Agencia Tributaria

TRIBUNAL PRUEBAS SELECTIVAS AL CUERPO
SUPERIOR DE VIGILANCIA ADUANERA
Resolución 18 de mayo de 2022 (BOE 24 de mayo)

Tercer ejercicio – Primera parte
Examen inglés – Turno libre
18 de noviembre de 2022

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Third Progress Report on the implementation of the EU Security Union Strategy

I. Introduction

The Security Union aims to ensure that the EU plays its full role in ensuring the safety of citizens while respecting the values that define the European way of life. Implementation is progressing on all four strategic priorities set out in the Security Union Strategy: (i) a future-proof security environment; (ii) tackling evolving threats; (iii) protecting Europeans from terrorism and organised crime; and (iv) a strong European security ecosystem.

The COVID-19 pandemic has accentuated key vulnerabilities, while threats and challenges to European security continue to evolve in response to changing technologies and international developments. The second Security Union report charted the particular challenges for security presented by the COVID-19 pandemic.

This third report focuses on the developments of the past six months linked to the most significant emerging threats in this period. It highlights in particular the need to intensify cooperation not only within the EU, but also internationally, with a broad array of stakeholders and partners.

The Security Union Strategy is being taken forward in the context of threats that are increasingly cross-border and cross-sectoral. The digital world continues to be exploited for malicious ends. Cyber-attacks originating in or outside Europe, including ransomware, are ever more frequent, hitting core state functions, such as healthcare and crucial infrastructure, industries and public bodies, as well as individuals. Foreign information manipulation and interference activities are on the rise, and have in some cases gone hand in hand with cyber activities, in particular hack and leak operations. Organised crime of all kinds continues to operate cross-border, and an effective response relies on partnerships beyond the EU. International developments require vigilance in the context of potential radicalisation and terrorism, as well as hybrid attacks including, during this reporting period, at the EU's external border.

To address these increasingly sophisticated global and cross-border threats, the EU is stepping up not only its own response but also cooperation with international partners. This is a core theme of this report.

At the same time, work is intensifying to reinforce security in the Schengen area. Close cooperation between Member States is crucial to the overall security of the Schengen area. A substantial new package including measures to enhance police cooperation and the security of the Schengen area has been prepared by the Commission to provide further improvements in this regard.

EU agencies are fully involved in this work through their operational activities in support of Member States' national authorities, and by providing expertise, information and situational awareness on the most pressing threats.

Further details and updates on the full range of initiatives under the Security Union are presented in an Annex to this Communication

II. A future-proof security environment

Digital infrastructures, technologies and online systems allow us to create business, consume products and enjoy services. However, this growing digitalisation of our environment also makes us more vulnerable to attack. The scale, frequency and sophistication of cybercrime and cyber attacks is increasing, according to both **Europol**'s Internet Organised Crime Threat Assessment published in November 2021, and the EU Agency for Cybersecurity (**ENISA**)'s annual Threat Landscape report of October 2021. Governments in Europe faced at least 198 cybersecurity incidents in the past year, making public administration the most heavily targeted sector. Highly-skilled and well-resourced malicious actors come from inside, but also from outside the EU, and exploit the borderless nature of the global, open internet and the jurisdictional gaps of current frameworks. Cyberattacks and cybercrime are often interlinked, as demonstrated by numerous incidents where criminals are targeting vulnerabilities to extort money, and are a constant threat that continues to evolve. Cybercriminals may simply be motivated by increasing opportunities for the monetisation of their activities, but other malicious state or non-state behaviours are motivated by more complex geopolitical and ideological considerations, in addition to financial gains. Data gathered by **ENISA** has shown that state-backed hackers also reached 'new levels of sophistication and impact' with attacks targeting public and private sector supply chains.

It is therefore particularly important to maintain a high level of ambition for EU action, both in terms of the level of security we seek to achieve, and the pace at which we work to achieve it. The European Council of October 2021 addressed the marked increase in malicious cyber activities. It reaffirmed the EU's commitment to an open, free, stable and secure cyberspace, and stressed the need for effective coordination and preparedness in the face of growing cybersecurity threats. It also emphasised the necessity to step up action in the fight against cybercrime, in particular ransomware attacks, and enhance cooperation with partner countries, including in multilateral fora.

IV. Protecting Europeans from terrorism and organised crime

Terrorism

The Terrorism Situation and Trend Report published by Europol in June 2021 indicated that Member States considered that jihadist terrorism remained the greatest terrorist threat in the EU. The report confirms that the most frequent type of jihadism-inspired attacks in the EU, Switzerland and the UK, has been assaults in public places targeting civilians. All completed jihadist attacks in 2020 were committed by individuals acting alone. It also indicates that several suspects arrested in 2020 had online contact with followers of terrorist groups outside the EU. The self-proclaimed Islamic State terrorist group and the al-Qaeda network continued to incite lone-actor attacks in Western countries, showing how external and internal security are closely interlinked. In August, the Justice and Home Affairs Council stated that “the EU and its Member States will do their utmost to ensure that the situation in Afghanistan does not lead to new security threats for EU citizens”. Steps have been taken to ensure that all available tools are used to respond to possible threats.

In light of the developments in Afghanistan, the EU Counter Terrorism Coordinator in coordination with the Commission, the European External Action Service, the Presidency and key EU Agencies, drew up **a Counter-Terrorism Action Plan on Afghanistan**. The Action Plan sets out 23 recommendations in four areas: security checks – preventing infiltration; avoiding Afghanistan becoming a safe haven for terrorist groups; monitoring and countering propaganda and mobilisation (e.g. role of Radicalisation Awareness Network); and tackling organised crime as a source of terrorist financing. The Action Plan was welcomed by Member States at the Justice and Home Affairs Council on 8 October 2021. A first achievement has been a voluntary procedure for enhanced security checks on people coming from Afghanistan, which was endorsed by the EU Standing Committee on Internal Security on 22 November 2021. At a technical meeting with members of the Taliban declared interim Afghan government on 28 November 2021 in Doha, the EU urged Afghanistan to take determined action to fight all forms of terrorism.