Council of the European Union

Brussels, 4 December 2017
(OR. en)

14965/17

CYBER 190
TELECOM 320
ENFOPOL 576
JAI 1116
MI 883
COSI 306
JAIEX 105
RELEX 1033
IND 339
CSDP/PSDC 673
COPS 377
POLMIL 155

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. prev. doc.:	14435/17 + COR 1
No. Cion doc.:	12211/17, 12210/17
Subject:	Draft Action Plan for implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - approval

1. At the meeting of the Horizontal Working Party on Cyber Issues ("HWP Cyber") of 26 September 2017 the Commission presented its cybersecurity package, including inter alia a Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[1]. A political response to the initiatives outlined in that Joint Communication were set in Council Conclusions adopted on 20 November 2017[2].

[1] doc. 12211/17.
[2] doc. 14435/17 + COR 1.

2. The European Council of 19 October in its conclusions[3] stipulated that "Commission's cybersecurity proposals should be developed in a holistic way, delivered timely and examined without delay, on the basis of an action plan to be set by the Council".

3. On this ground and in view of the outcome of the policy debate on cybersecurity held during the TTE Council of 24 October 2017, the Presidency discussed during the HWP Cyber of 6 November 2017 the approach and the possible structure of such an action plan.

4. In addition the Presidency organised an informal meeting to exchange views with delegations on the scope and content of future action plan on 13 November 2017.

5. On the basis of that input a draft action plan[4] was elaborated and sent to delegations for written comments. The latter allowed refinement of the initial draft and a revised version of it was presented and discussed at the HWP Cyber meeting of 29 November 2017. A number of additional comments and contributions were provided by delegations . They allowed to complete the negotiations at the working party level and to prepare the final compromise text[5].

6. The draft Action Plan is envisaged to remain a vehicle for horizontal monitoring and follow-up of the Council Conclusions implementation. Therefore the progress achieved would be regularly reviewed by the incoming Presidencies and presented to the Horizontal Working Party on Cyber Issues for information and discussions.

7. On this basis, COREPER is requested to invite the Council to approve the draft Action plan for implementation of the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, as set out in the Annex.

---

3 doc. EUCO 14/17.
4 WK 13046/17.
5 WK 13046/2/17 REV2.

The present draft Action Plan for implementation of the Council Conclusions on "Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" is a strategic-level document resulting of the tasking by the European Council of 19 October 2017 and the Council of 24 October 2017. As indicated within those Council Conclusions of 20 November 2017, the Action Plan is a living document and as such will be regularly reviewed and updated by the Council. It is envisaged as a tool for horizontal oversight and strategic follow-up of the implementation of the Council Conclusions and of the actions detailed below.

Action[6]	**Lead / primarily responsible**	**Stakeholders and/or other involved Parties**	**Deadline**	**Progress**	**Notes/Comments**
Ensuring full and effective transposition and implementation of the NIS Directive					
Transposition and implementation of the NIS Directive	Member States; European Commission		May 2018	Progress summarized by Commission and discussed within the Cooperation Group	
Ensuring effective strategic cooperation between the Member States within the Cooperation Group	Member States / Presidency of the Council	European Commission, ENISA		Progress summarised within the regular report of the Cooperation Group	Work of Cooperation Group elaborated in more detail within the biennial work programme of the Group

[6] Where relevant, implementation of actions takes into account the resources within the MFF.

Achieving a full operational capability of CSIRTs Network	Member States / Presidency of the Council	ENISA, European Commission		Progress achieved summarized within the regular report of the Network to the Cooperation Group	
Enhancing EU level response to large-scale cyber incidents by conducting regular pan-European cybersecurity exercises					
Conducting cyber diplomacy exercises on the usage of the Joint Diplomatic Framework against malicious cyber activities	EEAS	Member States, European Commission and ENISA		Successive Presidencies of the Council, discussions on exercising of the Framework have started during the EE Presidency	
Conducting regular CYBER EUROPE exercises	Presidency together with Member States	Member States, including the CSIRTs Network, ENISA, EEAS, European Commission			Frequency formulated in the tasking within the mandate of ENISA and during the discussions of the ENISA MB

Conducting regular strategic cybersecurity exercises in different Council formations	Presidency	supported by EEAS and/or European Commission		EU CYBRID 2017 conducted under the EE Presidency for FAC(D)	Regularity defined by Member States within the Council
Adoption by co-legislators of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")[7]					
Conducting in-depth discussions of the legislative proposal in HWP leading to a General Approach	BG Presidency		June 2018	Examination of the Proposal conducted by the EE Presidency	
Finalizing negotiations between the co-legislators	AT Presidency		December 2018		Indicative deadline

[7] Implementation takes place without prejudice to the competences of the European Parliament.

Establishing the Network of Cybersecurity Competence Centres (NCCC) with a European Cybersecurity Research and Competence Centre					
Delivering an impact assessment and budget forecast and relevant legal instruments for the establishment of the Network of Cybersecurity Competence Centres (NCCC) with a European Cybersecurity Research and Competence Centre	European Commission	Member States, EEAS, EDA	June 2018		Further steps upon the delivered instruments to be decided by Member States within the Council
Launching a pilot phase under Horizon 2020	European Commission	Member States, NIS Cooperation Group	end of 2018/early 2019		

Developing a European capacity for evaluating the strength of cryptography used in products and services available for citizens, businesses and governments within the Digital Single Market	Member States		2019		
Ensuring sufficient funding to support building cyber resilience and cybersecurity research and development efforts across the EU					
Ensuring sufficient financing for cybersecurity while respecting the available resources	Member States, European Commission		2020		

Enhancing public sector contributions to build cyber resilience and strengthen cybersecurity research and development efforts	Member States		2020		
Incentivizing private sector investments to build cyber resilience and strengthen cybersecurity research and development efforts	European Commission	supported by ECSO	2018		
Increasing investments into cybersecurity applications of new technologies	European Commission, Member States	supported by ECSO	2020		

Examining a possible proposal for establishment of a Cybersecurity Emergency Response Fund	Council[8]				Any consideration takes place only if proposal presented by European Commission
Keep sufficient funding for cybersecurity efforts within exiting instruments and agreed programmes	Member States, European Commission	EIB	2020		

[8] Without prejudice to competences of the European Parliament as appropriate.

Providing credible, trusted and coordinated cybersecurity services and their governance for the EU institutions					
Clarifying and harmonising the cybersecurity governance of the EU Institutions, bodies and Agencies	Council, European Commission and EEAS	EU Institutions, bodies and Agencies	2020	Report should be presented to the HWP on Cyber issues on the governance and the progress made thereof	
Ensuring adequate resources and support for the development of CERT-EU	EU Institutions, bodies and Agencies		2020	CERT-EU regularly reports to HWP Cyber on cyber threats to its constituency. Resourcing of CERT-EU can be raised within the relevant HWP Cyber discussions	
Increasing emphasis on cyber awareness, digital skills, education and training					
Enhancing cyber-awareness campaigns in Member States	Member States	ENISA	2020		

Enhancing cybersecurity in the curricula of academic, educational and vocational training programmes	Member States	European Commission, ECSO	2020	Progress tracked by Member States and European Commission	
Establishing a network of education points of contact (POCs)	Member States	ENISA	2020		
Mainstreaming and enhancing cybersecurity traineeship programmes	Member States	European Commission, ECSO	2020		
Providing cybersecurity-related awareness in public administration that participate in critical societal or economic activities	Member States		2020	Cyber Hygiene pledge signed by six Member States, EEAS and EDA in May 2015	

Strengthening the EU capacity to prevent, deter, detect and respond to malicious cyber activities					
Mainstreaming cybersecurity into existing crisis management mechanisms at the EU level	European Commission, Council	EEAS,EU Agencies	2018		
Adequately addressing cybersecurity incident response in the National Crisis Management mechanisms as well as provide necessary procedures for cooperation at EU level	Member States		2018		
Updating EU Cyber Defence Policy Framework	Member States, EEAS,EDA, European Commission		2018		
Encouraging cooperation between civilian and military cyber incident response communities	Member States				

Putting in place a cyber defence training and education platform	European Commission	EEAS, EDA, ESDC	end of 2018		
Taking full advantage of proposed defence initiatives to accelerate the development of cyber defence capabilities in EU	Member States	EEAS,EDA, European Commission			Cyber defence projects can be developed through PESCO, if deemed necessary by PESCO participating Member States. EDF can finance cyber projects if foreseen in the working programmes

Strengthening the fight against crime in and removing obstacles to effective criminal justice in cyberspace					
Developing a roadmap to countering the evolving criminality on the Dark Web	Europol	Member States	early 2018	Roadmap to be endorsed and implementation monitored by COSI	
Implementing practical measures proposed by Commission to tackle the challenge of encryption in the context of criminal proceedings while ensuring the respect of human rights and fundamental freedoms.	European Commission	Member States, Europol	ongoing	Progress monitored by CATS	

Improving the capability of law enforcement and judicial authorities to investigate and prosecute crime	Member States	European Commission		Progress monitored by COSI, voluntary codes of conduct with Internet Access Providers to be proposed to limit the number of subscribers behind each IPv4 by deploying alternative technologies to Carrier-Grade NAT (Member States). European Commission to raise the issue of source port number logging with the Internet Content Providers in the EU Internet Forum.	Taking into account the recommendations of the GENVAL final report on the 7th round of mutual evaluation on fighting cybercrime

Incentivizing the private sector deployment of IPv6, e.g. through possible introduction of requirements in public procurements	Member States	European Commission	ongoing	Progress to be monitored by relevant Council preparatory bodies (HWP Cyber, COSI)	
Developing and endorsing an Emergency Response Protocol for a coordinated EU law enforcement response to large-scale cyber incidents.	Europol	Member States, European Commission, EEAS, Council	early 2018	The Protocol to be endorsed and implementation monitored by COSI	
Delivering a legislative proposal on facilitating the cross-border access to e-evidence by the law enforcement authorities	European Commission	Council, European Parliament	early 2018	Progress monitored by CATS	

Presenting a progress report on the implementation of the practical measures for improving the cross-border access to electronic evidence (including cooperation between law enforcement authorities and private sector service providers)	European Commission	Member States	End of 2017	Progress monitored by CATS	
Creating a fully functional platform for the Members States to exchange securely European Investigation Order online forms and e-evidence.	European Commission	Member States	mid-2019	Progress monitored by CATS	

Strengthening international cooperation for an open, free, peaceful and secure global cyberspace					
Continuation of dialogue with international partners to influence global support for an open, free, peaceful and secure cyberspace	EEAS, Council, European Commission	Member States	Mid-2019	Progress monitored by HWP Cyber	
Developing an EU Cyber Capacity Building Network and EU Cyber Capacity Building Guidelines	EEAS, European Commission, with support from Member States				Possible cooperation with GFCE
Developing EU-NATO cooperation in training and education	EEAS, Council, EDA	Member States,			
Continuing of EU-NATO cooperation on cyber defence exercises and sharing good practices on crisis management	EEAS, Council	Member States, EDA, European Commission			

Addressing the critical cyber security applications of novel technologies in relevant international export control regimes	Member States, European Commission				
Developing and communicating a consolidated EU position on global internet governance discussions.	Council, European Commission, EEAS	Member States	2018 and ongoing	COSI to facilitate the adoption of a common EU position on a GDPR compliant WHOIS system, which will ensure timely and swift access to accurate Registration information on domain names and IP addresses owners (WHOIS data) for legitimate purposes including law enforcement, consumer protection, intellectual property rights protection, and cybersecurity activities.	