The terrorist attacks in Paris and Brussels, just as the earlier ones in Madrid and London, were a brutal reminder that central pillars of the EU, such as the ‘area of freedom, security and justice’, are being challenged. Terrorists know no borders. Although political commitments for joint European action have been made over decades, mindsets and willingness to cooperate – crucial ingredients in the fight against terror – have not lived up to the challenge. The enduring lack of coordination between security services, police and judicial authorities, at the national and the European levels, needs to be urgently tackled to reduce Europe’s vulnerability to such risks.*

**Achieving Breakthroughs in Information Sharing**

Fragmentation makes us vulnerable, starting from our understanding of the terrorist threat. This points to the need to realise a European modular, integrated identity management system based on biometry and anchored to common criteria. Such an integrated system will not be achieved overnight, but it requires immediate steps to be taken: the establishment of an ‘interoperable by design’ principle for existing databases, of a legally binding duty to share information, and of a duty to consult the common system for all Member States.

**Boosting Resources for Counter-Terrorism**

The resources and operational capacity of the European Counter Terrorism Centre (ECTC) at Europol must be significantly strengthened. Member States should commit themselves to permanent secondment of counter-terrorism experts in addition to *ad hoc* support on enhanced cross-border investigations. Ensuring compliance in secondment and information sharing requires incentives such as peer review, regular scoreboards and ex-post assessments.

**Creating a Genuine Digital Strategy**

Radicalisation has multiple causes but it thrives on the limitless possibilities offered by modern technology. There is no quicker way to spread hatred than through the Internet or mobile networks. Responding to this challenge is a shared task of governments, businesses and citizens at large. Agreed standards can help identify and take down radical content. Technological autonomy is key: Public-Private Partnerships are needed to identify, report and dismantle the abuse of social and digital platforms for radicalisation, recruitment, and the perpetration of terrorist activities.

**Stepping Up Action to Prevent Radicalisation**

Terrorists are criminals who have to be pursued but equal determination is needed to make sure their message does not spread to new followers. The work of the Radicalisation Awareness Network needs to be stepped up while political dialogue should be launched with the European Muslim community to facilitate its role in the fight against radicalisation. To this end, the Commission can mobilise a wide array of tools in the areas of social affairs and employment, youth and sports, education and culture.

* The UK, Ireland, and Denmark have opted out from legislation adopted in the area of freedom, security and justice. This implies that the key recommendations laid out in this paper may not be applicable to these countries.
The ‘Security Union’ proposed by President Juncker could be based on two key premises. Firstly, as the liberal philosopher Wilhelm von Humboldt famously put it, **without security, there is no freedom**. It follows that freedom and security are two sides of the same coin and we must act jointly to uphold them. The second premise proposes that **cooperation makes us stronger**: whereas national security remains firmly the responsibility of each Member State, threats to our safety and wellbeing are transnational and multifaceted. No Member State, even the biggest or the most powerful, can face them alone.

The new threats that challenge Europe’s security – nationally and at the level of the Union – are ever more complex and dynamic. Terrorist organisations are inherently transnational and operate both on the ground and as a virtual brand. They are organised in networks and sustain themselves through ‘hot swapping’: the ability to swiftly reorganise when a cell or unit is taken down without compromising the operations of the system. Against this backdrop, individual action by single nation states has proven insufficient. Furthermore, old means simply do not work. The threat is intrinsically cross-border in nature and of European scale.

**Figure 1: Top EU Countries of Origin for Foreign Fighters in Syria and Iraq, 2015**

Number of foreign fighters

- **United Kingdom**: 760
- **Spain**: 1700
- **France**: 470
- **Sweden**: 300
- **Denmark**: 125
- **Belgium**: 220
- **Netherlands**: 600
- **Germany**: 87
- **Austria**: 300
- **Italy**: 133
- **United Kingdom**: 760
- **Spain**: 1700
- **France**: 470
- **Sweden**: 300
- **Denmark**: 125
- **Belgium**: 220
- **Netherlands**: 600
- **Germany**: 87
- **Austria**: 300
- **Italy**: 133

*Source: The Soufan Group*

More coordination across all stages of investigations, law enforcement and criminal proceedings will be necessary, but not sufficient, to prevent future threats. Systems and bodies that can act swiftly on merged collective intelligence of services must complement increased cooperation between services responsible for combating terrorism, intelligence services, police forces, and judicial authorities as well as Europol, Eurojust, EU INTCEN and Frontex.

In the medium term, the European Union must be prepared to consolidate a **European multi-level counter-terrorism network** while respecting the competences of the Member States as well as the principle of subsidiarity. Competent authorities of the Member States would make up the bulk of this network. But proper Union-wide action also requires a further development of responsibilities at EU-level. According to Article 4 (2) TEU, national security remains the sole responsibility of each Member State. Notwithstanding, the Treaties comprise competence to safeguard European cross-border dimension of security.

Examining the experience of the United States post-9/11 suggests that strong institutions are needed to overcome the national and organisational silos that have hitherto often prevented efficient coordination. Understanding that ‘turf battles’ between different institutions prevented vital information exchange and contributed to the most horrific terrorist attack to date, the United States undertook a root-and-branch review of its law enforcement and intelligence services, dubbed the 9/11 Commission. Among the key outcomes were the creation of a Department of Homeland Security and the appointment of a cabinet-level post of Secretary of Homeland Security. The Department of Homeland Security unites under its roof many services that were previously managed independently of one another, such as US Customs and Border Protection, the Coast Guard, the Transportation Security Administration, the Citizenship and Immigration Services and the Secret Service. While the situation in Europe is of course not comparable, the **larger lesson of better integrating and coordinating across various policy fields that pertain to security does appear to be necessary** in order to prevent future attacks.
1. Targeted Assessment and Information Sharing

Counter-terrorism must start long before terrorist acts are perpetrated. Its decisive phase for intervention lies in properly identifying and assessing the challenges posed by trans-border terrorist networks. The interoperability of EU databases is the foundation of anticipation and preparedness in this context: border and law enforcement authorities must have appropriate access to all existing databases in order to monitor, track and tackle threats that move fluidly across physical and virtual borders.

Duty to Inform

Technical interoperability is insufficient without proactive willingness to share information that is operationable. **As digital technologies blur physical borders, counter-terrorism can no longer rest on the restrictive ‘need to know’ principle cherished by traditional intelligence; it must be rooted in a new culture of sharing – widely, timely and proactively.**

Persistent and painful failures have occurred in the past when it comes to feeding EU databases and exchanging information about foreign fighters and terrorists across the Union.

As regards information sharing, following Council decision 2005/671/JHA, Member States have in principle a duty to inform/share with Europol/European Counter Terrorism Centre. The scope of effectiveness of this decision should be reviewed to ensure the mandatory exchange of information regarding foreign fighters and other essential elements pertaining to terrorist threats. Ensuring compliance from Member States in secondment and information sharing would benefit from effective incentives such as peer reviews and regular scoreboards. Moreover, joint ex post assessments could provide the ground for constant learning and the creation of European best practices.

Towards Full Interoperability of Databases Based on Common Criteria

The European Agenda on Security and the Commission Communication on Stronger and Smarter Information Systems for Borders and Security of 6 April have launched a discussion on the future framework for more resilient information systems for border management and internal security, whilst ensuring that individuals’ data is safe. It is now time for delivery: interoperability and seamless exchange of information must be made operational urgently.

Against this backdrop, data is a key means for successful counter-terrorism, which requires common situational awareness and shared infrastructures. But data is today fragmented across a number of EU databases such as SIS II, Eurodac, VIS, EIS, Focal Point Traveller, to which some key agencies are currently even precluded access. This demands the setting up of a single, user-friendly interface permitting single search as well as the ability to perform batch comparisons across databases, which is not possible under the current framework. This will notably imply a review of SIS II and Eurodac regulations, to generalise search functions for biometrics/fingerprints and to allow batch comparisons for law enforcement purposes.
A Single European Identity Management System

Full interoperability should ultimately result in a Single European Identity Management System. This will require a two-step approach. In the short-run, the EU should prioritise ensuring interoperability of EU databases, based on shared criteria. This will pave the way for developing a single, modular, integrated identity management system for travel, migration, and security, based on biometric markers. Some Member States, such as Estonia, have successfully experimented with the integration of their databases. The setting up of a Single European Identity Management System would avoid the multiple collection, registration, and storage of personal data, and significantly enhance the performance of the system. Intelligent, proportionate, and carefully regulated access will remain a priority to ensure that individual data is safe and that there is no infringement of the right to privacy.

2. Bolstering Capacity to Respond

Providing for European security in an environment of multiple and shared risks requires a capacity to pursue and eliminate as many sources of threat, often in a transborder fashion. The necessary structures have begun to be put in place but they need to be reinforced rapidly given the imminence and magnitude of the challenge.

Strengthening the European Counter Terrorism Centre (ECTC)

An efficient response to terrorist threats requires the development of strategic capabilities at the EU level such as expertise, information checking and analysis, scenario and threat assessment and a wide range of operational responsibilities, from incident response and investigation support to coordination and frontline operations such as combating violent content online. The European Counter Terrorism Centre, set up in January 2016 within Europol, is a blueprint for how such tasks could be developed. Currently, ECTC has limited means (only 39 staff members and 5 seconded national experts).

To constitute an efficient European response, the ECTC needs to be strengthened in a number of frontline tasks: operational and resource-related challenges must be overcome and the Centre must be more effectively staffed with personnel from Member States’ services, not least in the form of permanent secondments of counter-terrorism experts, in addition to ad hoc support on enhanced cross-border investigations, carried out by the Joint Investigation Teams (JITs).

Digital Intelligence and Technological Autonomy

Digital technologies provide an open field of bottomless possibilities for tech-savvy terrorist actors, such as Daesh, which, in parallel to its territorial expansion, is building a ‘digital caliphate’. Security, therefore, cannot be achieved without superior technological capabilities that are a match to the terrorist threat. However, most public institutions are ill-equipped to face such realities - both in mindset and skills. Governments cannot do it alone: the infinite geography of the Internet requires networked action across borders.

As platforms can be exploited as vehicles for mass broadcasting of terrorist content, private corporations need to more proactively monitor their networks and inform governments of possible threats. Today, businesses are cooperative but too often only in response to government requests to take down objectionable content or users accounts. The onus of the initiative must be shifted: the online platforms’ ability to monitor user behaviour should give birth to a ‘voluntary regime’, where private actors, in cooperation with institutions, should actively exercise their responsibility to ‘notice and takedown’ radical content. As regards child abuse, there are already terms of reference which establish clear criteria for action. Although the definitions of ‘terrorism’ and ‘terrorists’ are less clear-cut, creating a set of standards can help in signalling and addressing risks. Further action could include reviewing the ‘mere conduit’ principle of the e-commerce directive, taking down extremely harmful content.

Technological autonomy should also become a European objective and governments should incentivise public-private partnerships in the domain of cybersecurity and Internet safety. Horizon 2020 already earmarks a budget of 1.7 billion euro for its ‘Secure Societies Programme’ and several actions of the 2016-2017 funding round relate specifically to the fight against terrorism. Future calls and the next annual programmes must be developed with heightened focus on counter-terrorism technology and capacity building, taking into account the needs of the security and law enforcement communities.

Public institutions and governments themselves must, in the meanwhile, take urgent action on ensuring their future ability to act as a security provider in the tech-savvy and increasingly digital world. They should start today by improving their digital fluency when it comes to counter-terrorism. This entails growing teams with the right set of skills: from data scientists and social media analysts to software engineers.
Various ministries and departments must build advisory capacity on cybersecurity and big data analytics to anticipate and manage risks in their fields. **Effectiveness will require a ‘service-oriented’ approach in government** that facilitates cross-institutional collaboration and information sharing. The ultimate goal must be to one day create a single, integrated data management environment that makes both access to – and input of – information easy and centralised. This will need a team of professionals from different disciplines and fields that can synthesise information that might otherwise seem unrelated. These are the preconditions to making society safe as the boundaries between the digital and physical space blur.

**Enabling and Mobilising Bottom-Up Actions**

The process of radicalisation is difficult to disentangle. It breeds on frustration and exclusion but reaches critical stage only in circumstances which cannot be easily universalised. This calls for a high degree of attentiveness to an entire spectrum of social and societal conditions which lead to marginalisation. **The Radicalisation Awareness Network (RAN) has become a hub of knowledge about radicalisation that should be further built upon.** It connects 2000 first-line practitioners and has recruited 140 consultants/experts. Its current scope, however, does not allow it to respond to all demands for engagement, preventing it from delivering impact where it would make an enormous difference – particularly in neighbouring countries.

The Commission can mobilise a wide array of tools in the areas of social affairs and employment, youth and sports, education and culture in the fight against radicalisation. **A virtual Erasmus exchange programme to connect students from Europe, the Middle East and Africa** would provide a platform for integration and social capital building.

A similar initiative was launched by President Obama in the US last year, with the support of the Massachusetts Institute of Technology to measure the effectiveness of the programme in removing prejudice and building trust, and the Aspen Institute as coordinator of the network of participating universities, research institutions and NGOs. Building on the success of the traditional Erasmus programme, the Commission has a chance to set a model of excellence for digitally-savvy integration.

**Facilitating Political Dialogue on Islam**

Europe is home to a large and diverse Muslim population, including a second-generation migrant youth that faces significant challenges of socio-economic and cultural inclusion. Disenfranchisement, discrimination and social exclusion create a fertile ground for radical interpretations of Islam that explicitly reject the core of our common values.

In the framework of the dialogue established by Article 17 (3) TFEU, **European Muslim community leaders have a defining role in the fight against radicalisation and jihadism.** Their engagement at the local and European level requires positive role-models and outspoken thought-leaders to step into the limelight. The European institutions should play their role in animating and facilitating dialogue within and with the Muslim community. They should support a network and platform for Muslim thinkers in Europe engaged in moderate Islam.

**Development and Cooperation for Transnational Security**

The transnational nature of new threats implies that development and cooperation policy needs to be an essential part of the basket of tools to ensure security. This would also imply a review of current spending,
especially in the Middle East and Africa, both in terms of where money is invested and of how projects are carried out - for example, favouring direct execution of programmes vis-à-vis relying on external consortia.

Recent events have, indeed, uncovered failures in cooperation with partners around the Mediterranean, despite shared concerns. EU home affairs diplomacy and counter-terrorism cooperation must be developed as a matter of priority with essential partners from Turkey to Morocco. They should be encouraged to cooperate with the ECTC network to ensure adequate information sharing and police cooperation, in particular through the Interpol system. A transnational network of liaison officers could also be established in key countries to facilitate law enforcement and judicial cooperation on counter-terrorism, in addition to the experts already deployed by the European External Action Service.

### 3. Managing by Anticipation

While terrorism is the most salient threat of the day, its forms and shapes will change over time. Europe must prepare for this, not only by enhancing its capabilities but also by aligning political capital and future trends. It must manage by anticipation and be prepared for the worst.

### Strategic Dialogues on Upcoming Challenges to European Security

The Treaty’s ‘solidarity clause’ (Article 222 (4) TFEU) foresees that ‘the European Council shall regularly assess the threats facing the Union in order to enable the Union and its Member States to take effective action.’ The European project was conceived as being forward-looking by design.

Against this backdrop - and following President Juncker’s ambition to converge towards a ‘Security Union’ - European institutions should sustain momentum and launch an assessment of the security challenges at European level, resulting in a report that identifies threats, response capabilities and policy priorities. This is precisely the type of exercise that the US government initiated after the 9/11 attacks, empowering an enquiry committee to conduct a thorough review of US preparedness and failings ahead of potential terrorist attacks.

The process could rely on peer reviews of national security arrangements with reference to the solidarity commitments foreseen by the Treaties (Article 222 and 42(7) TFEU). Given the volatility and frequency of current and future security threats, the review should be repeated annually and be discussed at a dedicated European Council or a ‘Strategic Dialogue on Upcoming Challenges to European Security’ with the aim of both anticipating and managing security risks.

In this context, the importance of security and the development of the Union as a security provider may justify the appointment of a European Security Adviser to the President of the European Commission, with a mandate that extends beyond counter-terrorism. This function would be part of a European Security Board, comprising the EU Counter-Terrorism Coordinator as well as all heads of Justice and Home Affairs agencies of the EU and the competent authorities of the Member States.

### Benchmarking Spending Against Future Priorities

The past year has shed light on the mismatch between unfolding threats and existing capabilities. It has also demonstrated that no country on its own can successfully manage this new threat. This calls for a more ambitious European response – right here at home but also in our geographic neighbourhood, and in the digital space.

There are a number of different sources of counter-terrorism funding spread across the EU budget. This makes the total EU and Member State spending difficult to estimate precisely. The main budgetary channel is the Internal Security Fund (ISF) with a total of 3.8 billion euro from 2014 to 2020 of which a small part goes to counter-terrorism actions (see Figure 2). In the 2007-2013 Multiannual Financial Framework, freedom, security and justice policies represented only 0.77% of the total EU budget.

![Figure 2: Internal Security Fund 2014-20 Million euro](http://ec.europa.eu/dgs/home-affairs/e-library/docs/invest-open-and-secure-europe/index.html)

The upcoming review of the Multiannual Financial Framework provides a timely and unique opportunity to benchmark the EU budget against emerging trends, of which security is at the core.
The Legal Basis for the Security Union

All the proposals linked to the Security Union can be implemented within the current Treaty framework on the basis of Article 88 (1), Article 222 (1) or 352 TFEU. Article 71 TFEU, establishing the standing committee, as well as Article 88 TFEU on Europol define a European institutional dimension on internal security. For example, under the umbrella of Europol, there is already a European Counter Terrorism Centre (ECTC), that is the platform for better coordinated exchange of information and data. The solidarity clause of Article 222 (1) TFEU is particularly relevant for a terrorist threat or attack. It was introduced in the aftermath of the terrorist attacks in Madrid, and proposes that in order to ‘prevent the terrorist threat in the territory of the Member States’ or in order to ‘protect democratic institutions and the civilian population from any terrorist attack’, the EU shall mobilise all the instruments at its disposal, including the military resources made available by the Member States. Moreover, if a Member State is the object of a terrorist attack, according to Article 222 (2) TFEU, the other Member States shall assist it at the request of its political authorities. In the framework of the area of freedom, security and justice Article 68, 74, 75, 77, 83, 84 and 87 TFEU comprise certain European competences that allow for (limited) action to prevent terrorism. These enable the EU to establish measures with regard to capital movements and payments, a better administrative cooperation among the Member States involving the Commission, or a genuine European Border Management System including a European Border Management Agency, for example.

Reflecting on Future Institutional Reforms

The United States example shows how important it is to establish a single point of competence and ownership for joint strategic intelligence, analysis and planning. US structures cannot be easily transposed to the European Union, but a common EU body for analysing terrorism, sharing intelligence and conducting scenario and threat assessment would help overcome many of today’s difficulties. One of its major tasks would be to provide for a European diagnosis of the counter-terrorist threat by ‘connecting the dots’ and coordinating intelligence capabilities. It would then develop strategic plans for counter-terrorist action. This potential agency could be headed by the EU Counter-Terrorism Coordinator and staffed with personnel from the responsible services of the Member States as well as EU institutions.

The lack of common culture is one of the main impediments to effective information exchange and prompt action on shared analysis. Today, European intelligence communities hail from 28 different national cultures. Beyond the definition of standards and practices (e.g. agreement on standard spelling and translation of Arabic names into the Roman alphabet across Member States), work towards common risk indicators and analysis is a first step in forging a more effective European intelligence culture. The creation of a European intelligence academy could therefore be supported to enhance cooperation between different European intelligence communities.

Building an EU Judicial Dimension of Counter-Terrorism

An effective European judicial response is needed to overcome the hiatus between transnational terrorist activities and repression which takes place only at the national level. Today, Eurojust serves the purpose of the exchange of information with certain powers of proposal. Thus, Eurojust should be strengthened, including in developing national rehabilitation strategies for returning foreign fighters. In addition, Article 86 TFEU foresees that a European Public Prosecutor’s Office (EPPO) may be established for serious cross-border crime, according to a specific procedure. Although the EPPO is primarily foreseen for fraud against the EU’s financial interests, Article 86(4) stipulates that the European Council may amend the Treaty, after consulting the Commission and gaining the consent of the Parliament, to extend its powers to include serious cross-border crime (such as terrorism).

An EU Public Prosecutor’s Office on Terrorism could, in liaison with Europol, be responsible for investigation and have the possibility to prosecute and bring cases to judgment in relevant national courts. The EPPO could have a role in the listing of persons, groups and entities involved in terrorist acts and subjecting them to restrictive measures.
4. Conclusion

If something can be imagined, there is a chance it will happen. Europe must collectively live up to a new reality that will be with us for at least a generation – a new enemy who is inherently transnational, digitally-savvy and out to inflict the biggest possible carnage on innocent civilians. New technologies that are seemingly innocuous in everyday use can be conduits for radicalising young people and powering simultaneous terrorist attacks. Scientific advancements can be abused for transmission of communicable diseases, contamination of food, soil, air and drinking water by chemical, biological, radiological and nuclear (CBRN) agents. In the face of such adversity, the European project has to muster the collective determination to stare down this new threat – and do so fast. That is why the time is ripe for a genuine ‘Security Union’.

The current level of fragmentation makes Europe vulnerable and calls for leaders to act together when the safety and physical integrity of citizens are put into grave danger. This is not only a plan of technocratic actions. It is first and foremost a political commitment to send a clear message that Europe is united in its resolve to fight terrorism.

This Strategic Note was written in collaboration with Michel Barnier, Special Adviser to President Juncker on European Defence and Security Policy.