POLICY INSIGHTS
Thinking ahead for Europe

No 2017-32 / August 2017

Reflections on the Terrorist Attacks in Barcelona

Constructing a principled and trust-based EU approach to countering terrorism

Sergio Carrera, Elspeth Guild and Valsamis Mitsilegas

Summary

This Policy Insight examines EU counter-terrorism policies in the aftermath of the recent terrorist attacks of 18 August 2017 in Catalonia and explores what more the EU can do to enhance the effectiveness and efficiency of those policies. To this end, it puts forward two policy recommendations:

- The EU should construct and progressively develop a principled and trust-based policy approach to countering terrorism.
- Such an approach would consist of an evaluation (fitness check) and regular reappraisal of the effectiveness and efficiency of current EU policies and their priorities –particularly those related to information exchange (and interoperability) and countering radicalisation.

The authors argue that the EU's present policy is based on two long-standing (mis)conceptions, namely that existing priorities and instruments are effective in preventing, investigating and prosecuting terrorist crimes and that EU principles and fundamental rights act as obstacles to efficient law enforcement. They examine these two conceptions and call for them to be reconsidered in light of existing research and evidence, explaining how they have led to what may be called the "EU liberal paradox". This paradox relates not only to the deleterious impact that counter-terrorism policies have on the EU and national constitutional principles, which terrorism seeks to destroy, but also the questionable extent to which the objectives pursued in EU security policies and tools are efficiently met in their implementation and practical uses.

If EU policies aimed at tackling terrorism are not properly informed and tested, and their societal impacts and ethical implications rigorously assessed, the result will be a lack of mutual confidence between EU and state law enforcement authorities and judicial practitioners, as well as social mistrust on the part of citizens and communities. The conclusions outline a set of recommendations for the next phases of the European Agenda on Security aimed at implementing a principled and trust-based EU approach in countering terrorism.

Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs section at CEPS He is Visiting Professor at the Paris School of International Affairs (PSIA) at Sciences Po (France), Associate Professor/Senior Research Fellow at the Faculty of Law in Maastricht University (The Netherlands), and Honorary Industry Professor/Senior Research Fellow at the School of Law in Queen Mary University of London (UK). Elspeth Guild is Associate Senior Research Fellow at CEPS and Jean Monnet Professor ad personam at Queen Mary, University of London as well as at the Radboud University Nijmegen. Valsamis Mitsilegas is Head of the Department of Law and Professor of European Criminal Law at Queen Mary, University of London. This paper was prepared in the context of the SOURCE Network of Excellence, which is financed by the EU FP7 programme with the aim of creating a robust and sustainable virtual centre of excellence capable of exploring and advancing societal issues in security research and development.

CEPS Policy Insights offer analyses of a wide range of key policy questions facing Europe. As an institution, CEPS takes no position on questions of European policy. Unless otherwise indicated, the views expressed are attributable only to the authors and not to any institution with which they are associated.

978-94-6138- 635-9
Available for free downloading from the CEPS website (www.ceps.eu) © CEPS 2017

CEPS ▪ Place du Congrès 1 ▪ B-1000 Brussels ▪ Tel: (32.2) 229.39.11 ▪ www.ceps.eu

Contents

1. Introduction 1

2. First assumption: Re-appraising effectiveness 2

2.1 Countering radicalisation 3

2.2 Information exchange and interoperability 5

3. Second assumption: Reappraising efficiency 8

4. Ways forward and recommendations 10

References 14

Reflections on the Terrorist Attacks in Barcelona

Constructing a principled and trust-based EU approach to countering terrorism

Sergio Carrera, Elspeth Guild and Valsamis Mitsilegas

CEPS Policy Insight No. 2017-32/August 2017

1. Introduction

On August 18th, Barcelona and the town of Cambrils in Tarragona (Catalonia, Spain) joined the ranks of many other communities across Europe to have been the victim of a terrorist attack. And the perpetrators of this latest attack employed the particularly terrifying technique of weaponing a vehicle and ploughing into pedestrians gathered in city centres, whose deadly effects have already been witnessed in Nice, Stockholm, Berlin and London. While the authorities continue their investigations into the attacks in Catalonia, we take this occasion to reflect on what lessons might be extracted from such horrific events with a view to constructing a more principled and trust-based EU approach to countering terrorism.

The European Union is often put under a spotlight after such acts of violence are committed. EU institutions and agencies are called upon by Member States (or feel the need) to show 'value' in responding to these events. The EU indeed has dynamically acquired experience in counter-terrorism policy and has adopted a great deal of counter-terrorism legislation over the last two decades. The entry into force of the Lisbon Treaty in 2009 further consolidated and expanded the EU's competence in this field.

In July, the European Commission published the 9th Security Union Progress Report,[1] which provides a 'state of play' on the implementation of EU policy, accompanied by a "Comprehensive Assessment of EU Security Policy". The latter highlights continued challenges and gaps in EU policies aimed at tackling terrorism. The next steps in EU counter-terrorism policies, however, call for more cautious, detailed and rational consideration.

In our view, the question of "*what more could the EU do in security policies?*" stems from two main assumptions, both of which are questionable and in need reappraisal.

A first assumption is that existing EU counter-terrorism initiatives – particularly policies focused on more information-sharing and those covering countering radicalisation – are effective in achieving their intended objectives, i.e. to prevent, properly investigate and successfully prosecute crimes related to terrorism. A second assumption is that EU principles – democracy, rule of law and fundamental rights – act as an obstacle to efficient counter-terrorism policies.

[1] European Commission, "The EU is driving work to share information, combat terrorism financing and protect Europeans online", Press Release IP 17/2106, Brussels, 27 July 2017.

The Policy Insight examines these assumptions and argues that they call not only for reconsideration, but also for informed EU decision-making. The assumption regarding the effectiveness of existing instruments and their main EU priorities should be regularly monitored and evaluated in light of the EU Better Regulation Guidelines,[2] and state-of-the-art research in the social sciences and humanities.

The second assumption poses equally profound risks. While acts of terrorism generally aim to undermine liberal democratic principles to which the EU and its Member States have long subscribed, some EU and Member State policies designed to counter terrorism paradoxically pose a challenge to these very same constitutional principles.

We argue that both assumptions, working either independently or in combination, lead to what may be called "*the EU liberal paradox"* in countering terrorism policies. This paradox manifests itself in a widening lack of mutual confidence between EU and state law enforcement authorities and judicial actors, but also in social mistrust on the part of citizens and communities at large who may see their rights, liberties and inclusion jeopardised. This same mistrust could have negative repercussions for the legitimacy of security policies and ultimately for the value added of 'more EU' in countering terrorism.

So, *where should the EU concentrate its efforts in developing effective counter-terrorism policies?* This paper argues that the best way to deal with the EU liberal paradox would be for the Union to construct and progressively develop a *principled and trust-based EU policy approach in countering terrorism*. In the conclusions, we outline specific ways forward for implementing this approach and advance a set of recommendations for the next phases of EU counter-terrorism policies.

2. First assumption: Re-appraising effectiveness

EU-level discussions in the aftermath of deadly terrorist attacks tend to start from the premise that existing public policies and their guiding priorities meet the *effectiveness test*; i.e. that they are well suited to achieve the objectives and goals pursued, chiefly the prevention, investigation and prosecution of terrorist crimes.[3]

The Security Union Task Force[4] of the European Commission recently delivered the above-cited "Comprehensive Assessment of the Union's Action in the Area of Internal Security".[5] The

[2] See the European Commission's webpage on "Better Regulation: Why and How". See also European Commission, "Better Regulation Guidelines", Staff Working Document, SWD(2015) 111 final, Strasbourg, 19 May 2015.

[3] F. de Londras (2015), "Governance Gaps in EU counter-terrorism: implications for democracy and constitutionalism", in F. de Londras and J. Doody (eds), *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism*, Routledge.

[4] European Commission, "President Juncker consults the European Parliament on Sir Julian King as Commissioner for the Security Union", Press Release IP 16/2707, 2 August 2016, Brussels.

[5] European Commission, Staff Working Document, "Comprehensive Assessment of EU Security Policy", Parts 1 and 2, SWD(2017) 278 final, Brussels, 26.7.2017.

exercise is a welcome step forward in the Commission's work for highlighting the value of several EU security policy developments and underlining a few caveats and shortcomings, which among others include obstacles in Member States' implementation.

The Commission's assessment falls short in providing an in-depth evaluation and/or 'Fitness Check' – in line with the Better Regulation Guidelines – of existing Union security policies, instruments and agencies. Such an evaluation, however, would be important before moving forward with the adoption of new initiatives building on the same assumptions.

EU security policy priorities have not always been based on an accurate understanding and diagnosis of the actual issues or phenomena that are intended to be addressed and their societal effects. Among the set of priorities underlying the so-called European Agenda on Security of April 2015,[6] which purports to drive the European Commission's work in this domain, has reaffirmed past EU policy priorities by giving priority to first, countering radicalisation (section 2.1 below) and secondly, information exchange and interoperability (section 2.2).

2.1 Countering radicalisation

Identifying, detecting and addressing the underlying factors and causes leading individuals to commit extreme forms of violence constitutes one of the key items in EU counter-terrorism policies. The European Agenda on Security underlined that the EU should address the root causes of extremism through preventive counter-radicalisation measures.

The events in Barcelona demonstrate that more policy efforts and academic research are needed to better understand why youth engage in extremism and the actual circumstances leading them to commit violence and deadly killings.

The concept of 'radicalisation' hides extremely complex and dynamic phenomena. An 'easy policy fix' simply does not exist. As the European Parliament (EP) Resolution *on the prevention of radicalisation and recruitment of European citizens by terrorist organisations* of November 2015 rightly acknowledged, radicalisation calls for a careful examination of the various global, sociological and political factors, and needs to be understood on a case-by-case basis, against the background and interactions of the individuals concerned.

The same EP Resolution acknowledged that the widespread practise of stereotyping religions across in the EU is leading to racism, xenophobia and intolerance. It underlined how "one of the arguments used by violent extremists in recruiting young people is that Islamophobia is increasing, following years of war on terror, and that Europe is no longer a place where Muslims are welcome or can live in equality and practice their faith without discrimination and

[6] European Commission, The European Agenda on Security, Communication, COM(2015) 185 final, Strasbourg, 28 April 2015.

stigmatization". These are all factors deserving careful consideration in the design and implementation of public policies addressing terrorism in the EU.

Furthermore, while much attention has recently been paid at EU levels to the so-called foreign fighters or Europeans traveling to Syria or Iraq,[7] the picture emerging from the attacks in Catalonia is far more complex. There is clearly not a single path that draws people to violence. From the available information at the time of writing, it appears that none of the individuals directly involved in the attacks corresponds to the 'foreign fighter' profile.

Counter-radicalisation policies in the EU have so far included 'hard' counter-terrorism responses, such as the adoption of new laws in various Member States allowing for pre-emptive judicial powers, deprivation of nationality and stop and search activities.[8] They have also included so-called 'softer measures' focused on supporting the involvement of local service providers in sectors such as health and education in preventing terrorism. While softer in nature, these initiatives have been shown to have important societal implications and often negative repercussions that are counter-productive in meeting their intended goals.

Previous studies[9] have demonstrated that counter-radicalisation policies call for a large degree of caution, particularly regarding their adequacy in diagnosing the phenomenon and the actual repercussions and wider societal impacts in communities concerned. If not carefully designed and implemented, counter-radicalisation actions involving a broad range of social actors – e.g. social workers, schoolteachers and health professionals – may in fact be detrimental to their objectives.

Counter-radicalisation initiatives and projects might in fact indirectly become sources of radicalisation, instead of helping to prevent or address it. The so-called Prevent I and II Strategy,[10] developed by the UK, is based on "a strong preventive component grounded on partnerships and community policing". Under this strategy, doctors and teachers were assigned the duty to assess and report individuals being at risk of extremism.

Research has revealed important shortcomings in the Prevent Strategy, however, which should be taken as 'lessons learned' in EU policy debates and agendas. A report published by the Open

[7] As detailed on the European Council webpage on "Response to foreign terrorist fighters and recent terrorist attacks in Europe", European Council. See also "Outline of the counter-terrorism strategy for Syria and Iraq, with particular focus on foreign fighters", 5369/15, Brussels, 16 January 2015; and Council of the EU, "The challenge of foreign fighters and the EU's response", FACTSHEET, Brussels, 9 October 2014.

[8] D. Bigo, L. Bonelli, E.P. Guittet and F. Ragazzi (2014), "Preventing and Countering Youth Radicalisation in the EU", Study for the European Parliament, DG IPOL, Brussels; V. Mitsilegas (2016), *EU Criminal Law after Lisbon*, Hart Studies in Criminal Law, Oxford: Hart Publishing.

[9] Ibid.

[10] UK Home Department, Prevent Strategy, Cm 8092, June 2011; see also "Prevent strategy to be ramped up despite 'big brother' concerns", *The Guardian*, 11 November 2016. For more information, see https://www.theguardian.com/uk-news/prevent-strategy .

Society Justice Initiative[11] characterised the strategy as "badly flawed" and having the effect of eroding trust.[12] It has been criticised for leading Muslim communities and young British Muslims to question their place in society, and for its use of an indicators-based method lacking any scientific rigor.

The Strategy, and its inherent approach, has been said to create the potential for discrimination and xenophobia, and the spread of a "feeling of suspicion" and mistrust within various communities. It also has the consequence of denigrating the value of diversity and pluralism in political debates.[13]

The concerns raised by the practitioners and communities most affected by the UK Prevent Strategy were echoed by the UK House of Commons (Home Affairs Committee), which advised the Government to "abandon the now toxic name 'Prevent' for the strategy and to rename it with the more inclusive title of 'Engage'" and to encourage a wider participation in the discussion by all communities involved.[14]

2.2 Information exchange and interoperability

A long-standing priority in EU counter-terrorism policies, which has now been re-codified in the EU Agenda on Security, has been more exchange of information between national law enforcement authorities, and the full use of existing databases or information systems. 'Big data' practices and electronic communications held by IT companies are increasingly 'in demand' in pre-emptive counter terrorism policies.[15]

This priority was confirmed in a report[16] published in May 2017 and prepared by a High Level Expert Group on Information Systems and Interoperability set up by the European Commission,

[11] Open Society Justice Initiative (2016), "Eroding Trust: The UK's PREVENT Counter-Extremism Strategy in Health and Education", New York, NY.

[12] "UK's Prevent counter-radicalisation policy 'badly flawed'", *The Guardian*, 16 October 2016.

[13] F. Ragazzi (2016), "Suspect community or suspect category? The impact of counter-terrorism as 'policed multiculturalism'", *Journal of Ethnic and Migration Studies*, Vol. 42, No. 5, pp. 724-741.

[14] UK House of Commons (Home Affairs Committee), "Radicalisation: the counter-narrative and identifying the tipping point", Eighth Report of Session 2016–17, HC 135, 25 August 2016, pp. 36-37. The report concluded: "Allaying these concerns and building trust will require full and wide engagement with all sections of the Muslim community, including at grassroots level—and not just with groups which already agree with the Government. The focus of the strategy should be around building a real partnership between community groups and the state. The concerns of parents about the lure of radicalisation, and their desire for support and advice, should be heeded. If stakeholders buy into such a strategy it can be successful, but unfortunately that is not what is currently happening", p. 19.

[15] S. Carrera, G. González Fuster, E. Guild and V. Mitsilegas (2015), "Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights", CEPS Report, Brussels. See also D. Lyon (2017), "Big Data Surveillance: Snowden, Everyday Practices and Digital Futures", in T. Basaran, D. Bigo, E. P. Guittet and R.B.J. Walker (eds), *International Political Sociology: Transversal Lines*, Routledge Studies in International Political Sociology, pp. 254-285.

[16] Report of the High Level Expert Group on Information Systems and Interoperability, May 2017 (http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1).

but whose actual membership has not been publicly disclosed.[17] The report calls for more 'interoperability' of existing EU information systems and the setting up of a 'European search portal' to all EU databases.

Access and sharing of relevant 'information' has been traditionally considered as a central tool for effective law enforcement cooperation in cross-border criminality. Over the last two decades, the EU has developed a plethora of information systems and databases.[18] These include such databases as the Schengen Information System (SIS II), the Prüm Framework[19] or the EU Passenger Name Record (EU PNR).[20]

While information-sharing may be seen to play a key role in effective crime-fighting, the increasing reliance on and calls for larger-scale and 'interoperability' of existing electronic information databases might not always the most effective way of countering terrorism. Large volumes of predictive information and 'intelligence' are not always effective for law enforcement practitioners in preventing these acts or bringing criminal suspects to justice.

In previous terrorist attacks in other European cities, some of the perpetrators were already known to law enforcement and intelligence authorities.[21] A majority of the individuals directly involved in the attacks in Catalonia had no previous criminal record. The Imam considered to be the leader of the attackers in Barcelona, Abdelbaki es Satty, had been convicted in Spain for a crime with no links to terrorism - drug trafficking - in 2010 and served a four-year prison term. He later travelled to Belgium and applied for a job there, but when the Imam of the Belgian municipality of Vilvoorde asked him whether he had a criminal record, he left the country. [22] It has been reported that a Belgian policeman had informally requested information in 2016 about Abdelbaki es Satty from a colleague in the Catalan police force, but apparently no relevant information about the suspect and his criminal record was found.

Recent media reports have highlighted that the Catalan police (*Mossos d'Esquadra*) had been asking for some time for full access to the police databases at national and EU levels, including

[17] See http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435

[18] S. Carrera, D. Bigo, B. Hayes, N. Hernanz and J. Jeandesboz (2012), "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals", Study for the European Parliament, DG IPOL, Brussels.

[19] 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.

[20] Directive 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016,

[21] This was for instance the case in respect of the attackers involved in the Paris terrorist attacks of November 2015. See "Revealed: How French secret services 'lost track' of one of the Bataclan bombers", Mediapart, 22 November 2015.

[22] El Mundo, "El Imam de Ripoll tenía una orden de expulsión que nunca se ejecutó", 22 August 2017. According to this same newspaper, the Imam was issued an expulsion order to leave the country, based on his previous drug trafficking. The order was not executed, however, following an appeal before a Court which granted him legal status to reside in Spain.

Europol information system.[23] The access and use of current EU databases by multi-level law enforcement authorities, particularly in Member States where law enforcement competences are de-centralised such as Spain, could indeed be more carefully evaluated and improved.

That notwithstanding, while policies calling for 'more information' may aim at helping to restore public confidence, they can also create a false expectation that the authorities have access to extensive data about possible dangerous persons. Such individuals cannot be monitored all the time and sometimes attacks are not prevented. Research has highlighted that more data without the necessary human and analytical resources has little value.[24] Large quantities of electronic information registered on potential suspects and data mining ('connecting the dots') have been described as "unreliable". They may decrease the probability of finding 'the right file' and increase false (positive and negative) alarms.[25]

Calls for 'big data' in law enforcement raise the question of the actual 'nature and quality' of that information, and the extent to which it will be admissible evidence in criminal proceedings before a tribunal. Criminal justice and police investigations require data that are considered 'admissible' by an independent judge.[26] In contrast, data qualified as 'intelligence' include any kind of information irrespective of its reliability, origins and quality, or compliance with admissibility and jurisdictional rules. As argued previously,[27] 'more' is not always 'more' in terms of effective counter-terrorism policies.

Not all EU institutions and Member States in fact agree on exactly what interoperability means or how widely the net should be cast. The concept entails a widening of the group of actors with access to rights to information systems and sometimes generates mistrust among the practitioners themselves. Experience has shown that trust works best among a limited number of actors with clearly defined roles and similar objectives.

Ownership of data seems to be an issue of critical importance in creating confidence in EU information systems. For instance, Europol maintains its own database, called the Europol

[23] El País, *Los Mossos lidian con la gran prueba del ISIS*, 21 August 2017; and El País*, "Cuanta más información puedas compartir sobre él, ¡mejor!",* 24 August 2017.

[24] D. Bigo, S. Carrera, E. Guild, E. P. Guittet, J. Jeandesboz, V. Mitsilegas, F. Ragazzi and A. Scherrer (2015), "The EU and its Counter-Terrorism Policies after the Paris Attacks", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels.

[25] "A false positive is when the system identifies a terrorist plot that really isn't one. A false negative is when the system misses an actual terrorist plot. Depending on how you 'tune' your detection algorithms, you can err on one side or the other", quoted from B. Schneider (2006), "Data Mining of Terrorists", blog. See also A. Scherrer and D. Bigo (2015), "Will the democratic debate over counter-terrorism gain the edge in battle?", openDemocracy, 11 February 2015; J. Vijayan (2010), "New York bomb plot shows limits of data mining", *Computer World*.

[26] D. Bigo, S. Carrera, N. Hernanz and A. Scherrer (2014), "The Use of Intelligence Information, the National Security or State Secrets Rule and Secret Evidence in National Legislation and Its Interpretation by Courts", study for the European Parliament, DG IPOL, Brussels.

[27] Bigo, D., S. Carrera, E. Guild and V. Mitsilegas (2016), "The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more information sharing", CEPS Commentary, CEPS, Brussels.

Information System (EIS).[28] Member State police authorities may feed it relevant information in fighting terrorism, but the Member State in question retains 'ownership' and has the right to restrict access – on a case-by-case basis – to only a few Member State counterparts.

The wider the interoperability and the circle of actors with access to databases, the more reluctant some actors may become to input sensitive information into a particular information system. The priority given to ever-wider access to databases may in turn have a deleterious effect on the quality of the data that actors are willing to share with other actors.

Widening access to sensitive information beyond the actors with specific and clearly defined expertise and powers can be detrimental to effective cooperation. Counter-terrorism magistrates may be able to share information without too much difficulty across borders. But if they know that the data that they share with their counterparts in another Member State may also become available to other actors - such as border and coast guards, police, etc. - this may no longer be the case.

3. Second assumption: Reappraising efficiency

The second assumption in EU counter-terrorism policies is that EU principles – democracy, rule of law and fundamental rights - act as an obstacle to effective counter-terrorism and law enforcement security policies. The compatibility between these policies and principles – specifically during the implementation of these policies- is often taken for granted. This is the case despite the fact the EU Better Regulation Guidelines identify societal and ethical costs – including fundamental rights impacts – as central components in *the efficiency test* in evaluating EU policies.

While the compliance of EU counter-terrorism policies with fundamental rights and rule-of-law is openly declared – in a rather formalistic fashion[29] – in all relevant official documents, the impacts of the prevailing policy priorities on these principles and wider societal and fundamental rights, such as those addressed in sections 2.1 and 2.2, are by and large not properly examined or addressed. As the Human Rights Commissioner of the Council of Europe has emphasised: "laws and policies that are human rights compliant preserve the values the terrorists are trying to destroy, weaken the pull of radicalisation, and strengthen the public's confidence in the rule of law and democratic institutions."[30]

EU principles relate to safeguarding privacy and data protection enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (EU Charter) when countering terrorism – which are

[28] For more information about the EIS, see https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

[29] See for instance the Commission Communication delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, COM(2016) 230 final, 20.4.2016, Brussels.

[30] Commissioner for Human Rights, "National human rights structures: protecting human rights while countering terrorism", Human Rights Comment, 6 December 2016, Council of Europe: Strasbourg.

of central salience in the EU data protection legal system. A key component of EU data protection law is the principle of purpose limitation of data gathered, accessed and exchanged.[31]

The European Commission's Seventh Progress Report towards an Effective and Genuine Security Union of 16 May 2017[32] has rightly underlined that a key challenge in moving forward in discussions related to the interoperability of EU information systems is to devise "the necessary strict rules on access and use without affecting the existing purpose limitation". It is indeed essential to ensure that information systems respect their specific data protection provisions and rules on access for competent authorities, separate purpose limitation rules for each category of data and dedicated data retention norms.

The Court of Justice of the European Union (CJEU) has played a key role in upholding EU rule of law principles in counter-terrorism policies. The CJEU has for instance clarified in landmark rulings such as *Digital Rights Ireland* or *Schrems* that generalised, large-scale and unlimited surveillance is contrary to EU privacy and data protection rights, and constitutes disproportionate responses in democratic societies.[33] The Luxembourg Court has equally underlined the need to show for any data access and sharing a link with specific, reasonable and individualised suspicion.

In its recent Opinion on the EU-Canada Passenger Name Record (PNR),[34] the CJEU struck down the validity of the EU-Canada Agreement because of its incompatibility with the EU Charter and EU data protection law. In this same Opinion, the Court has also laid down a set of 'benchmarks' for assessing the legality of current and future security measures, particularly the transfer of passengers' data in the scope of international agreements.

[31] See Article 5.1 of the General Data Protection Directive 2016/679 of 27 April 2016 which states: "personal data shall be (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')". See also paragraph 26 of Preamble and Article 4.2.a of the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, of 27 April 2016, OJ L 119/89.

On the purpose limitation principle, see E. Brouwer (2011), "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation" in L.F.M. Besselink, F. Pennings and S. Prechal (eds), *The Eclipse of the Legality Principle in the European Union,* Kluwer.

[32] European Commission, Seventh Progress Report towards an Effective and Genuine Security Union, COM(2017) 261 final, Strasbourg, 16 May 2017.

[33] See V. Mitsilegas (2017), "Surveillance and Digital Privacy in the Transatlantic 'War on Terror'. The Case for a Global Privacy Regime", Legal Studies Research Paper No. 251/2017, Queen Mary University of London; and S. Carrera and E. Guild (2015), "Safe Harbour or into the storm? EU-US data transfers after the Schrems judgment", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels.

[34] Court of Justice of the EU, Opinion 1/15, 26 July 2017.

These EU legal standards include, among others, the provision of sufficient guarantees of the integrity of individuals' personal data and their ability to seek effective remedies against the risk of abuse in third countries. They also require that access to and processing of electronic data are necessary (proportionate) and non-discriminatory and that clear and precise rules specify the conditions justifying the interference with privacy, subject to a review carried out either by a court or an independent administrative body.

The challenges posed by current EU counter-terrorism policies to fundamental rights are not confined to privacy, however. These policies may violate the right to a legal defence and fair trial guarantees for suspects in criminal investigations and proceedings, including the presumption of innocence as well as the principle of legality of criminal offences and sanctions enshrined in Articles 47-50 EU Charter. In addition, fundamental rights compliance is a central component of the right to good administration, envisaged in Article 41 EU Charter. In short, more attention needs to be paid to the impact on fundamental rights resulting from EU counter-terrorism policies, agencies and information tools.

4. Ways forward and recommendations

The next phases of EU policies on counter-terrorism should give priority to reinforcing EU principles and social trust in coordinated actions and common policies. Testing the effectiveness and efficiency of EU counter-terrorism policies must go hand-in-hand with a detailed and self-critical assessment of the extent to which current instruments and priorities are fit for purpose. These efforts should pay careful attention to the relationship between existing EU legal and policy instruments and agencies and EU and national rule of law principles, as well as their impacts on society and fundamental rights.

As a first step, the EU should conduct a formal evaluation or 'Fitness Check' on counter-terrorism policies and actors, which would include main contributions (added value), shortcomings and gaps in the current state of play following the EU Better Regulation Guidelines. The focus should be on effectiveness and efficiency of all existing legal instruments and international agreements, information-sharing databases and tools, projects and funding schemes and the work of all relevant EU Justice and Home Affairs agencies. Special attention should be paid to the existence, performance and (follow-up to) outputs of independent oversight venues and bodies and inquiries at domestic and EU levels.[35] The adequacy and 'fitness' of the existing framework should be fully analysed before embarking on or adopting any new policy instrument or database.[36]

A central challenge for EU policies is to arrive at an updated, accurate and inter-disciplinary diagnosis of the actual challenges and dynamic dilemmas posed by current instruments, tools

[35] Commissioner for Human Rights, "Democratic and Effective Oversight of National Security Services", Issue Paper, Council of Europe, Strasbourg.

[36] S. Alegre, J. Jeandesboz and N. Vavoula (2017), "European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection", European Parliament Study, DG IPOL, Brussels.

and actors. Similarly, in testing the effectiveness and efficiency of existing EU laws, special attention should be paid to the phases of implementation, operationalisation and use by domestic and EU authorities.

EU counter-terrorism policies would benefit from being regularly informed by in-depth and evidence-based analysis, drawing on the Social Sciences and Humanities (SSH) research to better understand the contexts in which various manifestations of violence, extremism and terrorism are embedded. Some initiatives, such as the Radicalisation Awareness Network (RAN) Centre of Excellence, evidence valuable potential, but the setting up of a permanent observatory of inter-disciplinary scholars specialised in countering terrorism, independent from the European Commission, could be central in ensuring well-informed EU policies.

The EU can bring value added by especially investing more action in furthering EU coordination of traditional policing and criminal justice cooperation in fighting terrorism. The widening of information through the interoperability of data systems will not make the investigation and prosecution of crimes any easier. More attention should be paid to ensuring that information and electronic data meet the standards of 'evidence' in criminal justice procedures, and to sharpening the analytical capacities of law enforcement actors, so that terrorist crimes can be effectively prosecuted before the relevant tribunals.

Priority should be also be given to improving the use and added value of existing EU databases in relation to controlling the acquisition and possession of firearms, explosives and other weapons, and the national implementation of existing EU rules and tools – specifying who has access to what, under which conditions and for which purposes and uses. Particular attention should be given to the accessibility to these EU databases in Member States with decentralised or regional police and law enforcement forces.

Further development of the existing Joint Investigation Teams (JITs) model coordinated by EU Agencies – Europol and Eurojust – for cross-border operational cooperation should be given a clearer priority. JITs consist of judges, prosecutors and law enforcement authorities, established for a fixed period and the purpose of conducting criminal investigations in one or several Member States. True, JITs are affected by a number of shortcomings – both at legal and procedural levels - which should be addressed. Eurojust should sit in the driver's seat in the operationalisation of the JITs model, and there should be more clarity regarding the role attributed to Europol in its new Regulation on the financing (awarding of grants) of JITs[37] so that any new joint investigation initiatives would fully meet EU legal standards covering prosecutorial investigations. It is essential for these shortcomings to be addressed, as JITs

[37] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, Article 61.

present an enormous opportunity to develop a *professional EU culture of cooperation* in countering terrorism and crime.[38]

To ensure the effectiveness and efficiency of EU counter-terrorism policies, particular attention should be paid to the compatibility between all existing instruments and agencies and the setting of EU benchmarks that have been developed since the entry into force of the Lisbon Treaty in 2009.[39] Post-Lisbon Treaty legal instruments and CJEU jurisprudence now provide a set of common EU standards that must be guaranteed in European and Member State actions against terrorism, including international cooperation.

A central outstanding issue that should be given additional priority is the national and EU democratic accountability and independent judicial control of activities carried out by EU agencies like Europol, Eurojust and eu-LISA. EU networks of independent national judges – such as the one enshrined in the European Judicial Network (EJN) – could play a more active role in monitoring the impact of these agencies' activities, and their use and management of accompanying databases, and other EU counter-terrorism legislative and policy instruments in light of criminal justice standards and the rights of the defence.

EU agencies, JITs, information systems and tools need to more closely adhere to EU and national rule of law and common legal standards on criminal investigations. A case in point are the benchmarks included in the European Investigation Order (EIO).[40] More research is needed regarding 'promising practices' in the application of the EIO and EU Mutual Legal Assistance Treaties (MLATs) for the use of digital data held by IT companies as evidence in criminal investigations and procedures.

On the phenomenon of radicalisation, the actual added value of the EU should be carefully re-examined. The suitability of this concept to fully capture the current dynamics of violence should be scrutinised. More in-depth studies on the causes and manifestations of youth violence and crime across the EU should be conducted. It is also crucial to carry out a detailed assessment of 'what has worked' and 'what has not worked' regarding past and ongoing policies and (EU-funded) projects dealing with countering radicalisation, including tackling cybercrime or radicalisation online.[41] Addressing illegal activities and content in the internet should respect existing criminal justice frameworks and constitutional guarantees.

[38] S. Carrera, E. Guild, L. Vosyliūtė, A. Scherrer and V. Mitsilegas (2016), "The Cost of Non Europe in the Area of Organised Crime", Study for the European Parliament, DG EPRS, Brussels.

[39] S. Carrera and E. Guild (2015), "Implementing the Lisbon Treaty: Improving the Functioning of the EU on Justice and Home Affairs", Study for the European Parliament, DG IPOL, Brussels.

[40] European Commission, "As of today the "European Investigation Order" will help authorities to fight crime and terrorism", Press Release, 22 May 2017.

[41] European Commission, Security Union: Commission accelerates measures to prevent radicalisation and the cyber threat, Press Release IP/17/1789, 29 June 2017. This should also apply to the work of Europol's European Counter Terrorism Centre (ECTC) and its EU Internet Referral Unit (IRU). For more information, see https://www.europol.europa.eu/newsroom/news/information-sharing-counter-terrorism-in-eu-has-reached-all-time-high.

The Commission 9th Progress Report on the Security Union has expressly acknowledged that "the importance of involving local practitioners, academics and researchers in efforts to prevent violent radicalisation in communities."[42] The EU presents a unique value added in bringing together various actors and networks from outside the public sector. Yet, while the involvement and cooperation of local communities may be a necessary component, these kinds of 'soft' public policies approaches should be designed and implemented with great care so as not to lead to further alienation and exclusion of relevant communities.

Such policies should be accompanied by the setting up of *firewalls* between the work of social service workers and professionals, including school staff and civil society actors, and law enforcement. These social actors play a key function in creating and fostering social trust. They should not be asked to act as intermediaries of law enforcement, or as 'watchdogs' in countering terrorism, which in turn would undermine their trust-building role. The recent events in Catalonia have been followed by violence against Muslims and destruction of mosques.[43] More EU policy attention needs to be paid to countering discrimination and Islamophobia and effectively addressing hate crimes and hate speech online against Muslims and Islam.[44]

Any future European cooperation in counterterrorism must also fully take place within the remits of EU rule of law and constitutional scrutiny. As a central actor in EU security policies, the European Parliament must be centrally engaged in EU counter-terrorism policymaking. The European Parliament is about to launch a new Special Committee on Terrorism,[45] which is a welcome initiative that was called for in a previous CEPS publication.[46] The Committee presents great potential in ensuring the much-needed democratic accountability of EU security policies and their implementation.

If the next generation of the EU security agenda is to be based on firm and solid foundations, the EU liberal paradox examined in this Policy Insight needs to be addressed through a *principled and trust-based policy approach*. Such an approach should evaluate and re-appraise current EU policy notions of effectiveness and efficiency in countering terrorism policies, instruments and actors, and bring EU and domestic constitutional principles and 'better regulation' rules and social trust-building measures into the heart of EU action.

[42] European Commission, Ninth progress report towards an effective and genuine Security Union, COM(2017) 407 final, Brussels, 26.7.2017.

[43] El País, "La islamofobia se desata en las redes y llega a la calle tras los atentados", 23 August 2017.

[44] Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328/55. For more information on EU policy and related initiatives in this area, see the Commission's webpage on Racism and Xenophobia

[46] D. Bigo, S. Carrera, E. Guild and V. Mitsilegas (2016), "The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more information sharing", CEPS Commentary, CEPS, Brussels.

As demonstrated in this Policy Insight, the EU liberal paradox in countering terrorism policies is not only about the impact of security policies on fundamental rights. If the effectiveness and efficiency of EU policies aimed at tackling terrorism are not properly grounded and their societal and ethical impacts regularly assessed, we will not only be abandoning EU principles, but we will also not get any security in return.

References

Alegre, S., J. Jeandesboz and N. Vavoula (2017), "European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection", European Parliament Study, DG IPOL, Brussels.

Bigo, D., L. Bonelli, E.P. Guittet and F. Ragazzi (2014), "Preventing and Countering Youth Radicalisation in the EU", Study for the European Parliament, DG IPOL, Brussels.

Bigo, D., S. Carrera, E. Guild and V. Mitsilegas (2016), "The EU and the 2016 Terrorist Attacks in Brussels: Better instead of more information sharing", CEPS Commentary, Brussels.

Bigo, D., S. Carrera, E. Guild, E. P. Guittet, J. Jeandesboz, V. Mitsilegas, F. Ragazzi and A. Scherrer (2015), "The EU and its Counter-Terrorism Policies after the Paris Attacks", CEPS Paper in Liberty and Security in Europe, CEPS, Brussels.

Bigo, D., S. Carrera, N. Hernanz and A. Scherrer (2014), "The Use of Intelligence Information, the National Security or State Secrets Rule and Secret Evidence in National Legislation and Its Interpretation by Courts", Study for the European Parliament, DG IPOL, Brussels.

Brouwer, E. (2011), "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation" in Leonard F.M. Besselink, Frans Pennings and Sacha Prechal (eds), *The Eclipse of the Legality Principle in the European Union,* Kluwer.

Carrera, S. and E. Guild (2015), "Implementing the Lisbon Treaty: Improving the Functioning of the EU on Justice and Home Affairs", Study for the European Parliament, DG IPOL, Brussels.

Carrera, S. and E. Guild (2015), "Safe Harbour or into the storm? EU-US data transfers after the Schrems judgment, CEPS Paper in Liberty and Security in Europe, CEPS, Brussels.

Carrera, S., E. Guild, L. Vosyliūtė, A. Scherrer and V. Mitsilegas (2016), "The Cost of Non-Europe in the Area of Organised Crime", Study for the European Parliament, DG EPRS, Brussels.

Carrera, S., G. González Fuster, E. Guild and V. Mitsilegas (2015), "Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights", CEPS Report, CEPS, Brussels.

Carrera, S., N. Hernanz and J. Parkin (2013), "The 'Lisbonisation' of the European Parliament: Assessing Progress, Shortcomings and Challenges for Democratic Accountability in the Area of Freedom, Security and Justice", Study for the European Parliament, DG IPOL, Brussels.

Commissioner for Human Rights (2015), "Democratic and Effective Oversight of National Security Services", Issue Paper, Council of Europe, Strasbourg.

de Londras, F. (2015), “Governance Gaps in EU counter-terrorism: implications for democracy and constitutionalism”, in F. de Londras and J. Doody (eds), *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism*, Routledge.

Lyon, D. (2017), Big Data Surveillance: Snowden, Everyday Practices and Digital Futures, in T. Basaran, D. Bigo, E. P. Guittet and R.B.J. Walker (eds), *International Political Sociology: Transversal Lines,* Routledge Studies in International Political Sociology, pp. 254-285.

Mitsilegas, V. (2017), “Surveillance and Digital Privacy in the Transatlantic ‘War on Terror’: The Case for a Global Privacy Regime”, Legal Studies Research Paper No. 251/2017, Queen Mary University of London.

Mitsilegas, V. (2016), *EU Criminal Law after Lisbon*, Hart Studies in Criminal Law, Oxford: Hart Publishing.

Mitsilegas, V., S. Carrera and K. Eisele (2014), “Who Monitors Trust in the European Justice Area? The End of the Transitional Period for the Measures under Police and Judicial Cooperation in Criminal Matters Adopted before the Lisbon Treaty”, Study for the European Parliament, DG IPOL (Internal Policies), Brussels.

Open Society Justice Initiative (2016), “Eroding Trust: The UK’s PREVENT Counter-Extremism Strategy in Health and Education”, New York, NY.

Ragazzi, F. (2016), “Suspect community or suspect category? The impact of counter-terrorism as ‘policed multiculturalism’”, *Journal of Ethnic and Migration Studies*, Vol. 42, No. 5, pp. 724-741.

Scherrer, A. and D. Bigo (2015), “Will the democratic debate over counter-terrorism gain the edge in battle?”, openDemocracy, 11 February.

Schneider, B. (2006), “Data Mining of Terrorists”, Blog (https://www.schneier.com/blog/archives/2006/03/data_mining_for.html).

UK House of Commons (Home Affairs Committee) (2016), Radicalisation: the counter-narrative and identifying the tipping point, Eighth Report of Session 2016–17, HC 135, 25 August 2016, pages 36-37.

Vijayan, J. (2010), “New York bomb plot shows limits of data mining”, (http://www.computerworlduk.com/data/new-york-bomb-plot-shows-limits-of-data-mining-3302/).

ABOUT CEPS

Founded in Brussels in 1983, CEPS is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process
- Provide a regular flow of authoritative publications offering policy analysis and recommendations

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals

Programme Structure

In-house Research Programmes

Economic and Finance
Regulation
Rights
Europe in the World
Energy and Climate Change
Institutions

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)
Energy Climate House (ECH)

Research Networks organised by CEPS

European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)