Dr Alexander Duisberg Partner
alexander.duisberg@twobirds.com
Bird & Bird LLP, Munich

European Commission takes steps against cyber terrorism in Security Union Report

The European Commission has recently published its 11th Security Union Report (the 'Report'), which includes a set of operational and practical anti-terrorism measures (COM (2917) 608 of 18 October 2017). The package presented aims at tackling terrorism and security threats to citizens in the EU, in particular those threats utilising cyber technologies and networks, as well as building resilience against those threats. With this initiative, the Commission is responding to the increased vulnerabilities in the EU and is striving to implement the measures over the next 16 months. The proposed measures are manifold and directed towards cutting terrorist financing, countering online radicalisation, boosting cyber security, enabling decryption where required to break into terrorist networks, and strengthening cross-border cooperation and information exchange between the relevant authorities, as well as removing obstacles for obtaining financial transaction data. In this article, Dr Alexander Duisberg, Partner at Bird & Bird, discusses the Commission's Report and the possible implications in the field of cyber security.

The key elements of the Report

The Report identifies three main pillars for tackling terrorism and the means supporting it: facilitate access to financial information, restrict access to explosive precursors, and support law enforcement in criminal investigations. The first pillar is based on the assumption that financial information, including data on financial transactions, can help expose terrorists and reveal suspicious activities, logistics and movements. Ultimately, such information is intended to assist law enforcement in preventing or resolving terror attacks. Restricting access to explosive precursors shall mitigate the threats posed by homemade explosives, in particular triacetone triperoxide ('TATP'). While this mainly covers the issue of physical access, availability of the relevant information over the internet is an increasing concern[1]. Supporting law enforcement refers, in particular, to the problem of cyber security and data protection in the context of criminal investigations. Finally, it aims at countering (online) radicalisation.

Comments on the Commission's action plans

As part of the Commission's wider approach to combating terrorism, the Report refers to two separate action plans, one 'to support the protection of public spaces,' and the other 'to enhance the preparedness against chemical, biological, radiological and nuclear security risks.' These do not come as a surprise. The proposed measures build on a range of statements and announcements made by the Commission in the recent past. In regards to accessing financial information, the Commission is following up on its 2016 Action Plan on terrorist financing and last year's Security Union Report, which analysed how authorities should access, exchange and use the relevant data. The measures in the Report aim, in particular, at preventing and detecting money laundering and terrorist financing. Cyber security, as mentioned above, was recently addressed by the Commission in last September's Letter of Intent to the European Parliament and the Council Presidency and the accompanying Roadmap for a More United, Stronger and More Democratic Union. In this Roadmap the Commission strives to set up, as a matter of priority, a cyber security package to effectively address the changed cyber threat landscape.

How the Commission proposes to improve cyber security against terrorism

Cyber security plays a prominent role in the Commission's plan to fight terror. In the Report, the Commission emphasises encryption issues: The Commission acknowledges that, on the one hand, encryption is key to ensure cyber security and for the protection of personal data. On the other hand, it is a given fact that criminals using encryption hinder law enforcement and judicial authorities in obtaining the information they need for criminal investigations, and for prosecuting and convicting criminals. Following intense discussions with technical and legal experts, the Commission now suggests an approach to support law enforcement and judicial authorities consisting of: (i) legislative measures to improve access to electronic evidence (see below), (ii) funding training on cross-border cooperation to develop an electronic platform, as well as (iii) technical and organisational measures that enable Member State authorities to effectively counter the challenges posed by encrypted information.

The envisioned legislative measures include creating a European legal framework for cross-border access to electronic evidence. A common problem for national law enforcement authorities is that necessary evidence is often located in another country. Accordingly, uniform access to evidence will enable authorities to access evidence and effectively investigate and prosecute criminal activities. The Commission plans to present its elaborate proposals early next year. These measures will involve practical implementation, such as setting up an electronic platform

Image: monsitj / iStock / Getty Images Plus

to allow an EU-wide exchange of information and a standardisation of judicial cooperation forms.

The kind of technical and organisational measures the Commission is considering

Technical and organisational measures mean, in particular, establishing a standardised level of expertise and technical resources across EU Member States. The fact is that most Member States do not have adequate expertise to access encrypted information in criminal investigations. Therefore, the Commission proposes a set of measures to tackle encryption, however, 'without prohibiting, limiting or weakening encryption,' the Report states. The measures are directed towards both national and European authorities: They include, for example, enhancing the decryption capabilities of Europol by creating 86 additional security-related posts, establishing a network of expertise and providing training programs for authorities' staff.

The Commission recognises that some Member States have developed their own techniques to overcoming encryption[2]. The Commission wants to put into the hands of Member State authorities a 'toolbox of alternative investigation techniques,' so that authorities can develop and use measures to obtain information from encrypted emails exchanged by criminals. At the same time, measures weakening encryption or having an impact on an indiscriminate number of people shall not be considered or pursued. Europol will be the custodian of that toolbox.

Any package of measures will only succeed if service providers and industry partners embrace the Commission's approach. To that end, the Commission will support structured dialogues with those parties, in particular within the context of the EU Internet Forum.

Other measures the Commission is taking to deepen the understanding and use of decryption techniques

The Commission sees an imminent need for training and skills development. In the Report, the Commission sets out its intention to set up a €500,000 funding package under the 2018 annual work programme of the Internal Security Fund Police for dedicated training for officers at law enforcement agencies and judicial authorities, on how to obtain necessary information from encrypted communications between criminals. Also the expertise of the European Cybercrime Training and Education Group ('ECTEG') shall be taken into account. Lastly, the Commission states it will support the development of an observatory function in collaboration with the European Cybercrime Centre ('EC3') at Europol, the European Judicial Cybercrime Centre ('EJCN') and Eurojust.

The Commission's intentions regarding online radicalisation

One of the key objectives for the Commission lies in countering online radicalisation, including through social media platforms[3], as well as other areas of networked terrorist collaboration. The Commission has set up a High Level Expert Group on Radicalisation to counter radicalisation and improve coordination between stakeholders. The Group's task is to set out recommendations for legal and organisational action. A first interim report containing recommendations for further work is expected by the end of this year. Further measures in that context include closer collaboration between counter-terrorism experts in EU delegations, enhanced cooperation between the Common Security and Defence Policy missions and operations, and the EU Justice and Home Affairs Agencies, in order to collect, analyse and exchange information, as well as strengthened international cooperation with partner countries in the Western Balkans, the Middle East, North Africa, Turkey, the Persian Gulf, the Sahel, and key strategic partners in the US, Canada and Australia, as well as with various international organisations.

[1] Recently on 31 October 2017, German police arrested a suspected terrorist who had procured TATP over the internet, presumably averting a terror attack.

[2] The German 'Federal Trojan' backdoor software tool for online search and possibly circumventing encrypted communication in the context of combating terrorism is an example of this.

[3] In that context, it is interesting to note that the German Bundestag has this summer adopted what is known as the Social Media Hate Speech Law. The Law is a forerunner in the EU-wide initiative to counter online radicalisation and is a key element to combating terrorist content online in Germany.