafficking or distribution of drugs. Drugs addiction led to over eight thousand overdose deaths in the EU in 2019. The bulk of **drug trafficking** operates across borders with many of the profits infiltrating the legal economy.[94] A new EU Agenda on Drugs[95] will strengthen the efforts of the EU and Member States in the areas of drug demand and supply reduction, defining joint actions addressing a common problem and reinforcing the dialogue and cooperation between the EU and external partners on drug issues. Following an evaluation of the European Monitoring Centre on Drugs and Drugs Addiction, the Commission will assess whether its mandate needs updating to meet new challenges.

Organised crime groups and terrorists are also key players in the trade of **illegal firearms**. Between 2009 and 2018, 23 mass-shooting incidents occurred in Europe, which killed over 340 people.[96] Firearms are often trafficked into the EU through its immediate neighbourhood.[97] This points to a need to reinforce coordination and cooperation both within the EU and with international partners, particularly Interpol, to harmonise the collection of information and reporting on firearm seizures. It is also essential to improve the traceability of weapons, including on the internet, and ensure information exchange between licensing and law enforcement authorities. The Commission is putting forward a new **EU Action Plan against firearms trafficking**[98] and will also assess whether the rules on export authorisation and import and transit measures for firearms are still fit for purpose.[99]

Criminal organisations treat migrants and people in need of international protection as a commodity. 90% of the irregular migrants arriving in the EU are facilitated by a criminal network.[100] Migrant smuggling is also often intertwined with other forms of organised crime, in particular trafficking in human beings.[101] Apart from the huge human cost of trafficking, Europol estimates that globally the generated annual profit for all forms of exploitation from human trafficking amounts to €29.4 billion. This is a transnational crime feeding on illegal demands from within and outside the EU and impacting all EU Member States. The poor record in identifying, prosecuting and convicting these crimes requires a new approach to step up action. A new **comprehensive approach to trafficking in human beings** will draw together the threads of action. In addition, the Commission will present a **new EU Action Plan against migrant smuggling** for 2021-2025. Both strands will focus on combatting criminal networks, boosting cooperation and support the work of law enforcement.

Organised crime groups – as well as terrorists – also seek opportunities in other fields, especially those generating high profits at a low detection risk, such as **environmental crime**. Illicit hunting and trading of wildlife, illegal mining, logging, and illegal waste disposal and shipments, have become the fourth largest criminal business around the

94 EMCDDA and Europol, EU Drug Markets Report 2019. (November 2019).
95 EU Drugs Agenda and Action Plan 2021-2025, COM(2020) 606.
96 Flemish Peace Institute, Armed to kill. (October 2019).
97 The EU has funded the fight against the proliferation and trafficking of small arms and light weapons in the region since 2002; it is notably funded the South-East Europe Firearms Expert Network (SEEFEN). Since 2019, Western Balkan partners have been fully involved in the Firearms priority of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).
98 COM(2020) 608.
99 Regulation (EU) No 258/2012 implementing Article 10 of the United Nations' Protocol against the illicit manufacturing of and trafficking in firearms.
100 Source: Europol.
101 Europol, EMSC, 4th Annual Report.

world.[102] There has also been criminal exploitation of emission trading schemes and energy certificate systems, as well as the misuse of funding allocated to environmental resilience and sustainable development. As well as promoting action by the EU, Member States and the international community to step up efforts against environmental crime[103], the Commission is assessing whether the Environmental Crime Directive[104] is still fit for purpose. **Trafficking in cultural goods** has also become one of the most lucrative criminal activities, a source of funding for terrorists as well as organised crime and it is on the rise. Steps should be explored to improve the online and offline traceability of cultural goods in the internal market and cooperation with third countries where cultural goods are looted as well as providing active support to law enforcement and academic communities.

Economic and financial crimes are highly complex, but they affect millions of citizens and thousands of companies in the EU every year. Combatting fraud is crucial and requires EU-level action. Europol, along with Eurojust, the European Public Prosecutor's Office and the European Anti-Fraud Office support Member States and the EU in protecting the economic and financial markets and safeguarding EU taxpayers' money. The European Public Prosecutor's Office will become fully operational late in 2020 and investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption and money laundering. It will also tackle cross-border VAT fraud costing taxpayers at least €50 billion every year.

The Commission will also support the development of expertise and of a legislative framework in emerging risks, such as crypto-assets and new payment systems. In particular, the Commission will look at the response to the emergence of crypto-assets such as bitcoin and the effect these new technologies will have on how financial assets are issued, exchanged, shared and accessed.

There should be zero tolerance for illicit money within the European Union. Over thirty years, the EU has developed a solid regulatory framework for preventing and combatting **money laundering** and terrorist financing, in full respect of the need to protect personal data. Nevertheless, there is growing consensus that the implementation of the current framework needs to be significantly improved. Major divergences in the way it is applied and serious weaknesses in the enforcement of the rules need to be addressed. As detailed in the Action Plan of May 2020[105], work is under way to assess options to enhance the EU's framework for anti-money laundering and countering terrorist financing. Areas to explore include the interconnection of national centralised bank account registries, which could significantly speed up access to the financial information for Financial Intelligence Units and competent authorities.

Profits of organised crime groups are estimated at €110 billion per year in the EU. The current response includes harmonised legislation on confiscation and asset recovery,[106] to improve the freezing and confiscation of criminal assets in the EU and to facilitate mutual trust and effective cross-border cooperation between Member States. However, only about 1% of these profits are confiscated[107], which allows organised crime groups to invest in the expansion of their criminal activities and to infiltrate the legal economy, and in particular small and medium enterprises, which have difficulties in access to credit, are a key target for

[102] UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime, June 2016.
[103] See The European Green Deal COM(2019) 640 final.
[104] Directive 2008/99/EC on the protection of the environment through criminal law.
[105] Action Plan on preventing money laundering and terrorist financing COM(2020) 2800.
[106] EU law requires Asset Recovery Offices to be established in all Member States.
[107] Report on Asset recovery and confiscation: ensuring that crime does not pay, COM(2020) 217 final.

money laundering. The Commission will analyse the implementation of the legislation[108] and the possible need for further common rules, including on non-conviction based confiscation. The Asset Recovery Offices[109], key actors in the asset recovery process, could also be equipped with better tools to identify and trace assets in a speedier way across the EU in order to step up confiscation rates.

There is a strong link between organised crime and **corruption**. It has been roughly estimated that corruption alone costs the EU economy €120 billion per year.[110] The prevention and fight against corruption will continue to be subject to regular monitoring under the rule of law mechanism as well as the European Semester. The European semester has assessed challenges in the fight against corruption such as public procurement, public administration, the business environment or healthcare. The Commission's new annual rule of law report will cover the fight against corruption and enable a preventive dialogue with national authorities and interested stakeholders at EU and national level. Civil society organisations can also play a key role in stimulating the action of public authorities in preventing and fighting organised crime and corruption, and these groups could usefully be brought together in a common forum. Due to their cross-border nature, another key dimension is cooperation and assistance on organised crime and corruption with neighbouring regions to the EU.

Key actions

- Counter-Terrorism Agenda for the EU, including renewed anti-radicalisation actions in the EU
- New cooperation with key third countries and international organisations against terrorism
- Agenda on tackling organised crime, including trafficking in human beings
- EU Agenda on Drugs and Action Plan 2021-2025
- Assessment of the European Monitoring Centre for Drugs and Drug Addiction
- 2020-2025 EU Action Plan on Firearms trafficking
- Review of legislation on freezing and confiscation and on Asset Recovery Offices
- An assessment of the Environmental Crime Directive
- An EU Action Plan against Migrant Smuggling, 2021-2025

4. A strong European security ecosystem

A genuine and effective Security Union must be the common endeavour of all parts of society. Governments, law enforcement, the private sector, education and citizens themselves need to be engaged, equipped, and properly connected to build preparedness and resilience for all, particularly the most vulnerable, victims and witnesses.

All policies need a security dimension and the EU can make a contribution at all levels. In the home, domestic violence is one of the most serious security risks. In the EU 22% of women have experienced violence by an intimate partner.[111] EU accession to the Istanbul

[108] Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime.
[109] Council Decision 2007/845/JHA on cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime.
[110] Estimating the total economic costs of corruption is difficult, though efforts have been made by bodies including International Chamber of Commerce, Transparency International, UN Global Compact, and the World Economic Forum, suggesting that corruption amounts to 5% of global GDP.
[111] A Union of Equality: Gender Equality Strategy 2020-2025, COM(2020) 152.

Convention on preventing and combatting violence against women and domestic violence remains a key priority. Should the negotiations remain blocked, the Commission will take other measures to achieve the same objectives as the Convention, including proposing to add violence against women to the list of EU crimes defined in the Treaty.

Cooperation and information exchange

One of the most critical contributions the EU can make to protecting citizens is through helping those responsible for security to work well together. Cooperation and information sharing are the most powerful tools to combat crime and terrorism and pursue justice. To be efficient, it needs to be targeted and timely. To be trusted, it needs to be used with common safeguards and controls.

A number of EU instruments and sector specific strategies[112] have been set up to further develop **operational law enforcement cooperation** between Member States. One of the main EU instruments supporting law enforcement cooperation between Member States is the Schengen Information System, used to exchange data on wanted and missing persons and objects in real time. The results have been felt in the arrest of criminals, seizures of drugs and the rescuing of potential victims.[113] However, the level of cooperation could still be improved through streamlining and upgrading the available instruments. Most of the EU legal framework underpinning operational law enforcement cooperation was designed 30 years ago. A complex web of bilateral agreements between Member States, many outdated or underused, risks fragmentation. In smaller or landlocked countries, law enforcement officers working across borders have to carry out operational actions following, in some cases, up to seven different sets of rules: the result is that some operations, such as hot pursuits of suspects over internal borders, simply do not happen. Operational cooperation on new technologies such as drones are also not covered by the current EU framework.

Operational effectiveness can be supported by specific law enforcement cooperation, which may also help to provide key support to other policy goals – such as providing security input for the new assessment of foreign direct investment. The Commission will look at how a Police Cooperation Code might support this. Member States' law enforcement authorities have increasingly made use of support and expertise at EU level, while EU INTCEN has played a key role in promoting the exchange of strategic intelligence between Member States Intelligence and Security Services providing intelligence situational awareness in favour of EU institutions.[114] **Europol** can also play a key role in expanding its cooperation with third countries to counter crime and terrorism in coherence with other EU external polices and tools. However, Europol today faces a number of serious constraints – notably as regards the direct exchange of personal data with private parties – which hinders it from effectively supporting Member States in combating terrorism and crime. Europol's mandate is now being assessed to see how it should be improved to ensure that the Agency can fully perform its tasks. In this context, relevant authorities at EU level (such as OLAF, Europol, Eurojust and the European Public Prosecutor's Office) should also cooperate more closely and improve the exchange of information.

Another key connection is with the further development of **Eurojust** to maximise the synergy between law enforcement cooperation and judicial cooperation. The EU would also

[112] Such as the EU Maritime Security Strategy Action Plan which led to important achievements with the cooperation on coast-guard functions between relevant EU Agencies.

[113] The EU fight against organised crime in 2019 (Council, 2020).

[114] EU INTCEN serves as the only gateway for Member States Intelligence and Security Services to provide intelligence-led situational awareness to the EU.

benefit from more strategic coherence: **EMPACT**[115], the EU policy cycle for serious and international organised crime, provides a criminal intelligence-led methodology for authorities to jointly tackle the most important criminal threats affecting the EU. It has resulted in important operational results[116] in the past decade. Based on practitioners' experience, the existing mechanism should be streamlined and simplified to better address the most pressing and evolving criminal threats for a new Policy Cycle 2022-2025.

Timely and relevant **information** is key for the daily work of pursuing crime. Despite the development of new EU level databases for security and border management, much information is still located in national databases or exchanged outside these tools. The result is a significant additional workload, delays, and an increased risk that key information is missed. Better, quicker and simplified processes, involving all the security community, would bring better results. The right tools are essential if information exchange is to meet its potential in the effective pursuit of crime with the necessary safeguards so that data sharing respects data protection laws and fundamental rights. In light of technological, forensic and data protection developments, and changed operational needs, the EU could consider if there is a need to modernise instruments such as the **2008 Prüm Decisions**, establishing automated exchange of DNA, fingerprint and vehicle registration data, to enable the automated exchange of additional data categories that are already available in Member States' criminal or other databases for the purpose of criminal investigations. In addition, the Commission will look into the possibility to exchange police records to help identify if any police record on a person exists in other Member States, and facilitate access to these records once identified, with all the necessary safeguards.

Information on travellers has helped to improve border controls, reduce irregular migration, and identify persons posing security risks. Advanced Passenger Information data are the biographic data for each passenger collected by air carriers during check-in and sent in advance to the border control authorities at destination. The revision of the legal framework[117] could allow for more effective use of the information, while ensuring compliance with data protection legislation and facilitating the flow of passengers. Passenger Name Records (PNR) is the data provided by passengers when booking flights. The implementation of the PNR Directive[118] is key, and the Commission will continue to support and enforce this. Moreover, as a mid-term action, the Commission will launch a review of the current approach on **PNR data transfer to third countries**.

Judicial cooperation is a necessary complement to police efforts to fight cross-border crime. Judicial cooperation has gone through a more profound change in the last 20 years. Bodies such as the **European Public Prosecutor's Office** and **Eurojust** need to have the means to function to their fullest extent or be reinforced. Co-operation between judicial practitioners could also be enhanced, through further steps on the mutual recognition of judicial decisions, judicial training, and information exchange. The goal should be increased mutual trust among judges and prosecutors, central to smooth cross-border proceedings. The use of **digital technologies** can also improve the efficiency of our justice systems. A new digital exchange system is being set up to transmit European Investigation Orders, mutual legal assistance requests and related communications between Member States, supported by

[115] EMPACT stands for European Multidisciplinary Platform Against Criminal Threats.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.
[117] Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data.
[118] Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Eurojust. The Commission will work with Member States to accelerate the roll-out of the necessary IT systems at the national level.

International cooperation is also key to effective law enforcement and judicial cooperation. Bilateral agreements with key partners play a key role in securing information and evidence from beyond the EU. **Interpol,** one of the largest inter-governmental criminal police organisations, has an important role. The Commission will look at possible ways of reinforcing cooperation with Interpol, including possible access to Interpol databases and the strengthening of operational and strategic cooperation. Law enforcement authorities in the EU also rely upon key partner countries to detect and investigate criminals and terrorists. **Security partnerships between the EU and third countries** could be stepped up in order to increase cooperation to counter shared threats such as terrorism, organised crime, cybercrime, child sexual abuse and trafficking in human beings. Such an approach would be based on common security interests and builds on established cooperation and security dialogues.

As well as information, exchange of expertise can be of particular value in increasing the preparedness of law enforcement to **non-traditional threats**. As well as encouraging exchanges of best practice, the Commission will explore a possible **EU-level coordination mechanism for police forces** in case of force majeure events such as pandemics. The pandemic has also proven that Digital Community Policing, accompanied by legal frameworks to facilitate online policing, will be fundamental in tackling crime and terrorism. Police-community partnerships, off and online, can prevent crime and mitigate the impact of organised crime, radicalisation and terrorist activities. The connection from local to regional to national and EU police solutions is a key success factor for the EU Security Union as a whole.

The contribution of strong external borders

Modern and efficient management of external borders has the dual benefit of maintaining the integrity of Schengen and providing security for our citizens. Engaging all relevant actors to make the most of security at the border can have a real impact on the prevention of cross-border crime and terrorism. Joint operational activities of the recently strengthened European Border and Coast Guard[119] contribute to the prevention and detection of cross-border crime at the **external borders** and beyond the EU. Customs activities in detecting safety and security risks in all goods before they arrive in the EU and in controlling goods when they arrive are crucial in the fight against cross-border crime and terrorism. The forthcoming Action Plan on the Customs Union will announce actions to also strengthen risk management and to enhance internal security, including in particular by assessing the feasibility of a link between relevant information systems for security risk analysis.

The framework for **interoperability between EU information systems** in the area of justice and home affairs was adopted in May 2019. This new architecture seeks to improve the efficiency and effectiveness of the new or upgraded information systems.[120] It will lead to faster, more systematic information for law enforcement officers, border guards and migration officials. It will help correct identification and contribute to fighting identity fraud. To make this a reality, implementation of interoperability should be a priority, both at

[119] Composed of European Border and Coast Guard Agency (Frontex) and the Member States' border guard authorities and coast guard authorities.

[120] The Entry Exit System (EES), the European Travel Information and Authorization System (ETIAS), the extended European Criminal Records Information System (ECRIS-TCN), the Schengen Information System, the Visa Information System and the future updated Eurodac.

political and technical level. Close cooperation between EU agencies and all Member States will be paramount in order to achieve the goal of full interoperability by 2023.

Travel document fraud is considered one of the most frequently committed crimes. It facilitates the clandestine movement of criminals and terrorists, and plays a key role in trafficking in human beings and in the drugs trade.[121] The Commission will explore how to extend existing work on the security standards of EU residence and travel documents, including through digitalisation. As of August 2021, Member States will start issuing identity cards and residence documents according to harmonised security standards, including a chip containing biometric identifiers that can be verified by all EU border authorities. The Commission will monitor the implementation of these new rules, including the gradual replacement of documents currently in circulation.

Strengthening security research and innovation

Work to ensure cybersecurity and to combat organised crime, cybercrime and terrorism all rely heavily on developing tools for this future: to help create safer and more secure new technologies, to address the challenges brought about by technologies, and to support the work of law enforcement. This in turn relies on private partners and industries.

Innovation should be seen as a strategic tool to counter current threats and to anticipate both future risks and opportunities. Innovative technologies can bring new tools to help law enforcement and other security actors. Artificial intelligence and big data analytics could harness high-performance computing to offer better detection and quick, comprehensive analysis.[122] A key precondition to develop reliable technologies is high quality data sets, available to the competent authorities to train, test and validate algorithms.[123] More generally, the risk of technological dependence today is strong – the EU is for example a net importer of cybersecurity products and services, with all this entails for the economy and for critical infrastructures. To master technology and guarantee continuity of supply also in case of adverse events and crises, Europe needs presence and capacity in the critical parts of the relevant value chains.

EU **research, innovation and technological development** offer the opportunity to take the security dimension into account as these technologies and their application are developed. The next generation of EU funding proposals can act as a major stimulus.[124] Initiatives on European data spaces and cloud infrastructures have security factored in from the start. The European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[125] aim to set up an effective and efficient structure to pool and share cybersecurity research capacities and outcomes. The EU Space

[121] The link between document fraud and human trafficking is set out in Second report on the progress made in the fight against trafficking in human beings, COM(2018) 777 and the accompanying SWD(2018) 473 and Europol, Situation Report Trafficking in human beings in the EU, 2016.

[122] This should draw on the Commission's strategy on Artificial Intelligence.

[123] A European strategy for data, COM(2020) 66 final.

[124] The Commission's proposals for Horizon Europe, the Internal Security Fund, the Integrated Border Management Fund, the EUInvest Programme, the European Regional Development Fund and the Digital Europe Programme will all support the development and deployment of innovative security technologies and solutions along the security value chain.

[125] Proposal of 12 September 2018 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, COM(2018) 630.

programme delivers services supporting the security of the EU, its Member States and individuals.[126]

With over 600 projects launched for an overall value close to €3 billion since 2007, EU-funded security research is a key instrument to drive technology and knowledge in support of security solutions. As part of the review of Europol's mandate, the Commission will look into the creation of a **European Innovation hub for internal security**[127] that would seek to deliver common solutions to shared security challenges and opportunities, which Member States might not be able to exploit alone. Cooperation is fundamental to focus investment to best effect and to develop innovative technologies with both a security and an economic benefit.

Skills and awareness raising

Awareness of security issues and acquiring the skills to deal with potential threats are essential to build a more resilient society with better prepared enterprises, administrations and individuals. Challenges to IT infrastructure and e-systems have revealed the need to improve our human capacity for cybersecurity preparedness and response. The pandemic has also highlighted the importance of digitalisation across all areas of the EU economy and society.

Even a **basic knowledge of security threats** and how to combat them can have a real impact on society's resilience. Consciousness of the risks of cybercrime and the need to protect oneself from it can work together with protection from service providers to counter cyber-attacks. Information about the dangers and risks of drug trafficking can make it more difficult for criminals to succeed. The EU can stimulate the spread of best practice such as through the network of Safer Internet Centres[128] and ensure that such goals are factored into its own programmes.

The future Digital Education Action Plan should include targeted measures to build security IT skills for the whole population. The recently adopted Skills Agenda[129] supports skills building throughout life. It includes dedicated actions to increase the number of graduates in science, technology, engineering, arts and mathematics needed in cutting-edge areas such as cybersecurity. Additional actions, financed by the Digital Europe Programme will allow professionals to keep pace with evolutions in the security threat landscape and, at the same time, fill the shortages in this field the EU labour market. The overall impact will be to allow individuals to acquire skills to deal with security threats and businesses to find the professionals they need in this area. The upcoming European Research Area and European Education Area will also promote careers in science, technology, engineering, arts and mathematics.

Also important is **victims**' access to their rights; they must receive the necessary assistance and support they need given their specific circumstances. Particular efforts are required

[126] For instance, Copernicus provides services allowing the surveillance of EU external borders and maritime surveillance which helps action against piracy and smuggling, as well as supporting critical infrastructures. Once fully operational, this will be a key enabler for civil and military missions and operations.

[127] This would work also with EBCGA/Frontex, CEPOL, eu-LISA and the Joint Research Centre.

[128] See www.betterinternetforkids.eu: the central portal and the national Safer Internet Centres are currently funded under CEF/Telecom, future funding has been proposed under Digital Europe Programme.

[129] European Skills Agenda for sustainable competitiveness, social fairness and resilience, COM(2020) 274 final

when it comes to minorities and the most vulnerable victims, such as children or women trafficked for sexual exploitation or exposed to domestic violence.[130]

There is a particular role for enhanced **skills in law enforcement**. The current and new technological threats calls for more investment in upskilling law enforcement personnel at the earliest stage and throughout their career. CEPOL is an essential partner to assist Member States in this task. Law enforcement training related to racism and xenophobia, and citizens' rights more generally, must be an essential component of an EU culture of security. National justice systems and justice practitioners must also be equipped to adapt and respond to unprecedented challenges. Training is essential to allow authorities on the ground to exploit these tools in an operational situation. In addition, all efforts should be made to reinforce gender mainstreaming and strengthen women's participation in law enforcement.

Key actions
• Strengthening of Europol mandate • Exploring an EU 'Police Cooperation Code' and police coordination in times of crisis • Strengthening Eurojust to link judicial and law enforcement authorities • Revision of the Advance Passenger Information Directive • Communication on the external dimension of Passenger Name Records • Strengthening cooperation between the EU and Interpol • A framework to negotiate with key third countries on sharing of information • Better security standards for travel documents • Exploring a European Innovation hub for internal security

V. Conclusions

In an increasingly turbulent world, the European Union is still widely regarded as one of the safest and most secure places. However, this is not something that can be taken for granted.

The new Security Union strategy lays the foundations for a security ecosystem that spans the entire breadth of European society. It is grounded in the knowledge that security is a shared responsibility. Security is an issue that affects everyone. All government bodies, businesses, social organisations, institutions and citizens must fulfil their own responsibilities in order to make our societies more secure.

Security issues now need to be viewed from a much broader perspective than in the past. False distinctions between the physical and digital need to be overcome. The EU Security Union Strategy brings together the full range of security needs and focuses on the areas most critical to EU security in the years to come. It also acknowledges that security threats do not respect geographical borders, as well as the increasing inter-connection between internal and external security.[131] In that context, it will be important for the EU to cooperate with international partners for the safeguard of all the EU citizens and to maintain close coordination with EU external action in the implementation of this Strategy.

Our security is linked to our fundamental values. All the proposed actions and initiatives in this strategy will fully respect fundamental rights and our European values. These are the foundation of our European way of life and must remain at the core of all our work.

[130] See Gender equality strategy, COM(2020) 152; Victims' rights strategy, COM(2020) 258; and the European Strategy for Better Internet for Children, COM(2012) 196.

[131] See the EU Global Strategy

Lastly, the Commission remains fully aware of the fact that any policy or action is only ever as good as its implementation. Relentless emphasis is therefore needed on the proper implementation and enforcement of existing and future legislation. This will be monitored through regular Security Union reports and the Commission will keep the European Parliament, the Council and stakeholders fully informed and engaged in all relevant actions. In addition, the Commission stands ready to participate in and organise joint debates with the institutions on the Security Union Strategy in order to take stock together of progress achieved while looking together at the challenges ahead.

The Commission invites the European Parliament and the Council to endorse this Security Union Strategy as the basis for cooperation and joint action on security in the next five years.