EUROPEAN COMMISSION

Brussels, 10.01.2017
C(2017) 8 final

Mr Liviu Dragnea
President of the
Camera Deputaților
Palace of the Parliament
Str. Izvor nr. 2-4, sector 5
RO – 050563 BUCHAREST

Dear President,

The Commission would like to thank the Camera Deputaţilor for its Opinion on the Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry {COM(2016) 410 final}.

The Commission notes with satisfaction that the Camera Deputaţilor shares its view that action at the EU level is required to strengthen Europe's cyber resilience system and foster a competitive and innovative cybersecurity industry. Without trust and security, there can be no Digital Single Market. Europe has to be ready to tackle cyber-threats that are increasingly sophisticated and do not recognise national borders.

In this context, the Communication proposes to reinforce cross-border cooperation involving all actors and sectors active in the cybersecurity domain, and to help develop innovative and secure technologies, products and services throughout the European Union. The action plan outlined in this Communication should be seen in the context of the 2015 Digital Single Market strategy[1] and the 2013 EU Cybersecurity strategy[2] as well as the two Directives on Network and Information Security (NIS) and Attacks Against Information Systems[3] (AAIS).

Recognising the urgent need for progress in view of fast evolving cybersecurity challenges, the Commission has already started to implement a number of initiatives outlined in the Communication. The agreement on a cybersecurity contractual Public Private Partnership (cPPP) was signed on 5 July 2016 in Strasbourg. Its governance structure, as well as a number of working groups, have already been established.

1 COM/2015/0192 final
2 JOIN(2013) 1 final
3 Directive (EU) 2016/1148 and Directive 2013/40/EU

The Commission has also already started consulting the Member States and other stakeholders on the possible development of a certification and labelling scheme for Information and Communication Technology (ICT) security products and solutions in Europe. The work leading to the evaluation of the mandate of the European Network and Information Security Agency has already been launched as well.

The Commission intends to regularly update the Member States on the progress made in relation to the various activities announced in the Communication. In response to the more technical comments in the Opinion of the Camera Deputaţilor the Commission would like to refer to the attached annex.

The Commission hopes that these comments address the concerns raised by the Camera Deputaţilor and looks forward to continuing our political dialogue in the future.

Faithfully yours,

Frans Timmermans
First Vice-President

Andrus Ansip
Vice-President

ANNEX

The Commission is pleased to offer additional information, grouped by topic, in relation to the issues raised by the Camera Deputaţilor in its Opinion.

Cybersecurity industrial capacities in the EU and SMEs' opportunities

The Commission shares the Camera Deputaţilor's views regarding the EU's dependence on a limited number of suppliers of operating systems and software. The Commission believes that, while it might not be possible to master the whole value chain of digital technologies in Europe, there is a need to at least retain and develop certain essential capacities in securing these technologies when used in European critical infrastructures. In this context the supply of products and services that provide for the highest level of cybersecurity is an opportunity for the cybersecurity industry in Europe and it could become a strong competitive advantage.

In order for Europe to take advantage of this opportunity it is necessary to foster trust and cooperation between the demand and supply side of cybersecurity products and solutions as well as to support more vigorously start-ups and microenterprises active in the field. The Commission is pleased to see that small and medium-sized entreprises (SMEs) are well represented in the European Cyber Security Organisation – the signatory of the Public Private Partnership contract. The association has also attracted interest from cybersecurity actors in 27 countries – including Romania – ensuring a geographical spread of its activities.

The Commission is committed to working closely with regions to develop Smart Specialisation Platforms as well as with the European Investment Bank and the European Investment Fund to explore opportunities for facilitating access to finance for those SMEs active in the cybersecurity field.

Certification & labelling

The Commission takes due note of the views of the Camera Deputaţilor on certification and labelling of ICT security products and services. The Commission has already started consulting the Member States and other stakeholders in order to develop a roadmap exploring the possibility of creating a European certification framework of ICT security products and services. The Opinion of the Camera Deputaţilor will be made available to the Commission's representatives and other stakeholders active in the process to inform these discussions. This initiative complements the Commission's efforts to develop and standardise security requirements in the field of the Internet of Things, 5G and cloud computing.

Cybersecurity public awareness

The Commission shares the opinion of the Camera Deputaţilor that public awareness of cybersecurity threats and preventive behaviour is an important element of increasing Europe's cybersecurity resilience.

The Commission would like to draw the Camera Deputaţilor's attention to the European Cybersecurity Month – the EU's annual advocacy campaign, organised by the European Network and Information Security Agency and supported by the Commission, that takes place each October and aims to raise awareness of cyber security threats, promote cyber security among citizens and provide up to date security information, through education and sharing of good practices. The Commission encourages all Member States to take an active part in the European Cybersecurity Month and also to use the campaign's materials on other occasions. The 2016 edition resulted in more than 440 awareness raising activities across 31 countries, including Romania.

Furthermore, the Commission would like to point out in general its funding of awareness raising projects, for example in the fields of cyber security and protection of electronic data.

In addition, the Commission supports the work of the cybercrime centres of excellence that have been established throughout the EU in order to foster the relation between academia and law enforcement.

Child prostitution, violent treatment, cyber bullying and terrorism

The Commission shares the Camera Deputaţilor's view that there are links between cybersecurity, attacks on bank accounts and terrorist financing. In this context, there is a strong need to coordinate and foster information sharing among all of the involved actors – including the financial sector, Computer Emergency Response Teams (CERTs) and law enforcement authorities – in order to prevent, mitigate, investigate and prosecute the respective cyber-attacks.

The Commission also shares the opinion of the Camera Deputaţilor that any child sexual abuse, especially when committed with the use of computers, requires a separate and comprehensive approach in fighting cybercrime. Its prevention must be a priority for our society. There is a strong link between strong cyber security and effective law enforcement action against child sexual abuse. Involved stakeholders play a crucial role as well, for instance when it comes to increasing the availability of trained hotlines, improving the skills of the investigating law enforcement officers, or the voluntary engagement of internet service providers. The Commission encourages the work of such stakeholders by providing opportunities for direct exchange and financing for projects. When discussing this subject, it is also necessary to remember that, in addition to facilitating effective investigation of these crimes, it remains equally crucial that everything is done to identify and protect the victims.

The 2011 Directive on combatting the sexual abuse and sexual exploitation of children and child pornography[4] provides an integrated and holistic approach to fight these crimes, encompassing their investigation and prosecution, as well as the assistance and protection of victims, and prevention.

[4] Directive (EU) 2011/93

The Commission agrees with the opinion of the Camera Deputaţilor that the internet can contribute to the expansion of crime, including purchasing weapons for terrorist purposes, and that international cooperation should be enhanced further. The Commission therefore supports the building of capacities which allow effective investigations on traditional offences committed on or with the use of the internet.

In addition to traditional crimes, cyber-attacks constitute a new and expanding type of crime in their own right. At EU level this threat has been addressed by the Directive on Attacks against Information Systems (AAIS) which provides common definitions and minimum standard for criminal liability of persons involved in cyber-attacks. The Directive explicitly addresses attacks against critical infrastructure systems as well as online identity fraud and the use of botnets. Furthermore, the Directive requires EU Member States to implement 24/7 points of contact and thereby facilitates effective international investigative cooperation.

Hybrid threats

The Commission shares the assessment of the Camera Deputaţilor that cyber-attacks can form part of broader 'hybrid' threats – involving a mixture of conventional and unconventional methods used in a coordinated manner by state and non-state actors while remaining below the threshold of formally declared warfare. The objective of this type of action is not only to cause direct damage and exploit vulnerabilities, but also to destabilise societies and create ambiguity to hinder decision-making.

Countering hybrid threats is largely a matter of national competence, as the primary responsibility for national security rests with the Member States. However, the Commission would like to draw the Camera Deputaţilor's attention to the recently adopted Joint Communication[5] setting out a framework for countering hybrid threats, which aims to help EU Member States and their partner countries counter hybrid threats and improve resilience, by combining European and national instruments in a more effective way than in the past.

Incident reporting

The Commission shares the opinion of the Camera Deputaţilor that incident reporting is one of key elements of strengthening cyber resilience in Europe.

The recently adopted Directive on security of network and information systems (NIS Directive) – the first piece of EU legislation on cybersecurity - establishes security requirements and incident notification obligations for the operators of essential services as well as for certain digital service providers. While it remains Member States' competence to structure incident reporting, the Commission hopes for fruitful cooperation among Computer Security Incident Response Teams within the CSIRTs network established by the NIS Directive. The work done under the Connecting Europe Facility Telecom programme on cybersecurity Digital Services Infrastructure may help to develop and deploy common cybersecurity incident management tools.

[5] JOIN(2016) 18 final http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

At the same time the Commission is committed to supporting bottom-up initiatives such as the sectorial Information Sharing and Analysis Centres to encourage information sharing between industry peers that can help increase the cyber resilience of different sectors.