EUROPEAN
COMMISSION

Brussels, 25.1.2017
COM(2017) 41 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL

Fourth progress report towards an effective and genuine Security Union

Fourth progress report towards an effective and genuine Security Union

I. INTRODUCTION

This is the fourth monthly report on the progress made towards building an effective and genuine Security Union and covers developments under two main pillars: *tackling terrorism and organised crime and the means that support them; and strengthening our defences and building resilience against those threats*. This report focusses on four key areas, information systems and interoperability, soft target protection, cyber threat and data protection in the context of criminal investigations.

The December Berlin Christmas market attack has again highlighted serious weaknesses in our information systems that need urgently to be addressed, in particular at EU level, to help national border and law enforcement authorities on the ground to do their demanding jobs more effectively. The fact that the different information systems are not interconnected – allowing attackers to use multiple identities to move undetected, including when crossing borders - and that that information is not routinely uploaded by Member States into the relevant EU databases are practical implementation weaknesses that need urgently to be remedied. Furthermore, when it comes to law enforcement measures on the borders and returning persons whose asylum requests have been rejected, further work is also needed.[1]

In terms of soft target protection, the Commission will accelerate the work it is doing to bring together experts from Member States to share best practice and agree standard guidelines.

The cyber threat facing the EU is receiving widespread media coverage and this report looks at the various different work strands in this area already underway. This covers both the prevention side – through work with industry to promote security by design and implementation of the Network Information Security Directive – and fostering cooperation between Member States and with international organisations and partners on dealing with cyber-attacks as they happen. In the coming months, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy will identify the actions needed to provide an effective EU-wide response to these threats, building on the 2013 EU Cybersecurity Strategy.

The protection of individuals' privacy and personal data is a key fundamental right and thus a cornerstone in any action towards a genuine Security Union. The Data Protection Directive for the police and criminal justice field adopted in April 2016 ensures a common high standard of data protection and will therefore facilitate smooth exchange of relevant data between Member States' law enforcement authorities. The Commission has also launched a revision of the ePrivacy Directive as part of its Data Package to extend the Directive's coverage to include all electronic communication providers and to bring its provisions in line with the General Data Protection Regulation. The proposal is designed to ensure privacy of electronic communication while also setting out the

[1] The Commission will bring forward a revised Action Plan on returns in the coming weeks, see Report from the Commission to the European Parliament, the European Council and the Council on the operationalisation of the European Border and Coast Guard, COM(2017) 42.

grounds under which restrictions of the scope of the ePrivacy Regulation can be envisaged, including for reasons of national security or criminal investigations.

II. STRENGTHENING INFORMATION SYSTEMS AND INTEROPERABILITY

President Juncker's State of the Union address in September 2016 and the European Council conclusions of December 2016 refer to the importance of overcoming the current shortcomings in information management and of improving the **interoperability and interconnection between existing information systems**. Recent events have again highlighted the urgent need to link existing EU databases together, not least to give border and law enforcement on the ground the tools needed to detect identity fraud. For example, the perpetrator of the December 2016 Berlin terrorist attack used at least 14 different identities and was able to pass between Member States without detection. There is a clear need for existing and future EU information systems to be searchable simultaneously using a biometric identifiers to close off this avenue for terrorists and criminals.

In this regard, the Commission launched work in April 2016 with its proposals for "stronger and smarter information systems for borders and security"[2]. This identified shortcomings in the functionalities of existing systems, gaps in the EU's architecture of data management, problems with the complex landscape of differently governed information systems and an overarching fragmentation caused by the fact that existing systems were designed individually rather than to fit together. As part of this process, the Commission launched the **High Level Expert Group on Information Systems and Interoperability** with EU Agencies, Member States and relevant stakeholders. On 21 December 2016[3] a Chairman's report set out the **interim findings** of the group which includes the priority option of creating a Single Search Portal to allow national law enforcement and border authorities to search simultaneously existing EU databases and information systems. The interim report also highlights the importance of data quality – since the information systems are only as effective as the quality and format of the data entered into them - and makes recommendations to improve the quality of data in EU systems through automated data quality control.

The Commission will rapidly follow up on the option to create a Single Search Portal and, together with the EU agency for the operational management of large scale IT systems, eu-LISA, will start its work on a portal capable of searching in parallel all relevant existing EU systems. A related study should be ready by June, as a basis for designing and testing a prototype of the portal before the end of the year. The Commission considers that in parallel Europol should continue its work on a system interface that will enable Member States' frontline officers when they are consulting their own national systems to consult automatically Europol's databases simultaneously.

The work towards the interoperability of information systems aims to overcome the current fragmentation in the EU's architecture of data management for border control and security and the related blind spots. When databases use a common repository of identity

[2] Communication "Stronger and smarter information systems for border security" COM(2016) 205 Final.

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

data – as envisaged for the proposed EU Entry/Exit System and the proposed European Travel Information and Authorisation System (ETIAS) – a person can only be registered under one single identity in the different databases, which prevents the use of different fake identities. As a first step as suggested in the interim findings of the High Level Expert Group, the Commission has asked eu-LISA to analyse the technical and operational aspects of implementing a shared biometric matching service. Such a service would enable searches across different databases with biometric data, which could expose false identities used by the person in question in another system. Beyond that, the High Level Expert Group should now assess whether it is necessary, technically feasible and proportionate to extend the **common identity repository** envisaged for the Entry/Exit System and ETIAS to other systems. In addition to biometric data stored in the biometric matching service, such a common identity repository would also include alphanumerical identity data. The Group should present its findings on this in its final report by the end of April 2017.

Recent security events highlight the need to re-examine the question of **mandatory information sharing** between Member States. The Commission proposal of December 2016 to strengthen the **Schengen Information System** foresees – for the first time - an obligation for Member States to issue alerts on persons related to terrorist offences. It is important that the co-legislators now work towards a swift adoption of the proposed measures. The Commission stands ready to examine if a mandatory obligation for information sharing should be introduced for other EU databases.

III. PROTECTING OUR SOFT TARGETS AGAINST TERRORIST ATTACKS

The Berlin attack was the most recent in the EU directed against so-called soft targets, which typically are civilian sites where people gather in large numbers (e.g. public spaces, hospitals, schools, sporting arenas, cultural centers, cafés and restaurants, shopping centres and transportation hubs). By their nature, these locations are vulnerable and difficult to protect and are also characterised by the high likelihood of mass casualties in the event of an attack. For all of these reasons they are favoured by terrorists. The threat of future attacks against soft targets including transport remains high, as confirmed by available assessments, including Europol's report on changes in Daesh modus operandi.[4]

The 2015 European Agenda on Security and the 2016 Communication on the Security Union highlighted the need for increased work to improve security and use of innovative detection tools and technology in protection of soft targets. The Commission has been working to support, and encourage the sharing of best practice between, Member States in developing better tools to prevent and respond to soft target attacks. This work has produced operational handbooks and guidance material. Currently, the Commission is developing, in close cooperation with Member States' experts, a comprehensive manual on security procedures and templates applicable to different soft targets (e.g. shopping

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, November 2016 – Europol Public Information, available at: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

malls, hospitals, sport and cultural events). The aim is to issue soft target protection guidance to Member States in early 2017 based on best practices in Member States.

In parallel, the Commission will convene in February the first workshop with national authorities on Soft Target Protection, with a view to exchange information and develop best practices on the complex issue of soft target protection and public safety and security. The Commission is also funding a pilot project by Belgium, the Netherlands and Luxembourg under the Internal Security Fund to establish a regional Centre of Excellence for law enforcement special interventions, which will offer training for Police officers who are often the First Responders in case of an attack.

Responding to attacks on soft targets is a key component of the Commission's work on civil protection. In December, the Commission announced the actions that it intends to pursue with Member States in order to protect EU citizens and reduce vulnerabilities in the immediate aftermath of terrorist attacks. These actions will strengthen the coordination between all the actors involved in managing the consequences of attacks and the Commission pledged to support Member States' efforts by facilitating joint trainings and exercises and by ensuring a sustained dialogue via existing focal points and expert groups. The Commission will also support the development of specialised modules for responding to terrorist attacks within the framework of the Union Civil Protection Mechanism and initiatives to share lessons learnt and raise public awareness.

Together with Member States, the Commission will also explore what EU support could be mobilised to help build resilience and strengthen security around potential soft targets. Member States could also apply for financing from the European Investment Bank (EIB) (including the European Fund for Strategic Investments) in line with EU and EIB Group policies. Any project would be subject to the normal decision-making procedures as set out in the legislation.

Regarding the specific soft targets in relation to transport public areas, such as public parts of airports or railway stations, the Commission's dedicated workshop in November 2016 with a wide range of stakeholders highlighted the need to maintain the balance between security needs, passenger convenience and transport operations. The conclusions underline the significance of building a security culture that encompasses not only staff but also passengers, the importance of local risk assessments as a base for defining appropriate countermeasures and the need to enhance communication between all parties involved.

IV. FACING THE CHALLENGES OF CYBER THREATS

Cybercrime and cyber-attacks are key challenges facing the Union and one where action at an EU level can help to strengthen our collective resilience. Every day, cyber security incidents seriously harm people's lives and cause major economic damage to the European economy and businesses. Cyber-attacks are a key component of hybrid threats – timed precisely in conjunction with physical threats, for example in connection with terrorism, they can have a devastating impact. They can also contribute to destabilising a country or challenging its political institutions and fundamental democratic processes. As we increasingly rely on on-line technologies, our critical infrastructures (ranging from hospitals to nuclear power plants) will become ever-more vulnerable.

The EU Cybersecurity Strategy from 2013 forms part of the core policy response on cybersecurity challenges. The central action is the Network and Information Security (NIS) Directive[5], adopted last July. It lays the groundwork for improved EU level cooperation and cyber-resilience by supporting cooperation and exchange of information amongst Member States and promoting operational cooperation in specific cyber security incidents and sharing information about risks. To ensure consistent implementation across different sectors and across borders the Commission will hold the first meeting of the NIS Cooperation Group with Member States in February.

In April 2016, the Commission and EU High Representative adopted a Joint Framework on Countering Hybrid Threats[6] which proposed 22 operational actions aimed at raising awareness, building resilience, better responding to crises and stepping up cooperation between the EU and NATO. As called for by the Council, the Commission and EU High Representative will provide a report by July 2017 to assess progress.

The Commission is also promoting and supporting technological innovation including by making use of the EU's research funds to drive new solutions and to create new technologies which can help strengthening our resilience against cyber-attacks (e.g. 'security by design' projects). Last summer we launched a EUR 1.8 billion private partnership on cyber security with industry.[7]

In transport, digitalisation is becoming a major enabler of the much-needed transformation of today's transport system. The fast pace of digitalisation brings many benefits, but it also makes transport more vulnerable to cyber-security or cyber-safety risks. Numerous actions are undertaken to mitigate the threat at different levels, specifically for aviation but also maritime, fluvial, rail and road transport.[8] The remaining challenge is to further clarify, harmonise and supplement the activities of different stakeholders engaged in enhancing different aspects of cyber resilience.

More widely, and given the rapidly evolving nature of the threat, in the coming months, the Commission and the EU High Representative will identify the actions needed to provide an effective EU-wide response to these threats, building on the 2013 EU Cybersecurity Strategy.

---

5 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

6 JOIN (2018)18.

7 Announced in the 2016 Cyber Resilience Communication, COM(2016) 410 final.

8 Examples are international guidelines, such as those developed by the International Maritime Organisation or through a recently adopted ICAO Resolution, with the joint initiative of the EU and the US; incident reporting whereby a more reactive mode is currently developed by the European Aviation Safety Agency , and cyber security by design, applicable to new systems being developed, such as Air Traffic Management Master Plan by the SESAR Joint Undertaking .

V. PROTECTING PERSONAL DATA WHILE SUPPORTING EFFICIENT CRIMINAL INVESTIGATIONS

The Data Protection Directive for the police and criminal justice field[9] is a building block in the fight against terrorism and serious crime. Based on a common standard of data protection laid down in the Directive, Member States' law enforcement authorities will be able to exchange smoothly relevant data while the data of victims, witnesses, and suspects of crimes will be duly protected.

Moreover, to ensure a high level of confidentiality of communications for both individuals and companies and a level playing field for all market players, as set out in the Digital Single Market Strategy of April 2015, the Commission adopted the proposed **ePrivacy Regulation** (replacing Directive 2002/58/EC) on 11 January.[10] As with the current Directive, the revised ePrivacy Regulation particularises the General Data Protection Regulation[11] and lays down a framework governing the protection of privacy and personal data in the electronic communications sector.

By means of this revision, all electronic communications data, even when communication is ancillary, is considered confidential/respected – whether it goes through traditional telecommunications services or other so-called Over-The-Top (OTT) services that are functionally equivalent (e.g. Skype and WhatsApp), which have often become interchangeable with normal telecoms operators for many users.[12] The obligations imposed on service providers – in addition to respecting their clients' privacy choices in the use, storage and processing of their data – also include the obligation of service providers based outside the EU to appoint a representative in a Member State. This will also give Member States the possibility to facilitate law enforcement and judicial authorities' cooperation with service providers to access electronic evidence (see below).

As under the current ePrivacy rules, law enforcement and judicial authorities' access to relevant electronic information necessary for investigating crime will be governed by the exception provided for in Article 11 of the proposed ePrivacy Regulation.[13] This provision gives the possibility in EU or national law to restrict the confidentiality of

---

9 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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. The Directive, in force since 5 May 2016, is to be transposed by Member States by 6 May 2018. The Commission has set up an Expert Group with Member States to exchange views on the transposition of the Police Directive.

10 Regulation on Privacy and Electronic Communications, COM(2017) 10.

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), which will become applicable on 25 May 2018.

12 This follows the approach taken in the proposed Directive establishing the European Electronic Communications Code, presented by the Commission on 14 September 2016 (the Telecoms Package), COM(2016) 590 final.

13 See Article 11(1), the 'data retention clause', which is unchanged from Article 15 of the ePrivacy Directive and aligned with the requirements of the GDPR. Such restriction must respect the essence of fundamental rights and be necessary, appropriate and proportionate.

communication, where necessary and proportionate, in order to safeguard national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This provision is particularly relevant for the national rules on **data retention**, i.e. for obliging telecommunications service providers to keep communications data for a specified period for possible law enforcement access, following the European Court of Justice (ECJ) annulment of the Data Retention Directive in 2014.[14] Since then, there has been no EU instrument for data retention and some Member States have adopted their own national data retention laws. The Swedish and British data retention laws were challenged before the ECJ who rendered its *Tele2* judgment on 21 December.[15] The ECJ found as incompatible with EU law national legislation that, for fighting crime, provides for general and indiscriminate retention of all traffic and location data of subscribers and users relating to all means of electronic communication. The implications of the ruling are being analysed and the Commission will develop guidance as to how national data retention laws can be constructed in conformity with the ruling.

Crime leaves digital traces that can serve as evidence in court proceedings; electronic communications between suspects are often the only lead law enforcement authorities and prosecutors can collect. However, getting access to **electronic evidence** – especially if it is stored abroad or on a Cloud – may be both technically and legally complex and often procedurally burdensome, which hinder investigators' need to move swiftly. To address these challenges, the Commission is currently assessing solutions to allow investigators to obtain cross-border electronic evidence, including making mutual legal assistance more efficient, finding ways of direct cooperation with internet service providers, and to propose criteria for determining and enforcing jurisdiction in cyberspace, in full compliance with applicable data protection rules.[16] The Commission reported to the Justice and Home Affairs Council on 9 December 2016 on progress made.[17]

A comprehensive (and still ongoing) expert consultation process has allowed the Commission to define the various, often complex problems raised by the access to electronic evidence, to gain a better understanding of current rules and practices in the Member States, and to identify possible policy options. The progress report provides an overview of ideas that have emerged thus far during the information gathering and expert process and that the Commission, in consultation with stakeholders, will now look into further in the coming months. As announced in the Commission Work Programme, the Commission will present an initiative in 2017.

---

14 ECJ Judgment in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* of 8 April 2014.

15 ECJ Judgment in Joined Cases C‑203/15 and C‑698/15 *Tele2* of 21 December 2016.

16 As committed in the European Agenda on Security, COM(2015) 185 final, and Commission's Communication on 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.

17 In its Conclusions on improving criminal justice in cyberspace of 9 June 2016, the Council called on the Commission to take concrete actions, develop a common EU approach and to present deliverables by June 2017.

VI. CONCLUSION

The next report due on 1 March will be an opportunity to review the progress on implementation of these and other key work strands.