



Plenary sitting

A8-0374/2018

21.11.2018

REPORT

on findings and recommendations of the Special Committee on Terrorism
(2018/2044(INI))

Special Committee on Terrorism

Rapporteur: Monika Hohlmeier and Helga Stevens

CONTENTS

	Page
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION	3
EXPLANATORY STATEMENT	56
INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE	60
FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE.....	61

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI))

The European Parliament,

- having regard to its decision of 6 July 2017 on setting up a special committee on terrorism, its responsibilities, numerical strength and term of office¹, adopted under Rule 197 of its Rules of Procedure,
- having regard to Rule 52 of its Rules of Procedure,
- having regard to the report of the Special Committee on Terrorism (A8-0374/2018),

Preamble

- A. whereas the Union is founded on the values of human dignity, freedom, equality and solidarity, respect for human rights and fundamental freedoms, as well as on the principles of democracy and the rule of law; whereas acts of terrorism constitute one of the most serious violations of these universal values and principles;
- B. whereas the EU should do the utmost possible to guarantee the physical and mental integrity of its citizens who are endangered by terrorists; whereas the fight against terrorism requires putting its victims at the centre; whereas societies must protect, recognise, support and compensate victims of terrorism; whereas Article 6 of the Charter of Fundamental Rights enshrines both the right to liberty and the right to security, which complement each other;
- C. whereas the response to the terrorist threat should always be in full compliance with the principles recognised by Article 2 TEU and should observe fundamental rights and freedoms, as well as the principles recognised, in particular, by the Charter of Fundamental Rights, considering the possible effect on innocent people who make up the vast majority of the population;
- D. whereas terrorism in all its forms and manifestations, committed by whomever, wherever and for whatever purposes, must be condemned, as it constitutes one of the most serious threats to international peace and security;
- E. whereas the terrorist threat has grown and rapidly evolved in recent years; whereas terrorist attacks have affected all of us deeply and have claimed the lives of and injured many innocent people; whereas the cross-border nature of terrorism requires a strong coordinated response and cooperation within and between the Member States, as well as with and among the competent Union agencies and bodies, and with relevant third countries;

Institutional framework

- F. whereas the security of one Member State is the security of all in the Union; whereas the

¹ Texts adopted, P8_TA(2017)0307.

threats posed by terrorism require a holistic approach linking internal and external security and ensuring national and European coordination; whereas the EU and the Member States have made progress in countering these threats, but this progress is unfortunately made under pressure of events rather than through pro-active measures, and the same level of progress is not being achieved across all Member States;

- G. whereas national security is the sole responsibility of the Member States as laid down in Article 4(2) TEU and Article 73 TFEU, while according to Article 4(3) and Article 42 TEU, the Union and the Member States shall assist each other in carrying out tasks which stem from the Treaties; whereas national security is increasingly dependent on its broader European dimension; whereas national security is not defined at EU level thus leaving a wide margin of discretion to Member States;
- H. whereas at the same time Article 4(2) TFEU designates the area of freedom, security and justice as an area of shared competence between the Union and the Member States; whereas the EU has specific competences as regards facilitating and encouraging coordination and cooperation between Member States, including harmonisation of the laws and practices of the Member States; whereas the mandate for EU action is provided by Article 67 TFEU to ensure a 'high level of security through measures to prevent and combat crime';
- I. whereas the national security and intelligence agencies of EU Member States and of some third countries cooperate effectively through the Counter Terrorism Group (CTG), an informal body outside the EU, and on a bilateral and multilateral basis; whereas the CTG has a platform for the exchange of operational intelligence that has improved the speed and quality of shared intelligence; whereas the EU has an established complex of structures dealing wholly or in part with terrorism, notably through Europol's European Counter Terrorism Centre (ECTC) as the central hub for law enforcement information exchange and cooperation in the field of counter-terrorism at EU level, and the EU Intelligence and Situation Centre (INTCEN) as the gateway for strategic intelligence from the intelligence and security services to the EU through which CTG information reaches European policy makers, and this is facilitated by the European Counter-Terrorism Coordinator;
- J. whereas the line between EU and national competence is not always clear because of different characteristics and geographical prerogatives, thus underlining the importance of cooperation between the two governance levels; whereas the diverse landscape of regional, national, EU and international actors in the fight against terrorism with overlapping competences and insufficiently delineated mandates, the multitude of formal and informal fora for cooperation and exchange of information, as well as the division of competences between the different regional and national agencies, between law enforcement services and intelligence services and between the EU and the Member States, underline the complexity of, and may give rise to difficulties with regard to, the coordination, efficiency and coherence of the response to the terrorist threat;
- K. whereas the Commissioner for Security Union is a valued actor in joining up the Commission's policy development, implementation, monitoring and evaluation; whereas the establishment of the position of Commissioner for Security Union signals the EU's commitment to encouraging and supporting cooperation between Member States on

issues of internal security, as well as to harmonising counter-terrorism legislation and ensuring better cooperation between law enforcement and judicial authorities, while fully respecting the status of these matters as national competencies as laid down in the Treaties;

- L. whereas the EU Counter-Terrorism Coordinator plays an important role in tracking the implementation of the EU counter-terrorism strategy; whereas the EU Counter-Terrorism Coordinator, in accordance with his or her mandate as determined by the European Council, ensures the implementation and assessment of the strategy and the coordination of work within the Union, and facilitates contact between the Union and third countries; whereas the EU Counter-Terrorism Coordinator provides valuable advice to, maintains contacts with, and helps strengthen the coordination between EU institutions, agencies and Member States; whereas his or her mandate and status are nevertheless ill-defined;
- M. whereas on 6 July 2017 Parliament set up a temporary Special Committee on Terrorism (TERR) with the aim of providing Parliament's view as to the practical and legislative gaps in the current counter-terrorism regime that have allowed the recent terrorist attacks in the EU to occur and to making recommendations that would help tackle the terrorist threat at EU level;
- N. whereas the European Public Prosecutor's Office, to be established on the basis of Council Regulation (EU) 2017/1939, shall have the important task of investigating and prosecuting criminal offences affecting the financial interests of the Union; whereas its establishment and the allocation of financial resources to this new body should not negatively impact the abilities of existing structures, such as Eurojust, to facilitate the efforts of the Member States in the fight against terrorism;
- O. whereas of 88 legally binding counter-terrorism measures proposed from September 2001 to summer 2013 only a quarter were subject to impact assessments and only three to public consultation¹; whereas this ratio has improved in recent years and the most recent initiatives presented by the Commission in 2017 and 2018 were accompanied by the necessary justification; whereas with the Agenda on Better Regulation adopted in 2015 the Commission has also strengthened its policy on stakeholder consultation; whereas counter-terrorism measures could be more effective and coherent if appropriate stakeholders are consulted and impact assessments are conducted;
- P. whereas the Commission's Comprehensive Assessment of EU Security Policy mentioned incomplete implementation as one of the challenges of the Security Union;
- Q. whereas evaluation of counter-terrorism measures is vital for assessing their effectiveness, relevance, coherence and compliance with fundamental rights, and determining whether additional action is necessary to address the shortcomings; whereas a difference exists between monitoring the extent of implementation and the actual effectiveness of implemented measures; whereas between 2001 and 2016 there were 17 monitoring implementation and evaluation reports compared to 10 counter-terrorism strategies and 55 legislative and non-binding measures; whereas it is necessary for

¹ Study on The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, [http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU\(2017\)583124_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf)

Member States to implement EU security laws quickly so that no loopholes emerge in the EU's comprehensive body of counter-terrorism measures;

Terrorist threat

- R. whereas in recent years, the EU Member States have suffered major terrorist attacks; whereas the deadliest attacks have been perpetrated or inspired by jihadist groups such as Daesh and Al Qaeda; whereas these terrorist groups¹ and their activities are sometimes facilitated by certain countries; whereas far right, far left and ethno-nationalist separatist violent extremism, aimed at overthrowing the democratic values and system governed by the rule of law in the EU through the illegitimate use of violence, also remain matters of concern;
- S. whereas, while most terrorist attacks carried out in the EU in 2017 were specified as separatist attacks (137 out of 205), Europol's TESAT 2018 report clearly states that none of the reported activities in any terrorist category have been as lethal and have had such an impact on society as a whole as those committed by jihadist terrorists; whereas the growing risk of retribution terrorism is a serious concern which should not be underestimated;
- T. whereas, as long as a terrorist attack is a 'widespread or systematic attack directed against any civilian population', terrorist murders should be covered by and fall under Article 7 of the Rome Statute of the International Criminal Court of 17 July 1998;
- U. whereas developments and instability in the Middle East and North Africa (MENA) have enabled Daesh and other terrorist groups to gain a foothold in countries bordering the EU and to recruit fighters from the EU on an unprecedented scale; whereas as a result the nexus between internal and external security has become more prominent;
- V. whereas thousands of European-born or resident citizens joined Daesh in terrorist activities in Syria and Iraq, but there has been a change of strategy since the military collapse of Daesh, with a decline in the numbers of those travelling to these countries for terrorist purposes, and terrorist jihadists and 'sleeper-cells' inside the EU being encouraged to carry out attacks in their home countries or countries of residence;
- W. whereas recent attacks have demonstrated that firearms and explosives are still traditional methods used by terrorist groups; whereas, however, there is a growing use by individuals of other weapons and methods that are much less sophisticated and more difficult to detect, aiming to cause a maximum number of random casualties among civilians;
- X. whereas the return of foreign terrorist fighters (FTFs) and their families poses particular challenges in terms of security and radicalisation, especially child returnees who pose specific problems as they need protection as victims but at the same time can also be potential perpetrators;
- Y. whereas some of these returnees have received prolonged ideological indoctrination and military training in the use of weapons and explosives, as well as various cover, assault and combat tactics, and have in some cases established links with other terrorists, possibly

¹ <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018D1084>

former foreign fighters, with whom they form transnational networks¹;

- Z. whereas perpetrators of terrorist attacks in the EU very often include EU nationals, often second- or third-generation migrants, who have grown up in the Member States which they have attacked, as well as foreigners who may in some cases have resided for a significant time in the Member State targeted;
- AA. whereas our open societies and open borders are vulnerable and are exploited by terrorist groups; whereas terrorists have made use of migrants' and asylum seekers' routes of access to European countries, exploiting the freedom of movement across Europe;
- AB. whereas there are documented cases² in which victims of severe crimes perpetrated by Daesh terrorists on Syrian or Iraqi territory have – despite considering themselves safe – met their tormentors again on EU soil where both have asked for protection;
- AC. whereas the flow of irregular migrants and refugees poses challenges to their integration into European societies and requires reinforced and specific investment directed towards social and cultural inclusion;
- AD. whereas new forms of terrorism may be used for an attack, among them cyber-terrorism and the use of weapons of mass destruction, possibly in connection with new technical equipment such as drones; whereas there is the precedent of a foiled attack involving the highly toxic biological agent ricin; whereas there are cases where terrorist groups have used or planned to use chemical, biological, radiological or nuclear (CBRN) materials, and shared via social media channels possible tactics and methods for attacks and targets;
- AE. whereas Member States have different strategies to respond to hybrid and CBRN-related threats and therefore different levels of preparedness;
- AF. whereas the European Council on 28 June 2018 welcomed the Joint Communication on Europe's resilience to hybrid and CBRN-related threats, seeking to identify areas where action should be intensified in order to further deepen and strengthen the EU's essential contribution to addressing these threats, as well as urging Member States and the Commission to work together to fully implement the CBRN Action Plan as a matter of urgency;
- AG. whereas caution should be used in political discourse exploited by both left- and right-wing agitators regarding or invoking the terrorist threat so as to avoid polarisation within societies and not to undermine democracy, social cohesion and human rights, thus playing into the hands and aims of terrorist organisations;
- AH. whereas the European Agenda on Security of April 2015 highlighted the need to tackle the nexus between terrorism and organised crime, underlining that organised crime feeds terrorism through various different channels, *inter alia* supplying weapons, financing through drug smuggling, and infiltrating financial markets;
- AI. whereas large-scale international terrorist organisations such as Daesh and Al-Qaeda are

¹ 2017 Europol TE-SAT report (page 14).

² <https://www.dw.com/de/jesidin-trifft-in-deutschland-auf-is-peiniger/a-45119776>

financially self-reliant and whereas illicit trade in goods, weapons, raw materials, fuels, drugs, cigarettes and cultural objects, among other items, as well as trafficking in human beings, slavery, child exploitation, racketeering and extortion, have proved to be means for terrorist groups to obtain funding; whereas the link between organised crime and terrorist groups constitutes a major security threat; whereas these sources could enable the continued funding of their future criminal activities;

- AJ. whereas significant risks are posed by interactions between terrorist organisations and organised crime groups, through which the capability to cause mass casualties among the civilian population of EU Member States connects with the logistical capacity to enable it; whereas there is a low level of law enforcement and intelligence reporting and analysis on the nexus between organised crime and terrorism; whereas investigative and judicial capacities focused on organised crime are often lacking in many Member States and at EU level;
- AK. whereas terrorism seeks to weaken and defeat democracies; whereas politicians and governments are crucial actors for achieving broad consensus and social resilience in order to effectively defend our democratic systems;

Preventing and countering radicalisation leading to violent extremism

- AL. whereas the Radicalisation Awareness Network (RAN) Centre of Excellence offers an important platform for the exchange of best practices among practitioners, including law enforcement authorities, and has contributed to the gathering of important knowledge in the field of preventing and countering radicalisation¹;
- AM. whereas the situation in each Member State differs and a newly revised European strategy for combating radicalisation could support national strategies, which are important in terms of providing general frameworks for programmes at national and local level; whereas these strategies must be coherent and effective and need sufficient financing for local authorities and civil society stakeholders so that these programmes can be implemented;
- AN. whereas it is impossible to identify only one path towards radicalisation; whereas, for instance, social cohesion, political context, economic condition, religious and ideological ideals, personal traumas and psychological vulnerabilities, as well as surroundings and networks, may constitute factors and triggers; whereas the gender dimension was until recently underestimated and there is a misconception about the role women can play; whereas women are not always passive subjects and they also act as mobilisers, recruiters, fundraisers and even as perpetrators of terrorist acts;
- AO. whereas some low-income neighbourhoods in European cities are facing mass unemployment and the systematic breakdown of the rule of law, creating the breeding grounds for religious extremism and terrorism; whereas the promotion of social inclusion and the active promotion of democratic values which all citizens must respect can help to

¹ Radicalisation is understood to mean a complex process by which an individual or a group comes to adopt increasingly extreme religious and/or political ideas/views potentially leading to violent actions, including the commission of terrorist acts. In line with Commission policy documents, any reference to ‘radicalisation’ is to be understood as ‘radicalisation leading to violent extremism and terrorism’.

reduce feelings of marginalisation and mitigate the risk of radicalisation; whereas combating radicalisation and violent extremism requires close and coordinated collaboration between all actors concerned at all levels of governance (local, regional and national), as well as with civil society and the private sector;

- AP. whereas experts highlight the positive experience offered by a multi-agency approach, focusing on creating infrastructures which take into account the various routes to radicalisation and the demographics at risk, and which ensure the provision of early-stage support to those vulnerable to radicalisation and their families from different authorities and organisations across multiple levels, and emphasising the supportive role of the police, thus strengthening the relationship;
- AQ. whereas so far no clear methodologies exist to measure the effectiveness of projects for preventing and countering radicalisation;
- AR. whereas several European funds and programmes can be used for projects countering and preventing radicalisation at the European, national, regional and local levels; whereas the EU budget up to 2020 allocates EUR 314 million for anti-radicalisation projects¹; whereas there is a need for a continuous evaluation of the effectiveness of those programmes; whereas measuring the effectiveness of preventive counter-radicalisation actions is intrinsically difficult and requires close cooperation between the Commission, Member States, individual stakeholders and researchers;
- AS. whereas Europol estimates that there were around 30 000 radicalised jihadists in the EU by 2018;
- AT. whereas a violent radicalised extremist discourse has been increasingly present in the territory of many EU Member States, often in printed form, or as teaching or audiovisual content, including on social media and satellite TV channels; whereas this discourse opposes democracy, the rule of law and human rights, undermines pluralism, promotes violence and intolerance against all other religions, is openly anti-Semitic, refuses equality between men and women, and promotes a retrograde model of culture and society;
- AU. whereas there is a prevalence of specifically Wahhabi and Salafist literature, which is fuelled by hate speech, available in certain bookshops and online in Europe; whereas this globalised and simplistic version of Islam breaks with the practices of Muslim communities in Europe and contributes to undermining their broader integration;
- AV. whereas it is the aspiration of Radical Islamic Fundamentalism for religion to dominate all spheres of life – individual, political and social – the consequence of which may be a form of communitarianism sensitive to the actions of jihadist recruiters;
- AW. whereas significant numbers of cases of radical hate preachers have been documented throughout Europe; whereas the hate preachers often originate from outside the EU, while some mosques receive opaque funding from third countries, many of which have

¹ Speech by Commissioner Jourová, in charge of Justice, Consumers and Gender Equality, at the Conference on Radicalisation in Prisons in Brussels on 27 February 2018, http://europa.eu/rapid/press-release_SPEECH-18-1221_en.htm

authoritarian or religious regimes that do not govern in accordance with democracy, the rule of law and human rights;

- AX. whereas there are self-designated religious teaching centres propagating extremist ideas in the EU, in which minors, including young children, may be exposed to a learning content contrary to democracy, the rule of law and human rights, and including violent content; whereas extremist organisations laying the ground for terrorist recruitment often exploit the vulnerabilities of young people by attracting them with social and cultural offers;
- AY. whereas the sophisticated web communication strategy of marketing terrorism by glorifying it, employed especially by Daesh, but also by other large-scale international terrorist groups, offers design copied from the global ‘youth culture’ such as online gaming, and thus has a strong appeal to children and young people; whereas this model is also luring them with social and cultural opportunities;
- AZ. whereas several recent investigations have shown that the internet and namely social media can act as a driver of radicalisation leading to violent extremism, as well as a tool for xenophobic groups to disseminate hate speech and illicit content especially among young people;
- BA. whereas following repeated calls for better commitment to countering terrorism, major internet companies are facing up to their responsibilities; whereas in the European Internet Forum launched in 2015 companies cooperate to remove terrorist content from their websites on a voluntary basis if they believe it is in breach of their terms and conditions; whereas a code of conduct for major IT companies was implemented in May 2016 with the aim of tackling illegal hate speech online; whereas this voluntary cooperation is nevertheless insufficient;
- BB. whereas by the end of the second quarter of 2018 Europol’s European Internet Referral Unit (EU IRU) had already assessed 54 752 pieces of content produced in 10 different languages across 170 online platforms, triggering 52 716 decisions for referral with a removal success rate of 89.5 % on the basis of voluntary consideration of abused OSPs¹;
- BC. whereas, although some progress has been made with regard to removal of online terrorist content, there is a need to scale up the companies’ engagement; whereas the removals are often neither complete, nor timely or permanent, the content being removed from one website but left on another belonging to the same company or the account being allowed to remain live and/or reappear after it has posted content in violation of a company’s terms of service; whereas effective, comprehensive and transparent reporting by companies and law enforcement has to be improved; whereas the companies and users in question should be able to seek judicial redress;
- BD. whereas, in response to larger companies removing more content, terrorist groups are increasingly using new and/or smaller platforms which are less suited to fast removal of terrorist material; whereas this diversification to smaller platforms makes additional technical support essential to enable, for example, the introduction of platform-agnostic automated tools, such as hashing technology, which can identify online terrorist content

¹ Europol, 6 September 2018.

in advance with a high degree of accuracy and prevent publication;

- BE. whereas the development of new technologies and access to artificial intelligence and algorithms may allow online terrorist content to be identified and reported swiftly; whereas the use of automated tools also carries risks of false hits;
- BF. whereas studies and reports show how prisons can easily evolve into microcosms of the crime-terror nexus, where recruitment and networking take place; whereas the internal situation in many prisons accelerates the threat of radicalisation of offenders, incubating and enabling terrorism; whereas many of those serving prison sentences will soon be released back into their communities, posing particular reintegration challenges and high risk of re-offending; whereas monitoring of such high-risk offenders is extremely resource-intensive for Member States' security services; whereas prison regimes and risk management can play a significant role in mitigating these threats; whereas even though Member States recognise the need to address the rise in prison radicalisation, more effective measures are needed;

Cooperation and information exchange

Horizontal issues

- BG. whereas retention of data, taking account of ECJ case law, is an essential part of the investigative process; whereas the police and judicial authorities and intelligence services usually rely heavily on communications data to successfully proceed with their casework; whereas the necessity of an appropriate data retention regime when it comes to the fight against terrorism was consistently raised during the work of the TERR Committee;
- BH. whereas the use of encryption will on the one hand make a significant contribution to security in the field of IT, but on the other hand will also be used by terrorists to protect their communications or stored data, which represents a considerable challenge for law enforcement, security and intelligence services, since they can be denied access to essential intelligence and evidence; whereas encryption becomes particularly critical when even the responsible online service providers are unwilling or unable to decrypt the communication;

Information systems

- BI. whereas there is a fragmented framework of existing systems, new systems in the process of development, proposals for future systems and proposals for reforms to address identified gaps and barriers still under negotiation; whereas this fragmented framework is the result of historical factors and a reactive approach in the proposal and adoption of new legislation;
- BJ. whereas there has been a significant increase in information exchanges since the Paris attacks in 2015, but data about information exchanges show that a small number of Member States are responsible for a large proportion of available content in and searches of EU databases;
- BK. whereas there are a number of obstacles to the proper functioning of the information systems, such as a complete lack of or incomplete implementation, lack of knowledge of

and/or sufficient training in the existing systems, lack of sufficient resources, including human resources, or of an adequate material base, and poor data quality in the information systems;

- BL. whereas information systems can be divided into centralised and decentralised systems, the former being managed by the EU and its agencies and the latter by the Member States; whereas centralised information systems include the Schengen Information System (SIS), the Visa Information System (VIS), Eurodac, the Entry/Exit System (EES), the proposed European Travel Information and Authorisation System (ETIAS) and the proposed European criminal records information system for third country nationals (ECRIS-TCN);
- BM. whereas decentralised systems and mechanisms for information exchange are managed by the Member States' authorities and include: the European Criminal Records Information System (ECRIS) for exchanging national criminal record information; the EU passenger name records (PNR) system requiring airlines to share passengers' data with national authorities for all flights between third countries and the EU; the Advance Passenger Information (API) system that collects information on passengers ahead of inbound flights to the EU; and the Prüm framework for exchanging DNA, fingerprints and vehicle registration data;
- BN. whereas the SIS is the biggest, most widely used and most efficient IT system of the European Union in the area of freedom, security and justice, and is supported by the network of SIRENE Bureaux, providing significant added value in the field of international police cooperation and border control and particularly in the fight against terrorism;
- BO. whereas the 2016 evaluation of VIS found that access to VIS for law enforcement purposes has been limited and fragmented across Member States;
- BP. whereas despite repeated calls to implement an EU system for recording passenger details (PNR), each Member State has not demonstrated commitment to this and the majority of Member States have not complied with the deadline for implementing this law; whereas Member States that miss this deadline should without any further delay undertake all necessary action to implement this directive in full with immediate effect;
- BQ. whereas several pilot projects are being implemented with the aim of overcoming the disadvantages of a decentralised EU PNR system; whereas there is a need for a quick reply to requests from passenger information units (PIUs) of other Member States, which may prove challenging as they are processed manually;
- BR. whereas – in the context of the Information Management Strategy (IMS) 6th Action List – there are currently two on-going pilot projects which aim to ensure interlinking with decentralised systems, namely ADEP (Automation of data exchange processes on police records) and QUEST (Querying Europol Systems); whereas six Member States are already involved in the ADEP pilot project for the automated transmission of police records between different countries and this project is working well; whereas such projects help provide real and workable solutions to the problems stemming from the lack of interconnectivity of decentralised information systems and help foster trust and cooperation between the Member States;

Interoperability

- BS. whereas the Commission put forward two proposals for a regulation establishing a framework for interoperability between existing and proposed centralised information systems in the fields of police and judicial cooperation, asylum and migration, borders and visas, namely VIS, SIS, EES and Eurodac, as well as ETIAS and ECRIS-TCN once the respective legal bases are adopted;
- BT. whereas criminals can still today be recorded in different databases that are not connected under different aliases; whereas the current EU data management architecture therefore needs to be improved by interoperability to eliminate blind spots and multiple false identities and provide the right information at the right time;
- BU. whereas within the territory of one Member State there may be a multitude of separate decentralised databases at federal, regional and local level, with different data inputs in different systems and complex procedures - or none at all - for the sharing or checking of the data by the relevant authorities at the different levels;
- BV. whereas the use of a common messaging format at EU level, such as a universal message format (UMF), will facilitate smoother exchange of data and information between parties and across interoperability systems; whereas establishing the need to use certain UMF fields for particular exchanges can contribute to the improvement of data quality in all of the systems across which messages are being exchanged; whereas the use of this common message format by Europol and Interpol should also be encouraged;
- BW. whereas eu-LISA should establish automated data quality control mechanisms and procedures as well as common data quality indicators and minimum quality standards for data stored in the information systems; whereas the goal would be for the EU information systems and interoperability components to automatically identify apparently incorrect or inconsistent data submissions so that the originating Member State is able to verify the data and carry out any necessary remedial actions;

Cooperation and exchange of information within and between Member States

- BX. whereas obstacles to a more fluid cooperation often stem from organisational and legal difficulties between the different national, regional and local structures within the Member States themselves, such as: overlapping competences and insufficiently delineated mandates; hesitancy to share information as this might result in loss of responsibility or loss of important information flows; legal obstacles when it comes to sharing information between different authorities; services being obliged to compete with each other for resources; and technical barriers to information exchange;
- BY. whereas the principle of data ownership is crucial for ensuring the confidence of counter-terrorism authorities in sharing information via EU databases between Member States and with Europol;
- BZ. whereas mixing intelligence and law enforcement information entails major legal challenges and risks due to the different accountability rules applying to both types of information, including risks to the fundamental right of suspects to a fair trial when intelligence information is used as evidence in court proceedings; whereas a legal

framework must be put in place for information exchange between intelligence and law enforcement authorities, especially since intelligence often concerns information on people who are not yet suspects within the framework of criminal investigations but might belong to terrorist networks or may be returning FTFs; whereas, however, this must not lead to any lowering of legal standards;

- CA. whereas policing and intelligence services receive, process and transfer both classified and unclassified information, which involves different regimes at every stage of using the information; whereas it is also necessary to distinguish between information used as intelligence, i.e. information that is processed by professionals for a specific purpose, and regular information; whereas it is necessary to at least distinguish between criminal intelligence, which is related to a police criminal case, from security intelligence, which is processed within an administrative framework;
- CB. whereas intelligence information should be given a special, even higher level of protection over police information because of the different working methods involved, such as the gathering of confidential information from sources and informants who must be kept anonymous, as well as the different objectives that require greater sensitivity;
- CC. whereas a possible solution could also be offered by the creation of counter-terrorism centres or units within the national territory; whereas such centres allow representatives of the different services to communicate with each other on a regular basis and discuss how best to cooperate and exchange information; whereas this helps build trust between the services and fosters a better understanding of their respective working methods and challenges;
- CD. whereas security services tend to cooperate and exchange information bilaterally or multilaterally – notably through the Counter Terrorism Group (CTG) and with the EU bodies via EU INTCEN – by sharing strategic intelligence; whereas it is necessary to find a practical solution to fill the existing gaps between the parallel tracks of the law enforcement community and the intelligence community, for example by identifying specific areas of cooperation, in order to allow for more efficient cooperation, while still keeping them separate;
- CE. whereas it is possible to increase effectiveness in the use of the Counter Terrorism Group (CTG) and the EU Intelligence and Situation Centre (EU INTCEN) structures for the exchange of information;
- CF. whereas the Member States' civilian and military security and intelligence agencies systematically share their intelligence, including that related to terrorism, with the EU Intelligence and Situation Centre (EU INTCEN) within the External Action Service (EEAS) which provides intelligence analysis, early warning and situational awareness to the various EU decision-making bodies;
- CG. whereas communicating the post-hit information only to the SIRENE Bureau of the Member State issuing the alert under Article 36 and not to other Member States is sometimes insufficient for the purposes of following up the movements of individuals related to terrorism or completing the relevant information in respect of such individuals; whereas the early warning of other Member States that might be concerned could, for example, be necessary in cases where the person did not return directly to the Member

State of origin or where s(he) was accompanied by nationals of another/other Member State(s) in respect of whom no alert had been issued since they remained unknown to the latter's competent authorities;

- CH. whereas the UK Government has notified the EU of its intention to leave on 29 March 2019; whereas it has, however, expressed its wish to continue its cooperation with the EU in the area of security and counter-terrorism; whereas the EU and the UK are highly interdependent in the area of security and counter-terrorism, with the UK participating in many key EU legal instruments in the area of judicial cooperation in criminal matters and having access to many EU systems and databases for the exchange of information; whereas arrangements should be found with the EU as regards all pending proceedings; whereas any future agreement should seek to make provision for the UK and the EU to be able to continue to share, collect and analyse vital information in the fight against serious crime; whereas the withdrawal agreement should ensure a smooth transition regime and avoid, as far as possible, operational gaps or obstacles that reduce the EU's capacity to effectively fight organised crime and terrorism;

Cooperation and exchange of information with the EU agencies

- CI. whereas efficient and systematic cooperation between the Member States and the EU agencies, in accordance with their legal mandates, as well as among the agencies in the counter-terrorism field, is imperative, especially cooperation between Europol and Eurojust in order to more effectively support the efforts to detect, prevent, investigate and prosecute the perpetrators of a terrorist attack; whereas Eurojust has appointed a specialised counter-terrorism prosecutor to make the bridge with the ECTC at Europol in order to increase cooperation and information exchange between the two agencies;
- CJ. whereas information exchange between EU agencies is not ideal because of the use of different secure means of communication; whereas the establishment of an interinstitutional secure means of communication could facilitate and improve information exchange between agencies such as EU INTCEN, Europol and Frontex;
- CK. whereas designated CT Liaison Officers can bring added value both to the work of the agencies and to their own Member States;
- CL. whereas there are differences in the Member States as to the number of competent authorities that can consult the Europol databases or be in contact with Europol without going through the national liaison officers; whereas some Member States lack restricted and safe national police communication networks, preventing their competent authorities from decentralised access, particularly to the Secure Information Exchange Network Application CT-SIENA;
- CM. whereas several EU instruments such as Decision 2005/671/JHA, the CT Directive and the Europol regulation require Member States to share information on terrorism with the relevant agencies; whereas increased information sharing with Europol and Eurojust on a regular basis and in a timely and systematic manner, including contextual information, in accordance with their legal mandates, facilitates their work in detecting links between cases and providing an overview of challenges and best practice related to investigations, prosecutions and convictions for terrorist offences; whereas within the framework of Decision 2005/671/JHA, Member States still do not spontaneously exchange relevant

information with other Member States where such information could be used in the prevention, detection, investigation or prosecution of terrorist offences; whereas information shared with Eurojust has increased over the past years, but differences continue to exist between the Member States in relation to the amount, type and scope of the information shared, which may result in fragmentation of the information available;

CN. whereas CEPOL substantially contributes to counter-terrorism training for law enforcement officials of the Member States and in priority third countries;

Mutual recognition and mutual legal assistance

CO. whereas mutual legal assistance (MLA) mechanisms are progressively being replaced by mutual recognition instruments as the latter help improve cross-border cooperation between competent authorities within the EU by speeding up and streamlining the procedures; whereas the European Arrest Warrant (EAW) Decision and the European Investigation Order (EIO) Directive are examples of mutual recognition instruments that have been found by practitioners to be useful;

CP. whereas the principle of mutual recognition is, on the one hand, dependent on the existence of a high level of mutual trust between Member States and, on the other, helps increase mutual trust by allowing the authorities of different Member States to work efficiently together in the fight against terrorism;

CQ. whereas joint investigation teams (JITs) facilitate the coordination of investigations and prosecutions in cases with a cross-border dimension and allow for real-time exchange of information/evidence; whereas the practical benefits resulting from the use of JITs include improved information exchange, exchange of best practices, enhanced collection of evidence and mutual recognition of the actions carried out by the parties; whereas JITs require appropriate funding to work effectively;

CR. whereas close cooperation by online service providers (OSPs) is necessary when it comes to securing and obtaining electronic evidence at the request of the responsible law enforcement authority and based on due legal process, given its importance for investigating terrorist offences;

CS. whereas the Schengen area without internal borders is a fundamental achievement of the EU, which is only sustainable if the external borders are effectively secured and protected, illegal border crossings cease and internal security measures are adopted to face the risk of serious crimes; whereas many proposals have been adopted in order to strengthen security checks at the external borders; whereas some Member States have asked for more flexibility regarding the temporary reintroduction of checks at internal borders in the event of a serious threat to public order or public security, as proposed by the Commission;

CT. whereas on 7 April 2017, new Regulation 2017/458¹ amending the Schengen Borders Code entered into force in response, in particular, to the worsening terrorist threat in order

¹ Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the enforcement of checks against relevant databases at external borders, OJ L 74, 18.3.2017, p. 1.

to provide for systematic checks on all persons crossing the external borders, including individuals enjoying the right of free movement, against the relevant databases;

- CU. whereas some areas of the regulation governing certain fields of border control, such as the systematic consultation of databases during border checks and thorough checking of the required entry conditions, have not been implemented;
- CV. whereas the thwarted attack on the Thalys train of 21 August 2015, the Paris attacks of 13 November 2015 and the Brussels attacks of 22 March 2016 have demonstrated that in a limited number of cases, terrorists abused shortcomings in the border management policies of the EU and of several Member States, which were not ready for a mass influx; whereas it has been reported by law enforcement authorities that at least eight of these attacks' perpetrators entered the EU via irregular flows in July, August and October 2015; whereas in other cases, future perpetrators had remained in Member States in spite of being due to depart or be returned; whereas this demonstrates certain flaws in the EU's border management policies and their implementation at Member State level;
- CW. whereas the Council conclusions 10152/17 recommend to Member States that, when faced with irregular migrants, they perform checks, where relevant, at national level against databases fed and used by competent authorities and the national Automatic Fingerprint Identification System (AFIS), at European and international level against the SIS, Europol, VIS, Eurodac and Interpol databases (I-24/7 network) and more specifically Nominal data, Stolen and Lost Travel Documents (SLTD), Foreign Terrorist Fighters (FTF) and Travel Documents Associated with Notices (TDAWN);
- CX. whereas on the basis of Article 11 of Regulation (EC) 1168/2011 and the positive opinion of the European Data Protection Supervisor (EDPS), the European Border and Coast Guard Agency (EBCGA) is allowed to process personal data; whereas, however, EBCGA is experiencing difficulties in monitoring terrorism due to the short personal data retention period established by Regulation (EC) 2016/1624 that comprises only 90 days; whereas between Eurojust and EBCGA there is only a memorandum of understanding which includes the exchange of general, strategic and technical information but not the exchange of personal information; whereas there is need for a specific legal framework for EBCGA to process personal data in order to fulfil its tasks;
- CY. whereas there is a need for EBCGA officers to also access the Eurodac, SIS, EES and VIS databases at border crossing points in order to perform checks;
- CZ. whereas there are currently no minimum standards or common rules for the security of identity cards of Union citizens or of residence documents issued to Union citizens and their family members exercising their right of free movement;
- DA. whereas three quarters of the fraudulent documents detected at the external borders and in the EU imitate identity documents issued by the Member States and countries associated with the Schengen area; whereas national identity cards with a lower degree of security are the most frequently detected among the fakes;
- DB. whereas some Member States do not oblige air carriers on their territory to conduct conformity checks on passengers' personal data on their ticket and ID card or passport, which makes it difficult to ascertain whether the given identity matches the true identity

of the person; whereas this is of capital importance for flights within the EU; whereas, however, proper identity checks and the authentication of travel documents should remain tasks for the police authorities;

- DC. whereas battlefield evidence is often essential to identify potential foreign terrorist fighters and victims, and needs to be included in the relevant databases in order to reach border guards in real time, and to be shared with investigators and prosecutors for investigations and prosecutions;
- DD. whereas CSDP Naval Mission EUNAVFORMED (known as Operation Sophia) has technical and human capabilities to contribute to the fight against terrorism; whereas if it is to effectively contribute to this effort, the mandate of Operation Sophia has to be amended to specifically include the fight against terrorism, enabling it to operate throughout the national waters of all Member States in the Mediterranean Sea and in national waters of other coastal States, for which bilateral agreements or a Security Council mandate should be requested;

Terrorist financing

- DE. whereas several Member States have not yet ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 16 May 2005, also known as the ‘Warsaw Convention’, which constitutes the most comprehensive international convention on money laundering and terrorist financing; whereas confiscating the assets generated by criminal activities is a very efficient tool in fighting crime and terrorism, as it deprives criminals of the proceeds of their illegal activities and prevents terrorists from organising an attack; whereas the Financial Action Task Force (FATF) sets global standards for Anti-Money Laundering and Countering Financing of Terrorism and identifies jurisdictions with weak measures in place to combat money laundering and terrorist financing;
- DF. whereas the EU has adopted two legislative instruments to implement FATF recommendations, namely the 4th and 5th Anti-Money Laundering Directives (AMLD), in order to address the gaps identified in the light of terrorist attacks; whereas the Member States had until 26 June 2017 to transpose the AML Directive into their national legislation, but not all of them have done so; whereas several Member States continue to allow ultimate beneficiary owners of trusts, foundations and incorporated companies to remain anonymous as well as bearer shares which facilitate the concealment of the origin and destination of financial flows and the ownership of economic activities that provide cover to the financing of terrorism and organised crime; whereas the 5th AMLD will increase transparency on these issues;
- DG. whereas the European Parliament’s Committee of Inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to money laundering, tax avoidance and tax evasion (PANA) verified how tax evaders count on the active help of professional intermediaries, who apparently fulfil the relevant legal obligations;
- DH. whereas in July 2017, the Commission and Europol were granted observer status in the Egmont Group, an international united body composed of 156 financial intelligence units (FIUs), with the aim of increasing cooperation not only between FIUs, but also among

other competent authorities;

- DI. whereas abuse and misuse of social media fundraising, funding through charity and non-profit organisations, small wire transfers and pre-paid cards are among the funding methods for Daesh and other terrorist organisations; whereas micro lending platforms are used to facilitate all of these typologies;
- DJ. whereas alongside traditional terrorist financing methods such as private donations, extortion, kidnapping for ransoms, abuse and misuse of non-profit organisations, formal and informal remittance systems, the use of proceeds of criminal activities, cash or funds transfers through banks, recent terrorist attacks have shown that emerging financing methods via electronic, online payment methods such as virtual currencies or anonymous pre-paid cards and informal value transfer systems (IVTS) also pose a risk of being misused by terrorist organisations to finance their activities; whereas the anonymity surrounding certain cryptocurrencies is leading to an increase in their use for illegitimate activities; whereas their use by organised crime groups to finance criminal activities and terrorism, and to launder criminal proceeds, has increased over the past few years; whereas Europol has collaborated with national authorities in dismantling several criminal operations which involved trading in cryptocurrencies;
- DK. whereas in certain countries with less developed banking systems the prevalent use of mobile banking services often makes it difficult to identify the beneficiaries of cash transfers; whereas such transfers of funds by means of mobile banking present high risks for terrorist financing and whereas, on the other hand, the relevant services must be enabled to track certain terrorist financing without coming up against banking secrecy in the vast majority of cases; whereas the use and transfer of funds through alternative remittance systems also present a risk for terrorist financing;
- DL. whereas cooperation and exchange of information between obliged entities, FIUs and competent authorities are key to the effective fight against terrorist financing; whereas FIUs, in the performance of their tasks, should have access to information and be able to exchange it, including through appropriate cooperation with law enforcement authorities; whereas it is essential to further enhance their effectiveness and efficiency by having the Member States clarify their powers and the cooperation between them;
- DM. whereas the Terrorist Finance Tracking Programme (TFTP) is a useful tool for counter-terrorist financing; whereas it does not allow tracing terrorist financing activities using SEPA transactions, which leads to a significant information gap; whereas a TFTS system complementary to the existing TFTP Agreement would enhance the EU's capacity to prevent and investigate terrorist attacks by providing key additional information on terrorist financing activities and would be more efficient and effective than pursuing financial information concerning suspicious transactions through bilateral or multilateral information and/or legal assistance requests; whereas Parliament has on several occasions called for the introduction of such a system, including in its resolution of 25 November 2015 on the prevention of radicalisation and recruitment of European citizens by terrorist organisations¹;

¹ OJ C 366, 27.10.2017, p. 101.

Protection of critical infrastructure

- DN. whereas incidents involving critical infrastructure, in particular those related to terrorist attacks or attempted attacks, can have severe and cross-border consequences for the security of European citizens and states;
- DO. whereas services are delivered through increasingly complex systems, which makes the current sectoral approach to European critical infrastructures (ECIs) outdated;
- DP. whereas cyber-attacks on electronic services or interconnected systems are a key component of hybrid threats; whereas an increasing number of cyber-attacks have, or can have, physical effects on critical infrastructure and its users; whereas there is a need to increase readiness to counter cyber terrorist threats;
- DQ. whereas the Commission Comprehensive Assessment of EU Security Policy and the evaluation study of Directive 2008/114/EC indicate that: the threat to critical infrastructures is likely to continue to rise, that there is a need to enhance preparation and response capabilities and to revise Directive 2008/114/EC, and that there is an interest in targeting transport infrastructures; whereas a better framework is needed to improve rail security and to address the issue of protection of public areas of transport infrastructures, such as airports, ports and maritime transport facilities, as well as railway stations and also of energy production facilities, with particular attention to nuclear power plants;
- DR. whereas attacks on critical infrastructure could have catastrophic consequences; whereas Member States must ensure adequate, fail-safe protection of these facilities;
- DS. whereas incident reporting is essential in identifying shortcomings, improving the effectiveness of existing measures, assessing the performance of critical infrastructures during a disruptive event, raising awareness of the need to review existing security plans, and detecting the emergence of new threats;
- DT. whereas Member States need to organise more exercises in crisis response, including in third countries seeking their cooperation and upgrading of capacities;
- DU. whereas the protection and insurance of critical infrastructure and soft targets requires public-private cooperation, including in the cyber-domain;
- DV. whereas private security services play a role in ensuring resilient security chains, public procurement of their services should therefore be subject to specific quality criteria, with regard to aspects such as the training, vetting and screening of personnel, quality control and compliance assurance, and the implementation of technological developments and contract management;
- DW. whereas, following the 2012 evaluation of Directive 2008/114/EC, the Commission launched a pilot phase involving four critical infrastructures of a European dimension (Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network);
- DX. whereas the Commission, in its communication on the new Multiannual Financial Framework, proposes to significantly increase EU funding for security and defence, including EU internal security;

DY. whereas several terrorist attacks in the EU were perpetrated by individuals known to the authorities; whereas vehicle rental companies lack the ability to exchange information, such as booking or reservation data, with law enforcement agencies for the purpose of cross-checks against official watch lists and police databases;

Explosives precursors

DZ. whereas in 2015 and 2016, explosives were used in 40 % of the terrorist attacks committed in the EU¹;

EA. whereas the explosive used in most of the attacks was triacetone triperoxide (TATP)², a home-made explosive that remains the explosive of choice for terrorists; whereas TATP can be quite easily manufactured using only a few substances; whereas many civilian factories and facilities which use those substances remain accessible by criminals, including terrorists, since no executive measures of control have been enforced by the Member States, in spite of the EU CBRN Action Plan;

EB. whereas despite Regulation 98/2013, some terrorists are still obtaining explosives precursors, especially for TATP; whereas it is still possible to acquire the substances under Annex I; whereas Regulation 98/2013 does not provide sufficient restrictions and controls, for example by only requiring a registration of transactions; whereas ensuring stricter controls is a key priority;

EC. whereas the greatest problems regarding implementation include a lack of awareness of the existing legislation across the supply chain due to the large number of economic operators (retailers of household products), and enforcing the restrictions on internet sales, imports and intra-EU movements;

ED. whereas the Commission proposal of 17 April 2018 for a regulation on the marketing and use of explosives precursors (COM(2018)0209) provides for stricter and more harmonised rules concerning the making available, introduction, possession and use of substances or mixtures that could be misused for the illicit manufacture of explosives, with a view to limiting their availability to the general public and ensuring the appropriate reporting of suspicious transactions throughout the supply chain;

EE. whereas on online marketplaces chemicals can be found by their written name, their formula, or their Chemical Abstracts Service (CAS) identification number, but in many cases are only listed by their generic name; whereas there are so many variations to names that it would be easier to identify listings for specific substances if inclusion of a searchable CAS number were also required;

EF. whereas the Regulation only covers sales to the general public, and not to professional users, who are not defined in the Regulation; whereas the criteria for defining who is a professional user differ across the internal market;

EG. whereas, pursuant to the impact assessment of 17 April 2018 (SWD(2018)0104) and the associated proposal for a regulation (COM(2018)0209), training for customs authorities

¹ Europol Terrorism Situation and Trend Report (Te-Sat) 2017, p. 10.

² Europol Te-Sat 2017, p. 15.

on recognising explosives and explosives precursors during the course of their duties at the external border should be expanded;

Illicit weapons

- EH. whereas access to firearms and components of explosive devices plays a very important role in enabling terror attacks; whereas in the EU, violent-extremist groups often have to turn to criminal networks to acquire weaponry; whereas according to Europol's Te-Sat 2018 report, firearms were used in 41 % of all attacks, a slight increase compared to 2016 (38 %) ¹;
- EI. whereas in recent years an increase in converted blank firing weapons and reactivated firearms has been observed; whereas several recent attacks have also been carried out with different types of knives;
- EJ. whereas the crime-terror nexus also eases the access of terrorists to firearms;
- EK. whereas the Council conclusions of 8 October 2015 invite Member States to systematically supply relevant information to Interpol and Europol;

External dimension

- EL. whereas a number of regions in the EU's neighbourhood, such as MENA and also the Balkans, are facing important challenges such as those relating to FTF and returnees management, as well as to home-grown radical cells;
- EM. whereas the Balkans remain a key region for European stability; whereas the challenges related to terrorism and Islamist extremism compound a regional context already weakened by ethnic, political and social polarisation as well as criminal networks; whereas the countries of the region have already been targets for terrorism (the attacks were prevented), and are already used as transit countries for people and weapons;
- EN. whereas all MENA countries have been confronted with major terrorist actions and remain prime targets; whereas these countries, on top of critical social and economic situations, may also face multiple challenges in relation to the return of FTFs from Daesh and Al-Qaeda, considering the large number of jihadists from this region; whereas information exchange and strong partnerships with these key third countries through an EU-coordinated approach, by offering cooperation and assistance in the form of capacity-building, make it possible to thwart attacks and dismantle terrorist networks;
- EO. whereas regions, such as MENA, the Sahel, the Horn of Africa, West Africa, the Gulf and Central Asia, have also experienced the development of terrorist networks linked to Daesh and Al-Qaeda; whereas religious extremism and sectarian violence benefiting from financing are serious concerns, enabling terrorist networks to spread, link up with other criminal enterprises and operate in those regions, targeting Europe and European interests;
- EP. whereas it is vital for the European Union to maintain strong cooperation with third

¹ Europol Te-Sat 2018, p. 9.

country partners in counter-terrorism; whereas the dialogue concerning the measures and actions undertaken to combat terrorism and terrorist funding and to prevent radicalisation must be maintained, particularly with the Gulf countries; whereas interparliamentary cooperation with these key third countries is one of the tools that should be strengthened;

- EQ. whereas the EU is cooperating with third countries in the area of counter-terrorism in a variety of ways; whereas a number of EU instruments can be used to finance CT programmes abroad; whereas the EU has deployed a network of CT experts within EU delegations; whereas EU agencies such as Europol, Eurojust and CEPOL are also cooperating with third countries in the area of counter-terrorism, through strategic and operational agreements for example;
- ER. whereas there is an EU sanction system in the area of CT with three types of measures, which is implemented by the EEAS; whereas this system is incomplete and underused owing to procedural constraints and reluctance on the part of the Member States;
- ES. whereas the Council Conclusions on EU External Action on Counter-terrorism adopted on 19 June 2017 recall the role of the Common Security and Defence Policy (CSDP) missions and operations in combating terrorism through enhancing security, stability, border control and security sector reform and in building counter-terrorism capacity and information sharing;

Victims of terrorism

- ET. whereas too many people have been the direct victims of terrorism across the EU, leaving thousands of families with post-traumatic conditions affecting their long-term well-being; whereas there is a lack of harmonised figures on the exact number of victims; whereas prior to 2001 most victims of terrorism were mainly attributable to the IRA and ETA, while since then the vast majority of deaths were as a result of terrorist actions organised or inspired by Al-Qaeda and Daesh;
- EU. whereas deaths caused by terrorist attacks destroy families, and many of the injured survivors of terrorist attacks suffer from disabilities, disfiguring and life-changing loss of limbs and psychological problems and their plight impacts heavily on close family and the community, while too often once the media spotlight has passed, the long-term needs of the victims are neglected; whereas post-traumatic stress syndrome is a major public health issue in Europe; whereas there are no overall European figures on the impact of terrorism on the mental health of the population following the various attacks;
- EV. whereas victims of terrorism have a very specific status, and meeting their needs is not only a legal obligation under EU, international and national law but also a responsibility for the whole of our societies; whereas recent attacks in the EU have seen victims emanating from a large number of different Member States;
- EW. whereas at European level there is no defined legal statute for victims of terrorism for the purposes of access to community services or compensation rights; whereas victims of the recent terrorist attacks in Europe still lack justice, proper treatment, victim support services and financial assistance; whereas victims of terrorism are at risk of secondary victimisation affecting them not only in judicial proceedings, but also in the many interactions they have with other state and non-state entities;

- EX. whereas there are still discrepancies in the way the provisions enshrined in Directive (EU) 2012/29 have been translated into procedures at national level; whereas the Commission has still not provided its report on the implementation of this directive; whereas on 30 May 2018 the European Parliament adopted a resolution on the implementation of this Directive¹;
- EY. whereas compensation for the victims of terrorism serves both as a form of recognition by society of the harm caused by the attack and as a means of financial support and restitution; whereas levels of compensation and procedures vary considerably among Member States, thereby aggravating victims' perceptions of injustice and the suffering they experience;
- EZ. whereas support systems need to be set up in such a way as to ensure that cross-border victims too are continuously and systematically accounted for and provided with support in their country while staying in touch with support providers in the country where the attack took place;
- FA. whereas Eurojust has been facilitating the execution of MLA requests for coordinating and granting assistance in the exercise of rights of victims of terrorism, considering the different rights and roles of foreign victims in their national legal systems;
- FB. whereas businesses, including SMEs, can also suffer damage from terrorism such as property damage and business interruption;
- FC. whereas Parliament has put forward a pilot project to establish a 'European Coordination Centre for victims of terrorism' by bringing together key operational experts, victim advocates and relevant organisations from around Europe with a view to identifying key priorities and issues for victims of terrorism and delivering coordinated support across borders;

Fundamental rights

- FD. whereas the European Union has a necessary role to play in promoting the respect of democratic values, including the rule of law and fundamental rights; whereas, however, there are extreme religious and political views and practices within the EU that fundamentally oppose these values;
- FE. whereas counter-terrorism measures and the protection of freedoms are not conflicting goals, but complementary and mutually reinforcing; whereas fundamental rights must be secured and protected for each and every individual and all measures in the fight against terrorism should affect the innocent and uninvolved general population as little as possible;
- FF. whereas any CT measures always have to fully guarantee all fundamental rights and principles, including those with regard to privacy and data protection, the right to freedom of thought, conscience and religion, as well as procedural safeguards, such as the presumption of innocence, the right to a fair trial and the right to information, ensuring that individuals have effective remedies at their disposal to challenge any violation of

¹ Texts adopted, P8_TA(2018)0229.

their fundamental rights, including the possibility of judicial redress, and that the Union *acquis* on procedural rights is respected; whereas such measures should take due account of the case law of the Court of Justice of the European Union;

- FG. whereas it is crucial that CT investigations adhere to high standards of professionalism with all the measures applied being targeted, proportionate and necessary; whereas CT policies should not lead to social exclusion and stigmatisation; whereas the Fundamental Rights Agency could be requested to provide an opinion on counter-terrorism legislation within the context of its Multiannual Framework;
- FH. whereas law enforcement and judicial personnel are at the forefront of CT operations; whereas there are multiple documented cases of police and judicial officials and their families being singled out for targeting and threats by violent extremists, some of which culminated in violent physical attacks and even murders; whereas political and public support of the law enforcement and judicial personnel who safeguard fundamental rights in CT investigations by risking life and limb, is of the utmost importance;
- FI. whereas the Charter of Fundamental Rights prohibits discrimination on the ground of disability and recognises the right of people with disabilities to benefit from measures to ensure their independence, social and occupational integration, and participation in the life of the community; whereas the rights of persons with disabilities in the EU are also protected by the UN Convention on the Rights of Persons with Disabilities;

Recommendations

Institutional framework

1. Considers that while Member States remain first in line to prevent and respond to threats because of their sovereign powers, a clear need exists to fully recognise the role of the European Union and of the counter-terrorism measures adopted within the framework of the ‘Security Union’ in supporting them, coordinating and sharing best practices, providing common solutions and adding value, so as to allow them to better counter the phenomena of radicalisation, extremism and terrorism; believes that in an area without internal borders, European action is vital in ensuring a high level of security across European territory and that deepening cooperation and the exchange of information between Member States and with the European Union is crucial to effectively respond to and prevent terrorist threats and protect citizens; urges the Member States and EU institutions to work towards a common strategic culture;
2. Believes that the EU and the Member States should improve their cooperation by strengthening existing European bodies, specialised EU agencies and services as well as the cooperation channels between Member States’ competent authorities and justice institutions; believes that adequate means should be granted to these EU agencies in order to enable them to deal with their increasing workload;
3. Stresses the importance of the exchange of good practices between Member States within the European Union, as well as with third countries; welcomes the initiatives taken by some Member States, as well as at the local level by some cities, and also by private operators, to identify effective counter-terrorism tools;

4. Calls on the next President of the Commission to maintain a self-standing portfolio for the Commissioner for Security Union;
5. Calls on the Council to retain the post of EU Counter-Terrorism Coordinator; considers that the EU Counter-Terrorism Coordinator should continue to play a proactive role in strengthening the EU's response in the fight against terrorism; calls for clarification of the status and role of the Counter-Terrorism Coordinator, as a bridge between the competent EU institutions and Member States' agencies;
6. Considers that freedom, security and justice are three aspects that cannot be analysed separately; considers that respect for fundamental rights must form an essential part of all legislative initiatives on terrorism; urges that the area of responsibility of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs should continue to include counter-terrorism, in order to ensure consistency with other legislative categories of work in the area of freedom, security and justice;
7. Calls on the Council to expand the powers of the European Public Prosecutor's Office to include the fight against organised crime and terrorism;
8. Calls on the Member States and the Commission to further strengthen and support the ATLAS Network of civilian anti-terror special operation units of the EU Member States;
9. Urges the Commission to systematically conduct impact assessments and citizen and expert stakeholder consultations of future counter-terrorism legislative proposals;

Terrorist threat

10. Calls on the Commission to work with the Member States towards more transparency and a common understanding of threat levels; calls on the Member States to swiftly transmit information on the change of the threat level and the rationale behind it; further calls on the Commission and the Member States not to restrict their view of terrorism to jihadism, but to remain equally vigilant as regards terrorist threats based on other motivations such as, for example, those mentioned in the Europol Te-Sat reports;
11. Calls on the Commission to promote, in the relevant international forums, the explicit categorisation of terrorism as a 'Crime against humanity', set out in Article 7 of the Rome Statute that led to the creation of the International Criminal Court;
12. Calls on all Member States, in line with the conclusions of the Council of Europe¹, to recognise that Daesh has committed genocide, notably against the Yazidi people, Christian and non-Sunni Muslim minorities, and requests all Member States to take prompt and effective action in accordance with their obligation under the 1948 Genocide Convention to prevent and punish acts of genocide, as well as their general responsibility to act against crimes under international law;
13. Calls on the Member States and the appropriate EU agencies to monitor all foreign terrorist fighters and to ensure harmonised security and judicial follow-up of identified

¹ Council of Europe report on 'Prosecuting and punishing the crimes against humanity or even possible genocide committed by Daesh' of 22 September 2017.

returnees to Europe; calls on the Commission to assist Member States in the establishment of aligned classification systems in order to distinguish between high, medium and low-risk returnees;

14. Recommends to the Member States that they provide appropriate structures to respond to child returnees, and in particular to develop a specialised risk and needs assessment tool based on the stages of development of children and on their degree of involvement in criminal activities abroad; underlines that rehabilitation programmes should be based on a multidisciplinary approach bringing together different kinds of expertise, including that of experienced professionals in the areas of trauma, extremism, child development, education and risk assessment and tailored to the local and national context, as well as clear legal and organisational structures for dealing with this alarming phenomenon; encourages Member States to cooperate with the International Committee of the Red Cross as it possesses particular access and expertise in this field;
15. Calls on the Commission to revise and update the CBRN Action Plan, and on the Member States to establish or strengthen and maintain appropriate ‘civil defence’ measures for preparedness against CBRN attacks by recruiting qualified and regularly trained personnel incorporating both full-time and voluntary staff, as well as appropriate technical infrastructure including response resources such as specialised mobile detection systems, stocks of essential medicines, care for victims, and the sharing of best practice; emphasises that these measures must be in line with a multidisciplinary strategy that contains methods of coordination, notification procedures, standard protocols, evacuation planning, public alarm systems and incident reporting; calls on the Commission and the Member States to gradually harmonise these strategies; calls on the Member States to create or strengthen specialised laboratories; asks the Commission in conjunction with Parliament to support relevant cross-border research activities; encourages enhanced cooperation with NATO’s Centre of Excellence on CBRN to ensure a transfer of best practices between emergency responders in EU and NATO member states;
16. Encourages Member States and the Commission to cooperate with the private sector in order to establish mechanisms that ensure a reliable, consistent and adequate supply of medical countermeasures, including potential use of the EU Joint Procurement Mechanism established by Decision 2013/1082 of 22 October 2013 on serious cross-border threats to health¹;
17. Urges, in order to facilitate accessibility, the updating and extension of the European Bomb Data System at Europol to the European analysis project – which serves as an information and coordination hub regarding all CBRN-related incidents throughout the EU – to be complemented by an adequately staffed multidisciplinary analysis team;
18. Welcomes the Commission’s plan to strengthen EU CBRN preparedness and response through cross-sectoral exercises for law enforcement, civil protection health structures and, where relevant, borders and customs within the existing financial instruments and operational tools, in particular the Union’s Civil Protection Mechanism, CEPOL and the Internal Security Fund – Police;
19. Urges the Commission and the Member States to set common standards for vetting

¹ OJ L 293, 5.11.2013, p. 1.

procedures at vulnerable institutions such as nuclear power plants or specialised laboratories;

20. Encourages the Member States to make more use of technical detection systems for CBRN substances, particularly at large-scale public events, and calls on the Commission in conjunction with Parliament to make further European funding available for comprehensive acquisitions of such systems;
21. Welcomes the creation within the European Counter Terrorism Centre (ECTC) of a knowledge hub on the topic of CBRN and related activities on explosives, which will operate alongside the European Nuclear Security Training Centre (EUSECTRA); calls for a standard procedure in which every Member State effectively shares information with the knowledge-gathering centre;
22. Welcomes the approval of a regulation on common rules in the field of civil aviation safety and the mandate of the European Aviation Safety Agency (EASA) and repealing Regulation (EC) No 216/2008¹; calls on the Commission to take security aspects into account for forthcoming delegated and implementing rules on drones and drone operations, including regularly updated risk assessments, mandatory registration, electronic identification and geofencing in all drone categories, and mandatory security licences and training courses for operators of security and inspection missions;
23. Notes that many persons carrying out terrorist activities in the EU have been known to start off in petty crime and to have been indoctrinated in violent extremism while in prison; invites Member States to ensure that their criminal law systems punish criminals appropriately and allow for a careful consideration of the risk of reoffending before an early release is authorised; stresses that prison time should enable rehabilitation, reintegration and prevention of repeat offences instead of fomenting violent extremism;
24. Underlines the ongoing threat of interactions between terrorist organisations and organised crime, particularly in relation to logistical capacities and weapons trafficking which could enable large-scale attacks;
25. Notes the increased cyber threat and underlines the importance of stepping up cyber security efforts also in the field of counter-terrorism;
26. Calls on the Member States to provide adequate resources to their public bodies involved in CT operations with all the technical, financial, educational and legal means necessary to protect themselves against violent extremists in fulfilling their duties;

Preventing and countering radicalisation leading to violent extremism

Structures for countering radicalisation

27. Calls for the creation of an EU ‘Centre of Excellence for Preventing Radicalisation’ (CoE PR), as a successor to the RAN, to be embedded in the Commission with adequate financial and human resources; believes its tasks should include coordination, facilitation of cooperation and exchange of knowledge, lighthouse projects and good practices among

¹ OJ L 212, 22.8.2018, p. 1.

Member States, policymakers, practitioners (by involving former RAN and ESCN structures), as well as engagement with religious leaders or communities and academics and experts, including IT specialists, in the area of preventing and countering radicalisation; points out that its activities should include the training of different categories of professionals, including judges and prosecutors, also by partnering with key strategic third countries; considers that this centre should also establish scientific methodologies to evaluate and measure the effectiveness of programmes and projects, so that the relevant policies can be adjusted if necessary;

28. Notes that the European Court of Auditors' report of 2018 on deradicalisation found that the Commission does not maintain a complete overview of EU-funded measures, and that no indicators or targets for EU funds are used to measure to what extent the approach is successful; calls on the Commission to ensure that sufficient funding under the Internal Security Fund is earmarked for preventing and countering radicalisation, which would streamline resources currently fragmented across different funds and programmes and allow for better coordination and visibility as well as higher effectiveness of their use on the basis of criteria which could be developed by the CoE PR;
29. Urges the Member States to adopt comprehensive national and regional strategies for preventing and countering radicalisation, with adequate financial resources for communities and partners at local level involved in the creation and implementation of programmes based on these strategies, and calls for a multi-agency approach; stresses that the best results are achieved in partnership with local communities; stresses further that objective qualitative and quantitative indicators which could be developed by CoE PR would enable local and regional authorities to map out the local specificities of radicalisation and better tailor programmes to the specific area;
30. Calls on the Member States to address radicalisation holistically, also in collaboration with local administrations, and to complement security approaches by strategies on social inclusion, economic and cultural integration and by long-term policies and investments in public services and infrastructure; exhorts both the Commission and the Member States to promote anti-discrimination campaigns;
31. Highlights the importance of conducting specific research into the role of women within targeted regions, countries and communities to understand their role and identify areas where women's organisations could contribute to building greater resilience to radicalisation;
32. Calls for the creation of a European Resilience Prize, which would be awarded every year by the European Parliament, and possibly in close consultation with the CoE PR, to the best social and cultural project at local level in the EU, thus promoting social engagement, in full accordance with democracy, rule of law and human rights and with the aim of building societies that are resilient against radicalisation;
33. Calls on Eurojust to continue its work in monitoring the jurisprudence in Member States as regards radicalisation leading to terrorism, including the use of alternatives to prosecution and detention, and to report regularly in its Terrorism Conviction Monitor (TCM); calls on the Member States, to this end, to transmit to Eurojust all relevant information on prosecutions and convictions for terrorist offences which affect or may affect two or more Member States;

Religious extremism

34. Urges the Member States to guarantee the freedom of religion and the right to exercise it freely, as enshrined in the Charter of Fundamental Rights, and in this context in particular also to encourage and tolerate only religious practices that are in full accordance with democracy, the rule of law, human rights and the laws in place in Member States; welcomes the initiatives by religious communities throughout Europe to counter the dangerous narratives from within their communities; stresses the need to encourage inter-religious and cross-cultural dialogue and cooperation with religious communities and local authorities to prevent radicalisation;
35. Calls on the Member States to conduct prior screenings of chaplains and to consistently blacklist on a case-by-case basis any hate preachers; calls on the Commission to introduce an EU watch list so as to better exchange information on extremist chaplains within the scope permissible in accordance with the law; encourages the Member States to find a common understanding and develop guidelines against which those chaplains could be screened;
36. Calls on the Member States to increase the offer of higher education opportunities for chaplains in the EU, with transparent scrutiny and only accrediting theological curricula that fully respect democracy, rule of law, human rights and the neutrality and democratic laicism of European countries, and revoking teaching licences in cases of misdemeanour;

Acting against hate speech and extremist groups

37. Calls on the Member States to implement the CT Directive and Framework Decision on Racism and Xenophobia, under which incitement to commit a terrorist act or a hate crime is a criminal offence, in order to exclude hate preachers from public activity using all legal measures, including refusal of visas or expulsion from EU territory, and to start judicial proceedings against such preachers and any agents of extremist and terrorist proselytism;
38. Urges the Member States to close places of worship and ban associations that are not in full compliance with applicable EU and national law, democracy, rule of law and human rights and that incite terrorist offences, hatred, discrimination or violence;
39. Invites the Member States to examine how to ensure that places of worship, education and religious teaching, charities, cultural associations and foundations and similar entities provide details regarding the provenance of their funds and their distribution, both within and outside the EU, and how data concerning these entities, where there exists suspicion or reasonable grounds to suspect links with terrorist groups, could be recorded and analysed by competent authorities in accordance with the EU legal framework and data protection rules; calls on the Member States to ban funding from third countries that oppose democracy, rule of law and human rights;
40. Asks the Member States to take swift legal action to ban and remove to the extent possible within their territories all printed and online propaganda that explicitly incites violent extremism and terrorist acts, including all content produced or spread by groups and individuals sanctioned by the EU or UN; asks for such propaganda to be removed from shops and online platforms as part of the referrals by the EU IRU, which could be

reinforced in human resources and capacities, if needed; calls for efforts to be made to track and/or identify the sources of such propaganda;

41. Calls on the Member States to take action against satellite TV channels disseminating violence, hate speech and incitement to terrorism, in accordance with the Audiovisual Media Services Directive; calls on the Member States to fully and swiftly implement the Directive to ensure that Article 6 on prevention of incitement to violence and hatred is in force across the EU; requests the Commission to prepare an analysis of possible legislative changes in the Directive in order to improve the effectiveness of blocking such channels broadcasting from third countries;

Education

42. Highlights that the Member States must ensure that all educational institutions provide education in accordance with the European Convention on Human Rights, through checks on curricula, regular inspections and sanctions for non-compliance;
43. Believes that education as a process to discover, explore, engage with and confront history, civilisations, cultures, ideologies and religions must become a fully fledged tool in the fight against all extremist violence and violent radicalisation processes; emphasises the importance of teaching non-discrimination and respect for other people's beliefs and of promoting social inclusion of all children, in accordance with the EU Charter of Fundamental Rights, as well as the UN Convention on the Rights of the Child;
44. Calls on the Member States to establish policies for the prevention of radicalisation, both specific (vulnerable groups) and non-specific (general); believes that gatherings in schools with victims, returnees and their families and people who have overcome radicalisation could be an effective tool for preventing radicalisation; encourages awareness training for practitioners who may interact with child returnees; notes that the best results are often achieved in partnership with local communities, challenging the core communications of terrorist groups with counter narratives;
45. Encourages the Member States to integrate media and information literacy and internet use into national education systems in order to empower young citizens with the tools to understand and assess the often unfiltered information that circulates online and to use the internet responsibly, with a view to avoiding possible risks of radicalisation;
46. Recommends that Member States establish guidelines for schools for tackling the possible radicalisation of pupils and to develop simple and clear procedures on how to deal with them; stresses the need for the involvement of child protection authorities and social services, with better cooperation with the relevant units of law enforcement and justice bodies in the process of addressing the most serious cases of radicalisation;

Internet

47. Underlines the need to achieve automatic detection and systematic, fast, permanent and full removal of terrorist content online on the basis of clear legal provisions including safeguards, and human review; further points out the need to prevent the re-upload of already removed content; welcomes the Commission's legislative proposal on preventing the dissemination of terrorist content online by obliging platforms to remove it fully; calls

on the co-legislators to urgently work on the proposal; invites the Member States to put in place national measures if the adoption of legislation is delayed;

48. Considers that the reporting should include descriptions and statistics on what content was removed and why, how many views the content received prior to removal, how long the content stayed online prior to removal and whether or not the account associated with the offending content was deleted and when; stresses that proper transparency is needed to assess whether state authorities are playing an appropriate role in investigating and prosecuting offences when illegal content is reported;
49. Welcomes the work of the Global Internet Forum to Counter Terrorism (GIFCT) and calls on the founding companies of the GIFCT to intensify their efforts in the shared industry hash database also by sharing knowledge with smaller technology companies; calls on technology companies to increase their efforts and funding for the development of methods to remove terrorist content quickly, but without endangering freedom of speech;
50. Welcomes the work done by Europol's EU IRU; calls on each Member State to establish a special unit in charge of reporting illegal content which could cooperate with the EU IRU in ensuring complementarity and avoiding unnecessary duplication in referring terrorist content to IT companies; calls for the EU IRU to be strengthened in order to facilitate and coordinate Member States' efforts to intercept, flag and delete terrorist content online; believes, furthermore, that it is crucial to collect the information on deleted online terrorist content and accounts at Europol, in order to prevent them from being uploaded again and facilitate analysis and criminal investigations;
51. Calls for the Commission to create an online European platform that citizens can use in order to flag online terrorist content, and asks companies to have adequate capacity to receive, review, process and respond to flagged content;
52. Calls for an effective partnership approach between law enforcement agencies, judicial authorities, the IT industry, internet service providers (ISPs), internet host providers (IHPs), social media companies and civil society organisations in developing and disseminating effective counter-narratives, also where appropriate with the inclusion of victims and former violent extremists, and to ensure that search engines place counter-narratives prominently; encourages the Commission and the Member States' authorities to strengthen their efforts to build effective counter-narratives and other strategic communications tools;

Prisons

53. Calls on the Member States to ensure secure and safe prison conditions for both detainees and staff, and to create specific procedures and indicators to identify and deal with radicalised inmates, in order to prevent radicalisation of others, as well as to ensure targeted monitoring and targeted disengagement measures, and to train prison staff accordingly;
54. Urges the Member States to guarantee the safety and physical and psychological integrity of staff in prisons and to provide them with psychological counselling; calls on the Member States to provide adequate resources, targeted training and supervision to prison authorities at all levels and especially to frontline staff closely working with juvenile

offenders and radicalised inmates; stresses, in particular, that staff must be adequately trained to detect signs of radicalisation at an early stage; encourages the Member States to take stock of the training courses developed with EU funds by the Confederation of European Probation (CEP), EuroPris and the European Penitentiary Training Academies (EPTA) network; calls for further EU contribution to enhancing training for prison officers on issues related to radicalisation and potential terrorist threats;

55. Stresses that prison authorities must develop specific tools and methods for identifying and monitoring radicalised inmates according to their degree of radicalisation and for their obligatory assessment prior to release; calls on the Commission to promote best practices on risk assessment methodologies of radicalised inmates developed by different Member States; considers that the inmates ranked as most dangerous must be flagged to the judicial authorities and/or national and external authorities in charge of counter-terrorism, with effective post-release parole requirements for those likely to threaten public security; urges the Member States to strengthen intelligence gathering regarding radicalised inmates and their follow-up, building on best practices in the Member States, such as the establishment of prison intelligence procedures; highlights that the appointment of a contact person responsible for combating radicalisation in the prison system may be useful;
56. Stresses that prison time should enable rehabilitation and reintegration instead of fomenting radicalisation; calls on the Member States to set up multidisciplinary disengagement programmes within prisons; believes that reintegration measures should be made an integral part of incarceration in order to prepare for the release of these inmates; considers that the CoE PR could carry out a follow-up of action plans against radicalisation in prisons and in post-prison transition;
57. Stresses that inhuman detention conditions, overcrowding and ill treatment are counter-productive as regards the objective of combating radicalisation and violent extremism; points out that in order to prevent radicalisation in prisons it is essential to establish detention rules that are differentiated according to the level of danger presented by the inmates; underlines in this respect that any specific programme dedicated to a certain group of prisoners must respect the same human rights and international obligations as for any prisoner;
58. Calls on the Commission to launch a European Forum on prison conditions in order to encourage the exchange of best practices between experts and practitioners across all Member States;
59. Draws attention to the various forms of illegal goods trafficking in prisons, particularly the trafficking of mobile phones, which allows incarcerated prisoners to remain in contact with external terrorist networks;
60. Urges the Member States to facilitate access to genuine chaplains as it reduces the risks of the self-organisation of radical religious cells; suggests introducing a system of licences based on background checks for chaplains accessing prisons in order to prevent the spread of extremist views among high-risk populations, and calls on the Council, with support from the Commission, to draw up guidelines on this based on best practices; calls on the Member States to regularly evaluate and monitor the chaplains with access to prisons; calls on the Member States to require standard training for chaplains working in

prisons based on best practices developed by Member States' penitentiary authorities, also in cooperation with third countries;

Cooperation and information exchange

Horizontal issues

61. Urges the Member States to implement, fully and on time, the existing legislation, and calls on the Commission to provide the necessary support; calls on the Commission to analyse the shortcomings in the transposition, implementation and application of the existing legislation, and to use its powers to initiate infringement proceedings when Member States fail to properly implement legislation;
62. Urges the Member States to ensure that they have the necessary technical equipment, software, security systems and qualified human resources to make full use of the existing information systems and cooperation mechanisms; reiterates the importance of ensuring that staff with access to such equipment have received appropriate training with regard to data;
63. Notes the insufficient nature of the security research being conducted by public institutions; calls for a more proactive definition of the needs (e.g. strengthening the European Network of Law Enforcement Technology Services (ENLETS), which is defining technological needs for law enforcement); calls for support for pilot projects on artificial intelligence and blockchain technology (remittances); calls for the active involvement of EU agencies such as Europol and CEPOL in EU security research projects; calls on the Member States to regularly organise foresight exercises looking into future threat scenarios; supports the continued funding by the Commission to set up modernised databases and provide up-to-date technical equipment and training for staff, and calls for a more ambitious approach in this respect;
64. Urges the Member States to develop the necessary technical standardisation, improvements with regard to data quality and legal framework for a future approach of 'information sharing by default' when it comes to sharing CT-related information with other Member States and relevant EU agencies and bodies on the basis of the applicable underlying legal regulations governing each information system, thus exchanging such information as a rule, and refraining from such exchange only in specific cases where circumstances require that it be withheld, namely when the sharing of information would jeopardise current investigations or the safety of an individual or would be contrary to the essential interests of the security of the Member State concerned; calls on the Commission to collect data on the implementation of existing obligations with regard to information-sharing by default;
65. Calls on the Member States to comply with their obligations under the CT Directive and Decision 2005/671/JHA to exchange relevant information in connection with terrorist offences as soon as possible with the competent authorities of other Member States; is of the opinion that the competent law enforcement authorities should, without any prior request being necessary, provide to the competent law enforcement authorities of other Member States information and intelligence in cases where there are factual reasons to believe that this information and intelligence could assist in the detection, prevention or investigation of offences;

66. Points out that existing opt-outs by some Member States from police and judicial cooperation measures for the prevention, detection, investigation and prosecution of terrorist offences and the financing of terrorism could endanger the speed and efficiency of terrorism investigations and may have detrimental effects; calls on the Member States to keep this in mind and to thoroughly weigh up the pros and cons of opt-outs in this crucial field;
67. Notes that the current existence of 28 different legal regimes for data retention may be counter-productive for cooperation and information exchange; urges the Commission to evaluate a legislative proposal on data retention which respects the principles of purpose limitation, proportionality and necessity, taking into account the needs of the competent authorities and the specificities of the field of counter-terrorism, by, among other measures, addressing new forms of communication, establishing strong safeguards on the storing of data by service providers and on the access side to data for criminal investigations, pseudonymisation opportunities, determining data categories that are particularly relevant for effectively combating terrorism and serious crime, providing specifically trained and supervised staff dealing with data access or introducing periodic threat-assessments as a basis for retention periods;

Information systems

68. Urges the Member States to ensure full implementation and to systematically check the relevant databases and information systems in full accordance with their access rights laid down in the underlying legal bases and to introduce all useful data in a timely manner while meeting the quality requirements of the respective information systems;
69. Urges the Member States to ensure that the relevant information available at local or regional level and in their databases is automatically uploaded where possible through smart technical solutions to national systems and, where appropriate, to relevant European databases to prevent information from being lost as a result of the fragmentation of jurisdictions, while ensuring that EU data quality, security and protection standards are met;
70. Calls on the Member States to use to the extent possible all link categories and implement all search combinations provided in SIS, and to ensure appropriate staffing levels and sufficient technical support for the SIRENE Bureaux;
71. Welcomes the revision of the Schengen Information System II (SIS II), requiring law enforcement authorities to also register the checks carried out on a target registered in SIS II and establishing a uniform use of SIS II with regard to terrorism; calls on the Member States to ensure that information in connection with terrorist offences is consistently and systematically uploaded to European systems and platforms, particularly in the case of alerts under Article 36 of the SIS II Regulation, and synchronised where possible by implementing a consistent three-tier information-sharing approach by making optimal and consistent use of SIS and Europol data; welcomes the new type of alert: an 'inquiry check' under Article 36 of the SIS II Regulation, and the new obligation for an immediate reply by the SIRENE Bureau in the event of an alert linked to terrorism; further calls on the Commission to determine, with the active participation and agreement of experts from the Member States, good practices in terms of follow-up procedures for hits on persons involved in terrorism or terrorism-related activities under Article 36;

72. Calls on the Commission to implement a ‘post-hit’ information exchange mechanism that would enable all Member States or at least those concerned to be informed of the hits generated by the movements of persons involved in terrorism or terrorism-related activities; underlines the need for mapping of the travel movements of FTFs, returnees and persons involved in terrorist activities based on SIS hits in order to gain a clear and comprehensive picture that can provide a basis for taking further measures;
73. Calls on the Commission to evaluate under which circumstances national intelligence services may continue to have direct access to relevant EU information systems, in particular SIS under its reformed legal regime, to avoid new security and information exchange gaps;
74. Welcomes the deployment of a central automated fingerprint identification system (AFIS) within SIS to enable end users to search SIS on the basis of fingerprint data; calls for the roll-out of the system by 2019; urges all Member States to implement the AFIS functionality of SIS immediately; notes that despite the legal basis of SIS II permitting the storage of fingerprints, such biometrics have so far only been used to confirm the identity of a person following a check on the person’s name or date of birth; believes that identification based solely on fingerprints would bring significant added value;
75. Calls on the Member States to ensure that their CT competent authorities have access to VIS and for a simplified procedure for such access;
76. Welcomes the creation of the European travel information and authorisation system (ETIAS), which will be applied to visa-free nationals of third countries;
77. Calls on the Commission to propose legislation establishing one centralised ECRIS system, allowing for the exchange of criminal record information concerning both EU nationals and third-country nationals;
78. Calls for private aircraft to be covered by the EU PNR Directive and for air carriers to be obliged to collect PNR data; calls on the Commission to evaluate security procedures enacted at aerodromes and smaller airports throughout the Member States;
79. Urges all Member States to fully implement the PNR Directive without delay and calls on the Commission to swiftly proceed with infringement procedures against those Member States who have not yet done so; calls on the Member States to interconnect their PIUs in order to facilitate the exchange of PNR data; calls on the Commission to propose technological solutions to make the exchange of PNR data and their integration into different systems less time-consuming and demanding in terms of human resources by automating the processing of requests from one PIU to another; encourages, therefore, projects such as the ISF project led by the Netherlands to develop PIU.net based on the existing FIU.net; asks the Commission, together with Europol, to support the development of joint targeting rules and risk assessments to be applied by the Member States;
80. Calls on the Member States to make their PIUs multidisciplinary units, including personnel from customs, law enforcement and intelligence authorities, in order for the competent authorities to better share information;

81. Notes that the deadline for implementing the Prüm decisions¹ of 23 June 2008 expired on 26 August 2011 and that even now not all Member States have fully implemented the decisions; calls on those Member States therefore to finally fulfil their obligations under EU law and fully implement the Prüm decisions and strengthen the Prüm network by updating their national processing systems to adapt to modern information technology; urges the Commission and the Council to modernise and upgrade the Prüm decisions of 2008 to link national systems more efficiently;

Interoperability

82. Welcomes the proposed regulations on interoperability; calls on the Commission to evaluate the potential and possible added value of additional information systems to be included in the future and to report to the European Parliament; believes that interoperability helps bring the relevant and necessary information together; emphasises that such a solution needs to find the right balance between legitimate needs for timely, efficient and relevant information for authorities in full accordance with their access rights and purpose limitation under the underlying legal bases and the fundamental rights of the data subjects;
83. Stresses the need to introduce a biometric matching service enabling querying with biometric data across several EU information systems so as to contribute to the fight against identity fraud and to prevent people from using multiple identities; stresses the need to feed the relevant databases with biometric data; also stresses the need to continuously improve the ability to recognise improperly used real, partly falsified or entirely falsified documents used for personal identification;
84. Urges that the work for further evolution of the UMF standard be initiated immediately, with the close involvement of eu-LISA, in order to ensure that the standard meets the needs of future interoperable IT systems and can be a part of the coordinated work towards improving data quality in large-scale IT systems;
85. Calls for the delineation of harmonised minimum data quality standards for data input to be established at EU level, in line with the criteria of the EU data protection *acquis*, and applied across IT systems in order to ensure consistent quality of the data therein; urges eu-LISA to establish common indicators and checks and to develop a central monitoring capacity for data quality for all systems under its competence; further recommends that when eu-LISA notes irregularities in its quality reports to the Member States, the Member State concerned should be obliged to correct the data or justify the lack of correction;
86. Criticises the lack of appropriate funding and staffing for eu-LISA, considering its continuously increasing responsibilities; calls for eu-LISA to be reinforced with the additional capacity and resources needed to perform the new tasks efficiently, and for this to be reflected in the new MFF;

Cooperation and exchange of information within and between the Member States

¹ Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1) and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12.).

87. Calls on the Member States that have not yet done so to create national counter-terrorism ‘fusion centres’, or coordination units, as well as coordinated databases, in order to centralise and facilitate the search, identification and exchange of terrorism-related information and intelligence from all relevant national authorities; considers furthermore that a proactive local and, where appropriate, regional policy is a prerequisite for an integral national security policy; calls on the Member States to share best practices in this respect, such as the Belgian ‘Lokale integrale veiligheidscellen’, which involve civil society stakeholders such as social services, local administration and local politicians, in discussing all indications of radicalisation, and with shared professional secrecy so that stakeholders with a professional duty of secrecy could also contribute;
88. Calls on the Member States to explore new approaches to improve cooperation and information exchange between law enforcement and intelligence services at national level which preserve the necessary separation between law enforcement and intelligence work and the required principles of information ownership and source protection and those related to admissibility of evidence in criminal proceedings;
89. Calls on the Member States to build on best practices by reinforcing the case-by-case cooperation and information exchange between public prosecutors and intelligence services in terrorism-related criminal investigations;
90. Recommends that Member States indicate in guidelines or through legislative action when it is permissible to exchange information between police and intelligence services with other Member States’ competent authorities and EU agencies, and believes that aligning national standards on this issue would contribute to an EU-wide answer to the question of when such information can be used and shared;
91. Calls on the Member States to ensure that any legal or political evaluation, check, procedure or lawsuit that provides intelligence information does so with a special degree of protection and to ensure that the protection of confidentiality and integrity of sources of intelligence and officials is maintained in order not to endanger the work and security of sources, informants and employees of the intelligence services;
92. Calls for the setting up of an EU Joint Intelligence Academy with common standards, in order to combine resources and develop synergies, trust and a common intelligence culture;
93. Recommends that the Member States examine the possibility of better coordination and cooperation between intelligence and law enforcement services at EU level, for example by sending intelligence experts in addition to law enforcement staff to the meetings of the Counter-Terrorism Joint Liaison Team (CTJLT) at Europol; calls on the Commission to increase support to the CTJLT, including adequate funding;
94. Calls on the Member States to optimise collaboration through the Counter-Terrorism Group, to further reinforce it as a joint cooperation and communication platform between national intelligence services, and to provide adequate funding; welcomes the setting up of a CTG Advisory Board to increase visibility and transparency and to speak publicly in the relations between the CTG and the relevant EU institutions and bodies and to guarantee that the European Parliament is continuously informed;

95. Asks the Member States to schedule regular exchange meetings between judges and representatives from the intelligence and law enforcement community in order to share knowledge about situational, investigatory or technical developments in the counter-terrorism field, enabling the judiciary to grasp the full picture concerning their jurisdiction and receive further training;
96. Calls on the Member States to further develop mutual cross-border police cooperation through joint threat assessment, risk analysis and patrols;
97. Calls on the Member States and European stakeholders to continue providing sufficient operational capacity and enhance maximum effective cooperation in the fields of counter-terrorism and EU internal security, including through adequate budgeting, so as to maintain a national security culture that is equipped to deal with the threat in the medium term;
98. Welcomes the European Council (at 27) Guidelines of 23 March 2018 in which it expressed ‘determination to have as close as possible a partnership with the UK in the future [...] in particular [in] the fight against terrorism and international crime’; believes that it is crucial to ensure continued mutual security cooperation and information exchange between the EU and the UK post-Brexit;
99. Recognises the close professional counter-terrorism collaboration between European countries and, as appropriate, with foreign counter-terrorism authorities, and calls for continued enhancement through operational missions, data analysis, more rapid exchange of intelligence, and the sharing of best practice;

Cooperation and exchange of information with the EU agencies

100. Calls for more systematic cooperation among the JHA agencies working on counter-terrorism to develop joint approaches and synergies given the increasing role of the agencies in this field; believes that regular joint meetings of all the key agencies could further develop joint work in this field and increase synergies with their liaison officers in delegations;
101. Calls on the Member States to increase the number of Seconded National Experts with a background in counter-terrorism to agencies with a view to ensuring representation of Member States’ needs and allowing the agencies to have the necessary expertise in this field, within the context of their mandates;
102. Calls for Europol to become a veritable hub for law enforcement information exchange and cooperation in the field of counter-terrorism in the EU; calls on the Commission to closely monitor this process and evaluate the need of possible legislative adjustment;
103. Invites Europol to make full use of its current rights to access SIS, VIS and Eurodac with the purpose of enhancing interoperability, while respecting fundamental rights and data protection legislation;
104. Calls on Europol to ensure the timely availability of QUEST to Member States, with the purpose of enhancing interoperability;

105. Calls for appropriate funding and staffing for Europol and Eurojust considering their continuously increased responsibilities and vital role in strengthening European law enforcement and judicial cooperation and in supporting the fight against terrorism;
106. Urges the Member States to ensure full use of the contacts between Europol and the relevant authorities when it comes to terrorist offences, considering that in the field of counter-terrorism speed is often essential; encourages the Member States to use ‘on-the-spot deployments’ of Europol specialists, as this increases trust and reduces administrative burdens; calls on the Member States to ensure direct access of Member States’ law enforcement CT services (beyond federal/central level) to Europol’s services;
107. Calls on the Member States to establish the necessary secure national law enforcement communication infrastructure and to promote direct and decentralised connectivity of CT services to CT SIENA and EIS, as this would reinforce searches and cross-matches;
108. Urges the Commission and the Member States to provide enhanced financial and human resources, including data scientists and big data analysts, for the development of technical solutions to deal with the high volume of data to be analysed; calls for Europol to be tasked with further R&D projects in this field in the context of its mandate for the benefit of Member States;
109. Calls on the Member States to make full use of technical solutions to improve sharing of information with Europol, in particular by automating the process of uploading data to the Europol information system for cross-checking purposes, for example by using the ‘data loaders’ developed by Europol;
110. Welcomes the new provision in the future SIS II allowing Europol, unless legal or operational reasons require otherwise, to be informed of any new alert or any hit linked to terrorism in SIS; notes that this will allow cross-checks and, if deemed appropriate, operational and/or thematic analysis, in order to proceed with the mapping of travel patterns and/or to analyse the possible connections of the located individual(s); calls on the Commission to quickly implement this new possibility in an automatic way;
111. Calls on Europol to publish an annual report on the amount and type of information shared by the Member States in the relevant EU information systems and with Europol, in order to identify gaps and promote information exchange;
112. Calls on Europol to fully develop biometric capacity as soon as possible, as it would be important for Member States to increasingly share biometric information with Europol;
113. Highlights that state-of-the-art end-to-end encryption of communications is an essential tool to safeguard confidentiality of communications and ensure legitimate transactions between consumers; calls on the Member States to ensure cooperation among all relevant stakeholders with a view to increasing the decryption abilities of the competent authorities and that the decryption abilities of the competent authorities are up to standard with a view to legal prosecution; welcomes the fact that Europol is developing decryption tools and expertise in order to become a hub for decrypting information lawfully obtained in criminal investigations and to better support Member States; further notes that the Commission amended the 2018 Europol budget with an additional EUR 5 million to reinforce its capabilities to decrypt such information and to develop a toolbox of

alternative investigation techniques at the disposal of Member States;

114. Welcomes the Paris Declaration of 5 November 2018 on the creation of a European Judicial Counter-Terrorism Register at Eurojust; calls for the immediate creation of such a register at Eurojust based on Council Decision 2005/671/JHA, amended by Directive 2017/541, with adequate financial and human resources;
115. Calls on the Member States to systematically involve Eurojust in their counter-terrorism investigations and prosecutions with a cross-border dimension and make efficient use of Eurojust's coordination tools;
116. Believes that operational agreements with third countries can be helpful for Europol's work, and notes the fact that the Commission is currently negotiating operational agreements with eight countries from the MENA region; requests the renegotiation of operational agreements with particular close partners, such as the EFTA countries;
117. Calls on Eurojust to continue enlarging its network of contact points in third countries, and encourages the posting to Eurojust of more liaison prosecutors, for example from the Western Balkans;
118. Is concerned about Interpol notices, particularly red notices, issued by certain third countries that use them for political purposes, thus impeding international cooperation in counter-terrorism;
119. Stresses the need for increased funding to CEPOL and to step up the development and delivery of innovative cyber-related training;
120. Invites CEPOL to continue developing training programmes for end users of SIS, on the basis of the SIRENE Manual and Best Practices Catalogue, on the topic of persons involved in terrorism or terrorism-related activities, including foreign terrorist fighters, who are the subject of SIS alerts;
121. Calls for an ongoing exchange of strategic information on counter-terrorism by national security services with EU institutions via the EU INTCEN; urges the Member States to further support the sharing of intelligence through the EU INTCEN and to optimise its work, so as to increase its effectiveness in the fight against terrorism;

Mutual recognition and mutual legal assistance

122. Expects the Member States to further educate and train judicial staff on the European Investigation Order (EIO) in order to ensure its comprehensive application;
123. Calls for the use of JITs in the event of terrorist attacks; believes that JITs increase the effectiveness of cooperation and the investigation of cross-border offences; further calls for the participation of Europol and Eurojust in these JITs, as this means better use of the resources and capabilities provided by the EU agencies; calls for improved and easily accessible funding to be provided for these JITs; further calls for the setting up of a special 'Erasmus for police officers' programme on the ground, preferably for junior and low-ranking officers, to encourage them to participate in JITs in other EU Member States at least once throughout their careers, thereby allowing those who do not necessarily have

experience in collaborating with their counterparts in other Member States to acquire additional experience and observe best practices on how to fight cross-border crime more effectively; encourages the extension of this programme to other security and correction officers in the future;

124. Calls on the Member States to make full use of the expertise and tools offered by Eurojust and the European Judicial Network (EJN), in particular in providing practical and legal information and support when it comes to MLA requests and assistance with mutual recognition requests, coordination of investigations and prosecutions, decisions on the best placed jurisdiction to prosecute, and coordination of asset seizures and confiscations;
125. Calls on OSPs and communications platforms to implement judicial decisions on counter-terrorism effectively; calls on the Commission to examine the possibility of a legislative proposal that obliges communication platforms present on the EU market to cooperate when it comes to encrypted communications if there is a judicial decision to that effect; stresses that such cooperation should not weaken the security of their networks and services, for instance by creating or facilitating ‘backdoors’;
126. Calls for the swift adoption of the Commission proposals for a regulation and directive aimed at improving cross-border access to electronic evidence; asks that OSPs provide single points of contact for law enforcement and judiciary requests;

External borders

127. Urges the Member States to invest in up-to-standard ICT equipment at all border crossings to allow for proper checks using all relevant databases; asks the Commission to set a benchmark for the technical standards of such ICT equipment, after consulting eu-LISA; considers that the work on the proposals for interoperability of information systems should be taken as an opportunity to improve and partially harmonise national IT systems and national infrastructure at border crossing points; welcomes the Commission’s proposal to reinforce support to Member States in securing the EU’s common external borders by at least tripling the budget for the Integrated Border Management Fund in the next MFF 2021-2027;
128. Welcomes the adoption of the recent reforms taken to strengthen the EU’s external borders at EU level, including the adoption of the EES and ETIAS and the reform of the SIS; calls on the Member States to fully implement these measures and, in cooperation with Europol, to support and contribute to the watch list for ETIAS and VIS; asks the Commission to closely monitor the implementation of the new Regulation (EU) 2017/458, which provides for systematic checks on all persons crossing the external borders and in particular the use of the derogation on systematic checks;
129. Calls on the Member States to bring their border management in line with the Integrated Border Management (IBM) concept; stresses the need to ensure full implementation of the IBM strategy at European and national level and thus strengthen the management of the external borders;
130. Welcomes the Commission proposal to the effect that information on long-stay visas and residence permits, including biometrics, for third country nationals should be included in VIS;

131. Urges the Member States to abandon the sale of residence permits and nationality via ‘golden visas’ and investment programme schemes given the high risk of corruption, abuse and misuse of the Schengen area for criminal purposes; asks the Commission to act sternly and swiftly demanding from Member States all relevant data and controls to ensure the integrity and security of the Schengen system;
132. Encourages the Commission to continue negotiations with third countries on return and readmission;
133. Encourages the Member States to use the revised visa waiver suspension mechanism, effectively notifying circumstances which might lead to a suspension of a third country’s visa waiver, such as a substantial increase in risk to public policy or internal security;
134. Calls on the Commission to prepare an evaluation of options and related impacts of a possible legislative proposal making it compulsory for air carriers and port, international bus or high-speed train operators to conduct conformity checks when passengers board, in order to make sure that the identity stated on the ticket matches the ID card or passport in the passenger’s possession; stresses the need to ensure that transport operators are not granted any tasks that only pertain to police authorities, such as proper identity checks or verification of the authenticity of ID or travel documents;

European Border and Coast Guard Agency (EBCGA)

135. Calls on the co-legislators to consider providing the EBCGA with a specific mandate for processing operational personal data suited to its operational role, including in the prevention and detection of cross-border crime and terrorism at the EU’s external borders; believes that such a mandate should allow for sufficient data retention periods and for the exchange of personal data with CSDP missions, Europol and Eurojust and, in specific circumstances and with the necessary safeguards, with third countries;
136. Notes that suspects whose personal data was previously processed by the EBCGA will disappear from the analytical system after 90 days and thus become unknown or new suspects; calls, therefore, for the retention period for personal data managed by the EBCGA for persons suspected of cross-border crime and terrorism to be extended to three years, in line with the retention period of Europol and Eurojust;
137. Considers it important for the EBCGA to have access to all relevant databases and information systems, especially the SIS, but also the EES, the VIS, Eurodac and the Europol information system, not only for the work of the border management teams, but also for analytical purposes related to new phenomena at the external borders or to changes in border movements or modus operandi;
138. Calls on the co-legislators to make it compulsory for the EBCGA to share urgent information with the Member States;
139. Urges the Member States and the EU bodies such as Europol and INTCEN to regularly pass to the EBCGA strategic information on counter-terrorism related to the border dimension, and to investigate whether any automated exchange with EBCGA of important (background) information coming from national investigations into incidents and illegal activities at border crossing points and irregular entry/exit movements, as well

as the use of intelligent ICT systems, could bring added value when establishing a comprehensive situational picture, considering also the manpower that the data analysis would require; believes such information should also include feedback after second line security checks and information related to document fraud;

140. Invites the EBCGA to develop training programmes and deliver training courses for border guards focusing on reinforcing checks against the relevant databases at external borders and supporting the implementation of common risk indicators;

Battlefield information

141. Welcomes Europol's participation in the law enforcement cell of the US-led Operation Gallant Phoenix (OGP) in Jordan, whereby it processes information obtained from the battlefield (and if possible helps to identify the victims) and exchanges it through established channels and procedures with Member States' law enforcement authorities via the Europol National Units; calls for full access for Europol to OGP;
142. Encourages all relevant actors to develop approaches making it possible to transmit and share battlefield information, within the scope permissible in law and with the necessary safeguards such as source protection with the civilian sphere, and to enter this information in the relevant databases so that the information reaches border controls at the EU's external frontiers in time; calls as well for the sharing of this information for purposes of investigation and prosecution;

Operation Sophia

143. Calls on the Council to extend the mandate of EUNAVFOR MED Operation Sophia, to enlarge its territorial scope in order to tackle ghost landings, and to specifically include in its mandate cooperation in the fight against terrorism;
144. Welcomes the creation of a crime information cell pilot project within EUNAVFOR MED Operation Sophia, composed of staff members from the relevant law enforcement authorities of Member States, Frontex and Europol, in order to improve information-sharing between them;
145. Calls on the Member States to seek an international legal mandate for EUNAVFOR MED Operation Sophia to take operational measures against vessels and related assets, even inside coastal states' territorial waters, arresting crews and impounding vessels and related assets suspected of being used for human smuggling or violating the UN arms embargo, but also for terrorism-related offences and oil smuggling;

Terrorist financing

146. Welcomes the legislative measures newly adopted at European level in the fight against terrorist financing; calls on Member States to fully implement all European anti-money laundering directives and instruments relating to the fight against money laundering and the financing of terrorism; urges the Commission to ensure that these instruments are transposed and function properly;
147. Encourages Member States and third countries to effectively and fully implement without

delay the conclusions of the ‘No money for terror’ conference held in April 2018 in Paris, as well as the FATF recommendations and the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the ‘revised FATF recommendations’); calls on the Commission and the Member States to support third countries in the implementation of these recommendations by providing technical assistance and exchange of good practices;

148. Calls on those Member States which have not yet ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism to ratify and transpose it;
149. Welcomes the methodology presented by the Commission regarding high-risk third countries that pose a threat to the financial system of the EU; calls on the Commission to apply this methodology, and in particular to establish an EU list of AMLD high-risk third countries by means of an independent, objective and transparent assessment, and to carry out this assessment as soon as possible;
150. Calls on the Member States to step up the monitoring of organisations suspected of engaging in illicit trade, smuggling, counterfeiting and fraudulent practices, via the establishment of JITs with Europol;
151. Is highly concerned at the scale of illicit tobacco markets in the EU, the proceeds of which can be used to finance terrorism, including via excise fraud; invites the Member States to consider ratifying and implementing the Protocol to Eliminate Illicit Trade in Tobacco Products to the WHO Framework Convention on Tobacco Control (WHO FCTC);
152. Welcomes the proposal for a regulation on the import of cultural goods; calls on the Commission to propose legislation for a robust tracing system for artworks and antiques entering the EU market, especially for items originating from conflict-affected and high-risk countries as listed by the Commission, as well as from organisations, groups or individuals included on the EU terror list; believes that this initiative should be supported by the creation of a standardised permit, without which trading in these items would be illicit, and of a passport for the export of each item; believes that digital tools should be developed for checking the authenticity of the documents concerned; considers that a comprehensive register of antiques for sale should be systematically kept and updated by art dealers;
153. Calls on the Member States to make it mandatory for companies involved in art dealing and the storing of antiques (i.e. so-called ‘freeports’) to declare all suspicious transactions, and to make the owners of companies dealing in and storing art and antiques who become involved in the trafficking of such goods subject to effective, proportionate and dissuasive penalties, including criminal penalties where necessary;
154. Welcomes the adoption of new rules regarding the control of cash entering or leaving the European Union,¹ and calls for their swift implementation; calls on the Commission to evaluate whether other assets should be included within the scope of this regulation, whether the disclosure procedure for unaccompanied cash fits the purpose, and whether

¹ Regulation of the European Parliament and of the Council on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 - OJ L 284, 12.11.2018, p. 6.

the threshold for unaccompanied cash should be reviewed in the future;

155. Calls on the Member States to cooperate more with Europol AP FURTUM and, as requested by UN Security Council resolution 2347, to provide customs and law enforcement authorities and public prosecutors' offices with dedicated personnel, as well as with effective tools and adequate training, through cooperation with the World Customs Organisation (WCO) and Interpol;
156. Calls on the Commission to develop, together with Member States and international partners, the monitoring of financial flows in a targeted manner, as well as ways of identifying users of electronic wallets, virtual currencies and prepaid cards, crowdfunding platforms and online and mobile payment systems in police or judicial investigations; calls on the Member States to regulate IVTS, emphasising that the aim is not to crack down on traditional informal money transfers, but on trafficking involving organised crime, terrorism or industrial/commercial profits deriving from 'dirty money'; calls for a focus on virtual currencies and FinTech and for exploration of the possibility of extending sanctions on those who abuse and misuse social media fundraising for terrorist purposes; calls on the Member States to encourage cryptocurrency companies to use analysis tools to assess potential criminal activity associated with the destination and recipient addresses and to ensure that they fully apply the anti-money laundering legislation when users convert cryptocurrencies to real currency;
157. Calls on the Commission to put forward a legislative proposal requiring mandatory registration and identification when conducting financial transactions via money transfer companies;
158. Calls on the Commission to assess the possibility of regulating alternative remittance systems by, for example, introducing mandatory registration or a licensing regime for brokers and an obligation of clear and precise record-keeping;
159. Is concerned about recent findings concerning increased activities of large-scale money laundering as a source for terrorism financing¹ through certain banking institutions in the euro area; calls for the establishment of a European Union Terrorist Financing Tracking System (TFTS) targeted on transactions by individuals with links to terrorism and their financing within the Single Euro Payments Area, which would ensure that a balance is struck between security and individual freedoms; points out that European data protection standards would apply to this intra-European system;
160. Urges better cooperation and exchange of information between obliged entities, FIUs and competent authorities regarding terrorist financing activities; calls on the Member States to ensure that their FIUs, regardless of their type, have unhindered access to financial information with a view to effectively combating terrorist financing; calls for greater harmonisation of the status and functioning of European FIUs; welcomes the proposal for a directive of the European Parliament and the Council laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences²; calls for better and fuller exchange of information and cooperation between Europol, Eurojust and third countries regarding

¹ [http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614496/IPOL_IDA\(2018\)614496_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614496/IPOL_IDA(2018)614496_EN.pdf)

² COM(2018)0213.

terrorist financing; calls for the swift adoption of the draft directive on access by law enforcement authorities to financial information and exchange of information between FIUs;

161. Urges Member States to allocate more resources to the national FIUs; calls on the Member States to make better use of the informal network of European Financial Information Units (FIU.net) and to further develop the capabilities of this network through Europol, so that it can be used to its full potential and in order to overcome the current cooperation difficulties and facilitate the manual processing of bilateral requests, while ensuring the autonomy and independence of FIUs; believes that an EU FIU could be necessary to coordinate, assist and support Member States' FIUs in cross-border cases if strengthening FIU.net appears insufficient;
162. Stresses the importance of enhancing interaction and exchange of information between investigative authorities and the private sector - specifically, obliged entities under the directive on anti-money laundering and countering terrorist financing (AML/CFT Directive) - in order to overcome the shortcomings of segregated and incomplete information submitted by suspicious transaction reports; calls on the Commission and the Member States to develop dedicated fora for sharing financial information, including on use of virtual currency and including the private sector, within safe channels and subject to EU data protection standards; notes the important role that Europol could play in this regard;
163. Calls for the organisation of specialised training courses for the law enforcement and judicial authorities of Member States on methods and developments in terrorist financing, in order to enhance capacity in Member States for investigating illicit activity, including on virtual currencies; stresses that such training should ensure a standard level of law enforcement competency across the EU, so that certain Member States do not fall behind; emphasises the importance of conducting the EU-wide risk assessments of virtual currency activities and of coordinating investigative initiatives to use findings from those assessments to develop strategies for regulatory and law enforcement approaches over the short, medium and long term;
164. Emphasises the vital importance of financial intelligence and tax information for counter-terrorism; regrets that in several Member States agencies combating money laundering and the financing of terrorism are among the intelligence services that receive the least funding; calls on the Member States to boost their human and financial resources significantly in the field of investigation and law enforcement in order to combat tax evasion and tax fraud that may be financing criminal or terrorist activities;

Critical Infrastructure Protection (CIP)

165. Calls on those Member States which have not yet done so to establish national CIP programmes addressing the issues identified by the Commission in its 2006 communication on a European Programme for Critical Infrastructure Protection (EPCIP), especially with regard to potential vulnerabilities; believes that EPCIP should be revised and updated;
166. Recalls that sensitive data and the systems it underpins are also part of critical infrastructure in Member States and thus should be properly safeguarded against

cyberattacks¹;

167. Welcomes the Commission's Action Plan to support the protection of public spaces, and encourages the Member States to exchange best practices and establish collaborative networks between public and private sector actors if necessary;
168. Urges that the co-legislators set up a successor to ISF Police for the new MFF period, with at least similar levels of funding;
169. Calls for the role of the Critical Infrastructure Warning Information Network (CIWIN) to be strengthened;
170. Demands that the designation of European Critical Infrastructures (ECIs) with an impact on more than one Member State follows a multilateral process involving all of the potentially affected Member States;
171. Calls on the Member States to establish national multidisciplinary crisis response centres for coordination and emergency response in case of an attack or incident; calls for these centres to make use of the EU Integrated Political Crisis Response (IPCR) arrangements contributing to and drawing on three key instruments, namely the central IPCR 24/7 contact point, the IPCR web platform, and the Integrated Situational Awareness and Analysis (ISAA) report;
172. Asks the Commission to establish a mapping of national crisis centres or crisis response mechanisms;
173. Encourages the Commission to continue to elaborate and disseminate guidance for Member States with the aim of increasing the protection of public spaces, as announced in its Action Plan to support the protection of public spaces;
174. Calls for Directive 2008/114 to be revised, in order to: provide similar rules and procedures for 'operators of essential services' as in the NIS Directive; ensure that designation of ECIs is carried out on the basis of an analysis of the systems supporting vital and cross-border services, rather than a sector-by-sector approach, taking due account of the importance of cybersecurity; allow the Commission to designate assets of pan-European services as ECIs; take due account of existing interdependencies; create an obligation for public and private operators of critical infrastructures to report incidents, conduct stress tests, provide appropriate training at the designated contact points, and establish quality requirements as regards business continuity plans, including operational plans, in the case of an incident or attack;
175. Recommends that the private sector be involved when devising programmes for the protection of critical infrastructure and soft targets, including in the context of cybersecurity; highlights the need to develop public-private dialogues to this effect and to develop national and local resilience;
176. Calls on the Commission to propose a European Certification Initiative for private

¹ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union - OJ L 194, 19.7.2016, p. 1.

security companies, aiming to specify the requirements and conditions under which they can operate within the critical infrastructure environment;

177. Underlines the need to put in place effective response strategies including clear lines of communication in the case of an attack, notably as regards immediate reaction teams, in order to reduce casualty rates and improve the management of the situation so as to minimise the impact on the public; urges the Member States to step up their engagement with the mechanisms that have already been put in place at European level;
178. Calls for the swift adoption of the revision of the Union Civil Protection Mechanism in order to strengthen prevention and preparedness, exchange of information at EU level, and the capacity of Member States to deal with different types of disasters;
179. Calls on the Commission to conduct an evaluation of options and related impacts for the creation of a system enabling the verification of the identity of persons renting vehicles, aircraft and watercraft;
180. Welcomes the cross-border exercise to improve the protection of soft targets against terrorist attacks, involving Belgium and the Netherlands, which took place in June 2017; notes that the exercise was funded by the Commission with the aim of measuring preparedness and crisis management functions in a situation where two attacks take place simultaneously in different countries; calls for similar exercises to be carried out involving Member States; believes that the EU can offer a supporting framework to that cooperation, notably in areas such as medical care (the European Medical Corps), public safety (the Health Security Committee), or decontaminating protocols, as well as coordinating special intervention units from the national police and civil protection forces;
181. Calls for legislation in the field of terrorism and national, regional and local response strategies for protection, resilience and response in case of an attack, to take into account the specific needs and circumstances of vulnerable people, such as persons with disabilities and minors; further calls for the involvement of persons with disabilities and their representative organisations in the decision-making that affects them;

Explosives precursors

182. Observes that regulated explosives, precursor substances and mixtures are accessed by terrorists; welcomes, therefore, the proposal of April 2018 for a regulation on the marketing and use of explosives precursors;
183. Calls for the establishment of a European system of licences for specialised buyers, different from the general public, which obliges economic operators to be registered in order to be allowed to legally manufacture, distribute or sell substances listed in the Annexes, or involving mixtures or substances containing them; calls on the Member States to set up inspection systems to identify non-compliance with the regulation by economic operators;
184. Welcomes the impact assessment of Regulation 98/2013 on explosive precursors, and encourages the co-legislators, for the proposal for a regulation 2018/0103/COD, to evaluate the mandatory information exchange process; calls for market surveillance

authorities to reinforce their surveillance activities for explosives precursors, as they clearly have the potential to adversely affect public security;

185. Calls on customs authorities, in cooperation with law enforcement authorities and on the basis of information from Europol and other data analysis systems, to improve the targeting of illicit online purchases of explosives precursors through screening on the basis of cargo information submitted by traders prior to the arrival or departure of goods in or from the EU, also making use of the customs risk management system (CRMS);
186. Calls on the Commission to work together with businesses on promoting guidelines for e-marketplaces on the security of sales of explosives precursors, restricting purchases of certain substances to professional users, and further detailing restricted product policies by determining permitted levels of quantity and purity;
187. Calls for the uniform use of certain standardised naming conventions that would allow economic operators and e-marketplaces to identify chemicals posted on their sites; calls on e-marketplaces subsequently to screen postings against these standardised keyword lists in order to monitor listings of regulated items;
188. Calls on the Commission to consider establishing common criteria for licences by harmonising conditions for granting and refusing requests and facilitating mutual recognition between Member States;

Illicit weapons

189. Calls for the rapid and effective implementation of the directive on control of the acquisition and possession of firearms in order to monitor their sales and use as effectively as possible and to avoid firearms and related equipment and tools being illicitly trafficked from both within and outside the EU; calls for the loopholes in the existing regulatory framework to be closed, for example by taking measures to stop the circulation of easy-to-convert blank-firing guns, Flobert guns, alarm pistols and similar weapons;
190. Calls on the Member States to adopt firearms and ammunition surrender programmes tailored to the specific context of the illicit firearms markets; calls for the effective penalisation of illicit firearms possession and trafficking; calls for strict and diligent implementation by Member States of the Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment;
191. Supports the revision of the EU Strategy to Combat the Illicit Accumulation and Trafficking of Small Arms and Light Weapons (SALW) by taking into account the new security and security policy context and the developments in SALW design/technology affecting the capacity to address the threat;
192. Believes the Member States should adopt an ‘investigate the gun’ approach, using specialised law enforcement cells and designed to pinpoint the actors and networks involved in this type of trafficking, combined with the checking of the various national ballistic databases;
193. Recalls that the Commission has adopted a report on the evaluation of Regulation

258/2012 that establishes rules for authorised export, import and transit for non-military firearms, reaching the conclusion that the regulation continues to be necessary but that its effectiveness is limited by the lack of precision of some of its provisions and the complexity of the interaction with other EU legislative instruments; encourages Member States' law enforcement authorities to set up specialised police teams to tackle illicit firearms trafficking, equipped with sufficient staff, expertise and equipment;

194. Encourages Member States to evaluate possible restrictions on the carrying of knives without a valid reason, the banning of particularly harmful knives such as zombie or butterfly knives, and the enforcement of these measures online;

External dimension

195. Urges the EU and its Member States to pursue global actions on the international stage to address the protracted conflicts that destabilise entire regions, feed the cycle of violence and suffering, and unfortunately provide fuel to many terrorist narratives;
196. Calls for the intensification of EU cooperation with neighbouring countries, particularly with transit countries and those that are the destination of foreign fighters, in the area of counter-terrorism; considers that the EU must maintain a global approach to counter-terrorism, with a specific focus on cooperation with key third countries on the basis of clearly defined priorities;
197. Considers that CT is a field which requires concrete expertise; calls, therefore, for the deepening of professionalisation of the EU network in this area, in particular by granting CT operative personnel coming from Member States a better and longer integration into the EU structure, beyond a single assignment within an EU delegation; considers that posting within the EU institutions would maximise expertise and use of competences in the field of CT;
198. Calls on the Commission to strengthen support to third countries, especially neighbouring countries, in their efforts to tackle crime and trafficking as a source of terrorist financing, and to strengthen links with them in order to accelerate the freezing of assets; is concerned, however, that anti-terror legislation in some of the EU's partner countries has too broad a scope and is abused to repress peaceful dissent; warns that criminalising the peaceful expression of legitimate grievances may lead to radicalisation; believes that the EU should strongly invest in actions addressing the root causes of terrorism in third countries; strongly supports external counter-extremism programmes in prisons, cooperative programmes with religious leaders and communities, inter-religious dialogues and fora, and in general all types of reconciliation programmes which lower inter-community tensions and prevent sectarian policies, in particular by economic, social and educational means;
199. Calls on the Member States to make full use of intelligence analysis on CT from the European Union Intelligence and Situation Centre (EU INTCEN); calls on the Commission to give a clear mandate for INTCEN to reach out directly to analysts within EU delegations in order to increase the flow of relevant information to the EU's central intelligence system;
200. Calls for enhanced cooperation and identification of synergies between Common Security

and Defence Policy (CSDP) missions and operations and Justice and Home Affairs Council (JHA) actions;

201. Calls for the simplification of the EU restrictive measures system in order to make it an effective tool in the area of CT;

Victims of terrorism

202. Calls on the Commission to establish an EU Coordination Centre for victims of terrorism (CCVT), which would provide timely and adequate crisis support in cases of attacks in one or more Member States; considers that inter alia the role of the CCVT should be to ensure urgent assistance to victims from another Member State as well as the provision of expertise at EU level by promoting exchange of knowledge, protocols and best practices; stresses the need to extend support and protection measures to indirect victims, such as victims' relatives, eyewitnesses and first responders;

203. Considers that, once established, the CCVT could collect statistics, and assist in and coordinate the setting-up of registers of victims of terrorism in Member States and at European level, on a basis of full compliance with the data protection legislation, in particular with regard to data subjects' rights and the purpose limitation principle; considers that it could also investigate and promote best practices - such as the creation of protocols - in order to:

- 1) guarantee initial emotional attention for the victims of terrorism;
- 2) provide them with subsequent psychological and emotional support;
- 3) avoid secondary victimisation during the judicial process or in bureaucratic interactions;
- 4) guarantee effective access to justice, especially in the case of attacks involving transnational victims;
- 5) foster good practices for the media on matters that are sensitive topics for victims of terrorism and their families;

considers that the CCVT could also establish a public register of accredited victim support organisations, which would be available for consultation and improvement of the protocols drawn up; urges Member States to appoint a single authority responsible for acting as a national contact point for the CCVT once established;

204. Calls on the Commission to establish a single on-line platform in all EU languages covering the rights of and support for victims of terrorism, which would be managed by the CCVT, with a single contact point at national level in each Member State, including a helpline;

205. Calls on the Commission to put forward a legislative proposal on the victims of terrorism that responds effectively to victims' needs in the short and long term, including a common definition of the status of victim of terrorism and of victims' rights, and a standardised form for claiming compensation, outlining clear duties and deadlines for insurers;

considers that there should be a simplified procedure at national level for granting automatic compensation to victims of terrorism shortly after an attack in order to meet their immediate needs, and that the question of further compensation should be reviewed at regular intervals on the basis of an assessment of the victim's situation;

206. Believes that the scope of application of the common definition of 'victim of terrorism' shall cover at least: 1) people deceased; 2) people who suffered physical and/or psychological damage; 3) people who suffered kidnapping or threats; 4) the spouse of the deceased or person linked to them by the same relation of affection, also including parents and children, grandparents and siblings;
207. Calls on the Member States to task multidisciplinary crisis response centres that provide coordination and emergency response with the implementation of national and local protocols relating to the prioritised swift identification of victims and their immediate management and referral to the competent services;
208. Calls on the Member States to ensure that a comprehensive response to the specific needs of victims of terrorism immediately after a terrorist attack and for as long as necessary is provided within the national emergency response infrastructure; considers that to that end, Member States should set up a single updated website with all relevant information and an emergency support centre for victims and their family members providing psychological first aid and emotional support, as referred to in Directive (EU) 2017/541 of 15 March 2017 on combating terrorism;¹
209. Stresses that notification of victims' families should be delivered by specifically trained professionals in a dignified, humane and appropriate way, ensuring that the media do not reveal their identities without their prior consent, and that particular attention, respect and priority should apply when dealing with children;
210. Calls for the full and effective implementation of Directive (EU) 2015/637 in order to ensure consular protection for EU citizens in third countries where their Member States are not represented; underlines that a growing number of European citizens have suffered terrorist attacks in a country that is not their own, and therefore urgently calls for the establishment of protocols in Member States to help non-national Europeans in the event of a terrorist attack, in line with Directive (EU) 2017/541 on combating terrorism;
211. Calls on the Member States to ensure that the necessary assistance provided to victims of terrorism also encompasses measures such as first aid, psychological support, protection from secondary victimisation, legal aid, effective access to justice, cash advances to help cover immediate expenses, certified childcare and home support, tax relief schemes, and help with transport in the case of a temporary or permanent disability;
212. Calls on the Member States, with the support of the Commission, to ensure that professionals of all relevant national services are adequately trained concerning the specific needs of victims of terrorism, and especially first responders; points out that the CCVT will help in the tasks of professional training, including for police officers, lawyers and other professionals dealing with victims, and with insurance companies or

¹ OJ L 88, 31.3.2017, p. 6.

compensation authorities;

213. Calls on the Member States to set up legal mechanisms to criminalise the glorification of a specific act of terrorism as it humiliates the victims and causes secondary victimisation by damaging the victims' dignity and recovery;
214. Calls on the institutions concerned to provide safeguards to prevent any subsequent victimisation derived from humiliation and attacks on the image of the victims coming from social sectors related to the attacker;
215. Asks Member States to forbid homages to those found guilty of terrorist activities by a judgment that has become final;
216. Asks Member States to pay special attention to victims where they can suffer harassment or fear that they might be attacked again by the social entourage of the aggressors;
217. Calls on the Member States to ensure that victims of sexual and other severe forms of violence perpetrated by Daesh terrorists outside of the EU are safe and without fear in the EU; calls on the Member States to bring such cases to court, even if the crimes have been committed outside of the EU and to involve the victims as valuable witnesses in the court proceedings;
218. Calls on the Commission to consider a financial scheme for the compensation of victims in the event of large-scale terror attacks, in order to support Member States when needed and in cross-border cases;
219. Calls on the Commission to initiate a dialogue with the Member States in order to reduce the large disparities existing in the levels of financial compensation granted at national level by Member States to the victims of terrorist attacks;
220. Calls on the Member States to ensure that all victims of terrorism are entitled to be a party in judicial proceedings relating to a terrorist attack concerning them, and to take into account the specific situation of cross-border victims; asks Member States to guarantee that degrading or humiliating contacts between the victims and the aggressor or the aggressor's entourage do not occur in criminal procedures;
221. Asks for enhanced promotion of the European Day of Remembrance of Victims of Terrorism (11 March);

Fundamental rights

222. Stresses that security measures, including counter-terrorism measures, must be pursued through the rule of law, must respect fundamental rights and must be adopted in a clear legal framework; calls, therefore, on the Member States and the EU institutions, when adopting and applying counter-terrorism measures, to respect fundamental rights, including those relating to privacy and data protection, freedom of thought and expression and non-discrimination, as well as procedural safeguards, including the presumption of innocence, the right to a fair trial, the right to information, and control by a judicial authority, as well as ensuring that individuals have effective remedies at their disposal to challenge violations of their fundamental rights, including the possibility of judicial

redress;

223. Calls on the Member States and the EU institutions, when adopting and applying CT measures, to find the right balance between the different fundamental rights involved and security needs; considers in this respect that the first priority should lie in protecting people's fundamental right to life and right to security;
224. Reiterates that international and regional human rights law makes it clear that states have both the right and the duty to protect individuals under their jurisdiction from terrorist attacks in order to ensure respect for the right to life and the right to security; recalls that the EU's cooperation with third countries in the field of CT must be based on respect for international human rights and humanitarian law, including the prohibition of torture;
225. Calls on the Commission and the Fundamental Rights Agency (FRA) to examine the challenges that exist in the field of counter-terrorism policies and to identify best practices within Member States, including practices which take into account the specific circumstances of vulnerable people such as persons with disabilities and minors; calls on the Commission to encourage the exchange of best practices and to develop guidance in this respect; further recalls that Parliament, the Council and the Commission have the option to request opinions from the FRA, within the context of its Multiannual Framework, on counter-terrorism measures;
226. Calls on the Member States to ensure that the necessary data protection safeguards are in place, in accordance with the applicable EU legislation, including appropriate technical and organisational measures to protect the security and confidentiality of personal data; urges them to provide clear rules as to who can access and consult which data in the systems, to maintain records of consultation and disclosure, and to ensure rights of access, rectification, erasure and restriction, as well as rights to compensation and judicial redress; calls on the Commission and the European Data Protection Supervisor to further develop innovative privacy-by-design solutions;
227. Believes that sound CT policies necessitate robust mandates for the public bodies involved in the fight against terrorism, as well as a high degree of public support for those authorities; notes the important role that oversight can play in fostering public trust and support; calls on Member States to provide oversight mechanisms for counter-terrorism measures in order to assess their impact; further calls on Member States to ensure democratic oversight and public accountability for all security and intelligence services, while preserving the necessary degree of secrecy;

o

o o

228. Instructs its President to forward this resolution to the Council and the Commission.

EXPLANATORY STATEMENT

Background

During the recent years, the EU faced an unprecedented wave of terrorist attacks on its soil, which have catapulted the issue of security to the forefront of citizens' concerns and have highlighted the problems with cooperation and sharing of information in this field. In fact, in a June 2017 Eurobarometer survey regarding citizens' overall awareness, experiences and perceptions of security, 92% of respondents agreed that national authorities should share information with the authorities of the other EU Member States to better fight crime and terrorism.

In the wake of these attacks, Member States and the EU have struggled to respond to the concerns of the citizens and to the challenges posed by the terrorist threat. New legislation was proposed, existing legislation was or is in the process of being revised and a debate was launched both in the EU and in the Member States as to how to best respond to the terrorist threat.

To react to these developments and in order to be able to provide its contribution, the European Parliament set up a special committee on terrorism (TERR) on 6 July 2017. The Committee was constituted on 14 September 2017. Its main goal is to address the practical and legislative deficiencies in the fight against terrorism, with a particular focus on cooperation and exchange of information.

Horizontal issues

One of the main issues identified and highlighted repeatedly by experts and practitioners is the need to implement fully the existing legislation in this field. Member States must not only provide the legislative framework, but also the necessary technical equipment as well as sufficient and well-trained staff to ensure the practical application of the existing measures.

The necessity of an appropriate data retention regime was also consistently raised during the work of the Committee. The rapporteurs believe it is necessary to provide for an EU regime on data retention, in line with the requirements stemming from the case-law of the Court of Justice, while taking into account the needs of the competent authorities and the specificities of the counter-terrorism (CT) field.

The rapporteurs regret that the existing opt-outs by some Member States from police and judicial cooperation measures for the prevention, detection, investigation and prosecution of terrorist offences could endanger the speed and efficiency of terrorism investigations and may have detrimental effects and call on Member States to abstain from opt-outs in this crucial field.

Preventing and Countering Radicalisation

Radicalisation as a source of home-grown terrorist attacks poses a big threat to the European Union. The main contributing factors to radicalisation are radical content on social media, personal contact with radicalised people and the ecosystem of radicalisation, including hate preachers and radical content in books, online or in audiovisual media. Another hotbed of radicalisation are prisons.

While the European Union has already launched several initiatives to tackle radicalisation, such as the Radicalisation Awareness Network and the EU Internet Forum, a more concerted and focused approach is needed to deal with this threat. Therefore, the rapporteurs propose the creation of a new EU Centre of Excellence for Preventing Radicalisation, which should coordinate and facilitate cooperation among Member States, policy makers, practitioners, experts and researchers in the area of preventing radicalisation and contribute to a targeted use of EU funds in this field. The role of civil society organisations and NGOs, which are indispensable for carrying out the preventing and countering radicalisation projects at local level, must also be highlighted. The necessary legal and financial pre-conditions for their work must be developed by the Member States.

In order to tackle the spreading of radical content online, the rapporteurs consider that the limit of voluntary action of companies has been reached and call on the Commission to present a legislative proposal obliging the companies to remove the terrorist content fully within one hour and to introduce clear reporting obligations for the companies on the incidence of the terrorist content and the removal rates, as well as sanctions for non-compliance.

Cooperation and information exchange

Cooperation and information sharing are indispensable to the fight against terrorism. The speed with which some of the recent attacks have been planned and executed requires that exchange of information and intelligence be rapid in order to be effective and to help prevent attacks. The cross-border nature of terrorism requires a strong coordinated response and cooperation within and between the Member States, as well as with and among the competent Union agencies and bodies.

The rapporteurs believe that there needs to be a shift to a new approach in information sharing. CT-related information must be shared by default and it should only be possible not to exchange in specific cases where the circumstances require that the information be withheld. Furthermore, technical solutions need to be implemented allowing for an automated loading of information from the regional to the national/federal systems and to the European systems. Cooperation and exchange of information between the different services, in particular between law enforcement and intelligence services, must be strengthened.

The rapporteurs calls for Europol to become a true hub for information exchange and cooperation in the field of counter terrorism in the EU. For this to happen, however, Member States must ensure the utmost flexibility for contacts between Europol and the relevant authorities in the Member States when it comes to terrorist offences. In addition, JITs must be used consistently in case of terrorist attacks, considering the predominantly cross-border character of these attacks. Europol and Eurojust should participate in these JITs as a matter of principle.

As for interoperability of centralised systems, the rapporteurs believe this a welcome step, but that it is also only a first step in creating a comprehensive framework of interoperable information systems. In the future additional systems, including national and decentralised systems, need to be covered.

External borders

A Schengen area without internal borders is only sustainable if the external borders are

effectively secured and protected. Some of the recent terrorist attacks have demonstrated major failures in European border-control policy since at least eight of these attacks' operatives entered Greece via irregular flows in July, August and October 2015. Although major progress has been done in this area and new measures were introduced, such as obligatory checks of SIS and Interpol databases at border crossing points, still more needs to be done in the area of integrated border management.

What is especially important is the creation of material conditions at the borders for the implementation of the new legislation, the introduction of biometric checks, interoperability of the databases and the use of all available data, such as PNR or battlefield evidence, in order to identify potential terrorists before they enter the territory of the EU. The role of Frontex in the integrated border management also has to be highlighted.

The rapporteurs recognise that EUNAVFOR Med Operation Sophia is currently the main security provider in the Mediterranean and it has at its disposal the necessary resources and capabilities to contribute also to the fight against terrorism. Therefore, they call for the mandate of operation Sophia to be amended accordingly and its territorial scope to be enlarged to cover also the new migration flows from Tunisia. A new UN Security Council resolution could be considered allowing Sophia access to coastal states' territorial waters in order to perform checks on suspicious vessels.

Terrorist financing (TF)

TF should be comprehensive and not just focus on financial flows but also on the financing of radicalisation, TF measures must address both large-scale funding of terrorists organisations and attacks that may require little money. Hence, it is paramount that TF exploits to the full financial intelligence in order to foster prevention.

The Member States and the Commission are requested to establish a European Union Terrorist Financing Tracking System (TFTS) for transactions of individuals with links to terrorism and its financing made within the Single Euro Payments Area, complementary to the Terrorist Financing Tracking Program (TFTP) with the US.

Protection of critical infrastructure

The rapporteurs call for Directive 2008/114 to be revised, to ensure that designation of European critical infrastructures (ECIs) is based on an analysis of the systems supporting vital and cross-border services, rather than a sector-by-sector approach. The new Directive should introduce an obligation to report incidents related to critical infrastructure, a framework for conducting stress tests, appropriate training of the designated contact points and quality requirements as regards the business continuity plans in the case of an incident or attack. The Commission must be able to designate assets of pan-European services such as Galileo or Eurocontrol as ECIs.

The rapporteurs also call on the Member States to put in place effective response strategies and to establish national multidisciplinary crisis response centres for the coordination and emergency response in case of an attack or incident.

Explosives precursors

In 2015 and 2016, explosives were used in 40% of the committed terrorist attacks in the EU, despite Regulation 98/2013 banning seven substances from being made available to the general public over the limit value and requiring suspicious transactions on eleven products to be reported. This is because perpetrators and potential terrorists still manage to buy the precursors online and because the current regulation allows different systems to be applied by Member States.

The rapporteurs therefore welcome that the Commission has proposed a new regulation, abolishing the registration system for prohibited substances and defining more clearly who is to be considered as the general public and as professional user. The rapporteurs call for stricter monitoring of online purchases and for refining the current customs common risk criteria to improve the targeting of illicit online purchases of explosive precursors.

Illicit firearms trafficking

Firearms were used in 41% of all attacks, a slight increase compared to 2016 (38%). The threat of firearms being used in terrorist attacks remains, also due to an increase in converted blank firing weapons and reactivated firearms available on the illicit weapons market. The rapporteurs call therefore for closing the loopholes in EU and national firearms legislation, for example, by taking measures to stop the circulation of easy-to-convert blank-firing guns and Flobert guns and alarm pistols.

Victims of terrorism

Member States are urged to transpose the provisions set out in Directives (EU) 2017/541 and 2012/29.

The Commission is requested to put forward a legislative proposal on victims of terrorism with a clear definition of their status and rights, including eligibility criteria and levels of compensation. It should also establish an EU Coordination centre for victims of terrorism (CCVT) so that it can provide timely and adequate crisis support in case of an attack in one or several Member States.

Fundamental rights

Respect for fundamental rights is an essential element in successful counter-terrorism policies and the correct balance needs to be found between the different fundamental rights involved to ensure the effectiveness of CT measures. In this respect, the rapporteurs underline that, while privacy is a fundamental right, the first priority should lie in protecting people's fundamental rights to life and security. In addition, the specific needs and circumstances of vulnerable/disabled people need to be taken into account.

INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE

Date adopted	13.11.2018
Result of final vote	+: 23 -: 2 0: 5
Members present for the final vote	Ivo Belet, Caterina Chinnici, Javier Couso Permuy, Edward Czesak, Arnaud Danjean, Gérard Deprez, Agustín Díaz de Mera García Consuegra, Doru-Claudian Frunzuliță, Elisabetta Gardini, Ana Gomes, Sylvie Guillaume, Monika Hohlmeier, Eva Joly, Jeroen Lenaers, Péter Niedermüller, Maite Pagazaurtundúa Ruiz, Birgit Sippel, Helga Stevens, Elena Valenciano, Geoffrey Van Orden, Kristina Winberg, Milan Zver
Substitutes present for the final vote	Lynn Boylan, Claude Moraes, Morten Helveg Petersen, Emil Radev, Josep-Maria Terricabras
Substitutes under Rule 200(2) present for the final vote	France Jamet, Manolis Kefalogiannis, Lukas Mandl

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

23	+
ALDE	Gérard Deprez, Maite Pagazaurtundúa Ruiz, Morten Helveg Petersen
ECR	Edward Czesak, Helga Stevens, Geoffrey Van Orden
ENF	France Jamet
PPE	Ivo Belet, Arnaud Danjean, Agustín Díaz de Mera García Consuegra, Elisabetta Gardini, Monika Hohlmeier, Manolis Kefalogiannis, Jeroen Lenaers, Lukas Mandl, Emil Radev, Milan Zver
S&D	Caterina Chinnici, Doru-Claudian Frunzulică, Ana Gomes, Claude Moraes, Péter Niedermüller, Elena Valenciano

2	-
GUE/NGL	Lynn Boylan, Javier Couso Permuy

5	0
ECR	Kristina Winberg
S&D	Sylvie Guillaume, Birgit Sippel
VERTS/ALE	Eva Joly, Josep-Maria Terricabras

Key to symbols:

+ : in favour

- : against

0 : abstention