PARLEU2017.EE

Parliamentary Dimension
of the Estonian Presidency
of the Council of the
European Union

Plenary Meeting of the LVIII COSAC
26–28 November 2017, Tallinn

Background Information

Session IV: State of play – building an effective and sustainable Security Union

It is the most basic and universal of rights to feel safe and secure in your home country and abroad. The Europeans rightly expect their Union to provide that for them. The Juncker Commission has made security a top priority. The European Union has taken decisive action to **deny terrorists the means to carry out attacks**, **as well as to share intelligence between Member States**, **protect Europeans online,** and **manage the borders better**. This background paper aims to give a brief overview of the four objectives set by the Commission in order to build an effective and genuine Security Union. The background paper is based on the tenth and eleventh progress reports towards an effective and genuine Security Union.

First, the **protection and management of Europe's external borders** is a prerequisite for free movement without internal borders. Therefore, it is essential to know who is crossing the EU's borders. Progress has been made in enhancing security at the external borders. The revised **Schengen Borders Code** allows systematic checks against the databases of all travellers crossing the external borders and thus helps to identify travellers who pose a threat to security. Political agreement has been reached at the EU level on the **EU Entry/Exit System**. Once in effect, the system will register the entry and exit data of non-EU nationals crossing the EU's external borders. This contributes to enhancing external border management and internal security. Also currently in process is establishing the **European Travel Information and Authorisation System**, which aims to collect information on individuals who intend to travel visa-free to the EU. This enables the identification of possible risks regarding irregular migration and security prior to arrival.

The **effective exchange of information** is equally important. This can be achieved first and foremost by maximising the benefits of the existing information systems. A good example is the increased use and number of hits produced by the **Schengen Information System**. According to the statistics, there has been a 40% increase in checks in 2016 compared to 2015. Also, hits increased accordingly from around 150,000 in 2015 to more than 200,000 in 2016. The second way to achieve this is by addressing gaps in the EU's architecture of data management. The third way forward is to ensure the interoperability of information systems. The objective is to make necessary information available more quickly and to eliminate the current blind spots caused by the unconnected databases.

Several EU level legislations have been adopted recently in order to **close down the space in which terrorists operate.** In May this year, the **Directive on combating terrorism** and the **Firearms Directive** were adopted. The first helps to prevent terrorist attacks by criminalising acts such as financing terrorism, undertaking training or travelling for terrorist purposes, as well as organising or facilitating such travel. The latter proposal significantly broadened the range of prohibited weapons, taking the most dangerous weapons out of wider circulation. Work has continued on EU proposals regarding terrorist financing, in the areas of **money laundering**, **illicit cash flows** and **freezing and confiscating assets**. Recent terrorist attacks have focused on the so-called **soft targets**, which are public areas such as schools, hotels, beaches, shopping malls, cultural and sports events, crowded areas, or transport hubs. The Commission has recently published the Action Plan to support the protection of public spaces and an **EU Policy Group on Soft Target Protection** has been set up to enhance cooperation and coordination between Member States.

The most **effective counter-terrorism policy is prevention**. However, radicalisation has different root causes and is usually the result of a combination of different factors. Thus, it requires measures not only at the EU level but also national and especially regional level. Terrorists are making use of new communication tools and are increasingly abusing the internet for their purposes. The internet provides radical recruiters more opportunities to interact with people who would otherwise not be reachable by conventional means. Addressing the root causes of extremism, therefore, requires action to tackle the surge of hate speech as well as the dissemination of extremist and terrorist material online. Measures also need to be taken to strengthen the resilience of individuals against such propaganda. The **EU Internet Forum,** established in 2015, brings together industry, Member States, law enforcement, and civil society partners to explore how to tackle the challenges of terrorist and extremist propaganda. In the past two years, the **EU Internet Referral Unit** at Europol has flagged terrorist content in over 350,000 items, 80–90% of which have been removed. There is also the **Radicalisation Awareness Network** (RAN) that connects EU, national and local level players who deal with prevention and countering radicalisation. The Commission has recently set up the **High-Level Expert Group on Radicalisation**, involving the main stakeholders to elaborate a set of guiding principles and recommendations for further work in this area.

In conclusion, work needs to continue in order to address the security challenges by making our information systems interoperable, preventing violent extremism and radicalisation, cutting off sources and channels of terrorist financing, and improving cybersecurity. There is a need to further develop and adjust the existing policies and tools in order to address the rapidly evolving security threats and challenges.

Some points for discussion:

1) In your opinion, what is the best approach to protect the so-called soft targets that have been a focus of the recent terrorist attacks?
2) How to enhance cooperation with social media companies to detect and remove terrorist content?
3) What do you consider to be the most effective means to counter terrorism at national and regional levels?