Council of the
European Union

Brussels, 11 May 2017
(OR. en)

8901/17

LIMITE

POLGEN 62	**IND 119**
JAI 413	**COTER 35**
TELECOM 115	**ENFOPOL 228**
PROCIV 43	**DROIPEN 60**
CSC 95	**CYBER 69**
CIS 7	**COPS 153**
RELEX 393	**POLMIL 51**
JAIEX 41	**COSI 98**
RECH 131	**DATAPROTECT 95**
COMPET 333	**CSDP/PSDC 241**

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	5776/2/16 REV 2
Subject:	EU Cybersecurity Strategy Roadmap - finalisation

1. The Roadmap was put in place in the second half of 2013 by the LT Presidency as a tool to support the implementation of the 2013 EU Cybersecurity Strategy. Throughout the years it has been regularly updated to reflect the progress on the respective actions.

2. Under the NL Presidency it was seriously restructured to take into account all the relevant instruments shaping the cyber policy as well as the related actors and cyber-related initiatives within other than the HWP on Cyber Issues Council Preparatory Bodies.

3. In view of the process launched recently by the Commission and EEAS to review the 2013 Strategy the Presidency has prepared an update of the Roadmap cross-checking the respective actions against their current state of play.

4. The Presidency would like to invite delegations to:

- take note of the updated version of the Roadmap;

- consider its future status in view of the upcoming new Cybersecurity strategy and its respective implementation.

ANNEX I

CYBER-RELATED INITIATIVES WITHIN THE HORIZONTAL WORKING PARTY ON CYBER ISSUES[1]

ROADMAP			
Work Strands	**ACTIONS**	**PROGRESS**	**Notes for reflection**
A. Values and Prosperity			
1. Defend a unified and strong position regarding the universal applicability of human rights and fundamental freedoms (§16)	**International Human rights Law in cyberspace**		**Action in multilateral fora UNGA 3C/ UNHRC**
2. Promote and protect values and interests within the Union and its external policies related to cyber issues (§15)	**Due diligence in cyberspace**		
3. Ensure that all EU citizens are able to access and enjoy benefits of the Internet (§ 19)	**DSM implementation**		
4. Cybersecurity is key to protecting the digital economy (§ 23.3)	Council Conclusions on Strengthening the Europe's Cyber Resilience		

[1] New actions in comparison to the previous version have been marked with **Bold** and *Italic*, ongoing actions - with **Bold**, whereas the completed ones bear no marking.

B. Achieving Cyber Resilience			
1. Proposal for a Directive laying down measures to enhance network and information security across the EU (§ 24)	CSIRT network and Cooperation Group		**Ensure collaboration between CSIRT network, CERTs and cyber LEA at national and EU level**
2. Take steps to ensure an efficient national level of Cybersecurity by developing and implementing proper policies, organizational and operational capacities in order to protect information systems in cyberspace, in particular those considered to be critical (§ 29.1)	**NIS Directive**: **Overview of PPP platforms in the EU - lead & coordination**		**Tasking**
3. Engagement with industry and academia to stimulate trust as a key component of national cybersecurity for instance by setting up PPP (§ 29.2)	cPPP on cybersecurity	Launched on 5 July 2016	**Optimise the use of existing public-private cooperation networks, such as EC3 coordinated Academic advisory network, and the Advisory Groups on Internet Security, Financial Service and Communication providers**
4. Support awareness raising on the nature of the threats and the fundamentals of good digital practices, at all levels (§ 29.3)	Cyber Hygiene Initiative[1]	Signed (18/5/2015) pledge to mitigate human-related risks in the cyberspace by LV, LT, EE, FI, AT, NL and launched the Cyber Hygiene Initiative.	**EC3 Cybercrime Prevention and Awareness Raising Programme**

5. Foster pan-European cybersecurity cooperation, in particular by enhancing pan-European cybersecurity exercises (§ 29.5)	International cyber exercises calendar		**Ensure the involvement of NIS entities, LEA and judiciary in such exercises in cooperation with ENISA, Europol and Eurojust**
6. Cybersecurity issues in light of ongoing work on the solidarity clause (§ 29.8)	***EU PACE 2017 (cyber component)***		
7. All EU institutions, bodies and agencies, in cooperation with MS to take the necessary action to ensure their own cybersecurity, by reinforcing their security according to the appropriate security standards (§ 25)	**Support CERT-EU as the shared security and incident response capacity of the EU institutions, agencies and bodies**		**Cooperation between Europol and CERT-EU**

C. Cybercrime			
1. Use of EC3 as a means of strengthening cooperation between national agencies within its mandate (§ 32)			
2. Strengthen cooperation of Europol (EC3) and Eurojust with all relevant stakeholders (§ 33)			
3. Operational capability to effectively respond to cybercrime (Strategy)	**Solutions to the legal gaps/ obstacles to cybercrime investigation/prosecution, as well as development of tools for mitigating technical challenges and responding to the newly emerged operational needs of MS**		
4. Swift ratification of the Budapest Convention on Cyber Crime by all MS (§ 34)	**Ratification by the three outstanding MS**		**Update**
5. Support training and up-skilling of MS whose governments and law enforcement authorities need to build cyber capabilities to combat cybercrime (§ 35)	Council Conclusions on Strengthening the Europe's **Cyber Resilience Training Competency Framework and Training Needs Analysis (EC3, ENISA, ECTEG, CEPOL, DG HOME), Freetool Project, EC3 signature courses**		

6. Use the Instrument contributing to Stability and Peace (IcSP, formerly Instrument for Stability (IfS)) to develop the fight against cybercrime (…) in third countries from where cybercriminal organisations operate (§ 36.3)			
7. Need for strong and effective legislation to tackle cybercrime (Strategy)	***Prevention/Awareness raising*** **Data retention** **E-evidence** **MLA** **Encryption** **Online investigation powers** **Cryptocurrencies** **Due diligence**		
* ISS Implementation	**R&D contribution to the fight against cybercrime**		

D. CSDP			
1. Develop a cyber defence framework (§ 37.1)	***EU PACE 2017 (cyber component)***		
2. Enhance MS's cyber defence capabilities (§ 37.2)	***EU PACE 2017 (cyber component)***		**Optimise the use of existing public-private cooperation networks, such as the EC3 coordinated academic advisory network, and the Advisory Groups on Internet Security, Financial Service, Communication Providers as we as MoUs-based collaboration with private partners towards combating cybercrime**
3. Develop cyberdefence capability concentrated on detection, response and recovery from sophisticated cyber threats (Strategy)	***Draft Council Conclusions on a Joint EU response to malicious cyber activities***		
4. Using the existing mechanisms for pooling and sharing and utilising synergies with wider EU policies (§ 37.3)			
5. Develop secure and resilient technologies for cyber defence and to strengthen cybersecurity aspects in EDA research projects (§ 37.4)			
6. New cyber threats (§ 37.5)	Hybrid Threats		
7. EU-NATO cooperation on cyber defence (§ 37.6)	Tallinn Manual 2.0		

E. Industry and Technology			
1. Necessity for Europe to further develop its industrial and technological resources to achieve an adequate level of diversity and trust within its networks and ICT systems (§ 38)	**Cyber security labels** **Certification** **Standardisation**		
2. Development of public-private partnerships, as a relevant instrument to enhancing cybersecurity capabilities (§ 40)	cPPP on cybersecurity	Launched on 5 July 2016.	

F. International Cyberspace Cooperation			
1. Improving coordination of global cyber issues and mainstreaming cybersecurity including confidence and transparency building measures into the overall framework for conducting relations with third countries and with international organisations (§ 45.2)	**Implementation Second set of CBMs**		
2. Budapest Convention as a model for drafting national cybercrime legislation (§ 44.1.a)			
3. Develop common EU messages on cyberspace issues (para.44.2	**EU Positions in international fora, e.g. follow-up to the Hague Conference**		
4. Strengthen CIIP cooperation networks (Strategy)	**International mechanisms for info sharing and policy coordination**		
5. Developing capacity building on cybersecurity and resilient information infrastructures in third countries (Strategy)	**Global Forum on Cyber Expertise**		**Definition of cyber capacity building?** **Mapping of the cyber capacity building iniatives?**

ANNEX II

CYBER-RELATED INITIATIVES WITHIN THE OTHER COUNCIL WORKING PARTIES

WP	INITIATIVE	RELEVANT DOCs	DATE
CCWP	7th Action Plan, reflective of the EU Policy Cycle:	12468/7/13 REV 7	
	Action 7.3 "To examine the working/investigative techniques applied by customs and other law enforcement authorities to combat customs related crime, including organized crime, through the Internet, and to explore the current situation regarding the existence of customs specialised units dealing with those crimes and to ensure follow-up to Action 5.2. Action implements MASP related to EU crime Priority "Cybercrime" (12759/3/13 REV 3)"	5751/1/14 (mandate) 9023/16 + COR 1 (final report)	Adopted on 1/06/2016
	8th Action Plan:	13749/3/15 REV 3	
	8.1. Illegal trade via Internet /small consignments; 8.2. Customs against internet crime (C@iC - extension of Action 7.3)	9021/2/16 REV 2 (mandate for 8.1) 7448/2/16 REV 2 (mandate for 8.2)	
GENVAL	7th Round of Mutual Evaluation on prevention and fight against cybercrime: - Questionnaire	5335/1/14 REV 1	
	Adoption of FR and NL reports	7587/15 DCL 1 (NL) 7588/2/15 REV 2 DCL 1 (FR)	24/06/2015
	Discussion of the UK visit report, adoption of SK report	9761/1/15 REV 1 DCL 1 (SK)	15/09/2015
	Discussion of the RO visit report, adoption of UK report	10952/2/15 REV 2 DCL 1 (UK)	29/10/2015
	Discussion of the EE and BG visit reports, adoption of RO report	13022/1/15 REV 1 EU REST (RO)	03/02/2016
	Discussion of the ES and LT visit reports, adoption of EE and BG reports	10953/15 DCL 1 (EE) 5156/1/16 REV 1 DCL 1 (BG)	16/03/2016

	Discussion of the MT visit report, adoption of ES and LT reports	6289/1/16 REV 1 DCL 1 (ES) 6520/1/16 REV 1 DCL 1 (LT)	27/04/2016
	Discussion of the CY and IT visit reports, adoption of MT report	7696/1/16 REV 1 DCL 1 MT)	24/06/2016
	Discussion of the PT visit report, adoption of CY and IT reports	9892/1/16 REV 1 DCL 1 (CY) 9955/1/16 REV 1 DCL 1 (IT)	20/07/2016
	Discussion of the DK visit report, adoption of PT report	10905/1/16 REV 1 (PT)	26/10/16
	Discussion of SI, PL, HU, CZ, EL visit reports, adoption of DK report	13204/1/16 REV 1 DCL 1 + COR 1 DCL 1 (DK)	14/12/16
	Discussion of HR, LV visit reports, adoption of EL, CZ, HU, SI, PL reports	14584/1/16 REV 1 DCL 1 (EL) 13203/1/16 REV 1 DCL 1 (CZ) 14583/1/16 REV 1 DCL 1 (HU) 14586/1/16 REV 1 DCL 1 (SI) 14585/1/16 REV 1 DCL 1 (PL)	03/02/17
	Discussion of LUX, IE, DE visit reports, adoption of HR, LV reports	5250/1/17 REV 1 DCL 1 (HR) 5387/1/17 REV 1 DCL 1 (LV)	07/04/2017
	Discussion of BE, AT, SV visit reports, adoption of LUX, IE, DE reports	7162/1/17 REV 1 (LUX) 7160/1/17 REV 1 (IE) 7159/1/17 REV 1 (DE)	05/05/2017

E-Justice	E-evidence/E-CODEX	CM 1189/1/17 REV 1 CM 2098/2/17 REV 2	31/01/2017 30/03/2017
PMG	EU Cyber Defence Policy Framework	15585/14 (adopted FAC)	07/11/2014 (agreed)
	Six-Month report on the EU Cyber Defence Policy Framework Implementation	10347/15	26/06/2015 (agreed)
	Second Six-Month report on the EU Cyber Defence Policy Framework Implementation	13801/15	9/11/2015 (agreed)
	Third Six-Month report on the EU Cyber Defence Policy Framework Implementation	9701/16	31/05/2016 (finalised)
	Technical Arrangement between NCIRC and the CERT-EU Cyber Defence	MD 005-16	10/02/2016 11/04/2016
	Council conclusions on countering hybrid threats	7857/16 (adopted FAC)	
	Exercise Specifications for the EU Parallel and Coordinated Crisis Management Exercise 2017 – EUPACE17	8809/17	04/05/2017
PSC	Discussion and conclusions on Developing a joint EU diplomatic response against coercive cyber operations	5797/6/16 REV 6 WK 2569/2017 INIT	23/06/2016 14/03/2017
LEWP	Findings and recommendations of Europol's iOCTA	12728/15	23/10/2015
COTRA	EU-US Cyber Dialogue (1st - 5/12/2014, Brussels; 2nd -7/12/2015,Washington, DC, 3rd - 16/12/2016) - ToR - debriefing	8266/14 (§15) COREU (EAS/1397/14) COREU (EAS/1194/15) COREU (EAS/0035/17)	17/11/2015 01/12/2015 15/12/2015

COASI	EU-Japan Cyber Dialogue (1st- 06/10/2014, 2nd - 25/1/2017)	COREU 1140/14 COREU EAS/0159/17	
	COASI-ASEAN Regional Forum - Workshop on Cyber Confidence Building Measures, Kuala Lumpur, 25-26 March	COREU 0433/14	
	Sino-European track-two cyber dialogue, Geneva 31/3-01/04/2014	CORUE 0442/14	
	COASI-ASEAN Regional Forum - Workshop on Cyber Confidence Building Measures, Kuala Lumpur, 25-26 March	COREU 0433/14	
	3rd EU-China Task Force (held on 21/11/2014) 4th EU-China Cyber Task Force (held on 3/12/2015 in Brussels)	COREU EAS/1372 COREU EAS/1176/15	
	EU-Republic of Korea Cyber Dialogue (held on 30/04/2015)	COREU EAS/0506/15	
	EU-India Cyber Dialogue (held on 21/05/2015)	COREU CFSP/EAS/0547/15	
	4th EU-China Cyber Taskforce (held on 3/12/2015)	COREU EAS/1176/15	
	EU-Republic of Korea Cyber Dialogue (held on 16/6/2016)	COREU EAS/0605/16	
COLAC	EU-Brazil Cyber Dialogue (ToR adopted through silence procedure)	COLAC 8/16 COREU EAS/0217/16	
DAPIX	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)	5455/15 (political agreement) Adopted	8/04/2016
	Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, which is intended to replace the 2008 Data Protection Framework Decision	5463/16 (political agreement) Adopted	8/04/2016
	Data retention	CM 2168/17 + 7597/17 CM 2677/17 + 8798/17	10/04/2017 15/05/2017
FREMP	Code of Conduct on countering illegal hate speech online - implementation follow-up and support to COM / FRA initiatives related to hate speech online		

TELECOM	Proposal for a Directive of the EP and of the Council concerning measures to ensure a high common level of network and information security across the Union	6342/13 (COM) 15229/2/15 (endorsement Coreper) 5894/16 (political agreement) Adopted	18/12/2015 17/02/2016 6/07/2016
	Council Conclusions on Internet Governance Commission Information Note on Internet Governance	16200/14 15009/15	27/11/2014
	World Summit on the Information Society+ 10 ("WSIS+10") Review Process (held on 15-16/12/2015) - Lines to take (LTT)(discussed also in CONUN) - outcome	9334/15 (approved Coreper) 15419/15	03/06/2015
	Council Conclusions on the transfer of the stewardship of the Internet Assigned Numbers Authority (IANA) functions to the multistakeholder community	9482/1/15 REV 1	12/06/2015
	Council Conclusions on World Radio-communication Conference 2015 (WRC-15) of International telecommunication Union (ITU)	13460/15	26/10/2015
	Council conclusions on e-Government Action Plan 2016-2020: Accelerating the digital transformation of government	12359/16	20/9/2016
	Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code	12252/1/16	14/9/2016
	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)	5358/17	12/1/2017
	Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of Internet connectivity in local communities	12259/16	14/9/2016
	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Interoperability Framework – Implementation Strategy	7791/17	23/03/2017

CODEV	Council Conclusions on mainstreaming digital solutions and technologies in EU development policy	14682/16	28/11/2016
COHOM	EU Human Rights Guidelines on Freedom of Expression Online and Offline - implementation update	9647/14 (adopted FAC)	7/10/2015
	Council conclusions on the Action plan on human rights and democracy 2015 - 2019	10897/15	
	Council Conclusions on EU Priorities at UN Human Rights Fora in 2016	6012/16	15/2/2016
	Council Conclusions on EU Priorities at UN Human Rights Fora in 2017	5689/17	27/02/2017
IPCR FOP	Crisis Response 2014 exercise (27/11/14) (cyber was the main trigger of the crisis)	15776/14 (instructions) 17032/14 (outcome)	
COSI	EU ISS implementation	5645/2/17 REV 2 + COR 1	14/03/2017
	Policy Cycle (2014-2017) - cybercrime one of the 9 EU crime priorities	12095/13	
	Multi Annual Strategic Plans (MASP)	12759/3/13 REV 3	
	Operational Action Plan (OAP) CSE 2017	15232/1/16 REV 1EU REST	
	OAP Card Fraud 2017	15231/1/16 REV 1 EU REST	19/12/2016 (adopted)
	OAP Cyber Attacks 2017	15233/1/16 REV 1 EU REST	
	OAP 2016 Progress Reports on CSE, Card Fraud and Cyber Attacks	6563/17 EU REST 6562/17 EU REST 6564/17 EU REST	
	Continuation of the EU Policy Cycle for the period 2018-2021	7740/17 (adopted by Council)	27/03/2027
	EU Internet Forum		19/12/2016
	Effective operational cooperation in criminal investigations in cyberspace	8634/2/16 REV 2	17/05/2016

CATS/JHA Counsellors	E-evidence in criminal proceedings in cyberspace	13689/15 14369/15 (discussion in Council)	11/12/2015
	Council Conclusions on the European Judicial Cybercrime Network	10025/16 (Adopted JHA Council)	9/06/2016
	Council Conclusions on improving criminal justice in cyberspace	10007/16 (Adopted JHA Council)	9/06/2016
EUMC	Discussions on the EDA's Evaluation of the Results of the Feasibility Assessment for an EU Cyber Defence Centre / Capability for CSDP	EEAS (2016) 754 REV 2	
	Draft EU Concept on Cyber Defence for EU-led Military Operations and Missions		Expected approval in October
Security Committee	Information Assurance Security Policy on Network Defence Information Assurance Security Guidelines on Boundary Protection Services Information Assurance Security Guidelines on Network Defence Information Assurance Security Guidelines on Intrusion Prevention and Detection Information Assurance Security Policy on Interconnection	8408/12 13909/12 (R-UE/EU-R) 9650/15 7867/15 6488/15	
Competitiveness and Growth	Council Conclusions on Single Market Policy	6197/15 (adopted Competitiveness Council)	
	Council Conclusions on the Digital transformation of European industry	9340/15 (adopted Competitiveness Council)	
Research	Council Conclusions on Open, data-intensive and networked research as a driver for faster and wider innovation	9360/15 (adopted by the Competitiveness Council)	
CONUN	World Summit for Information Society+10 Review Process - Lines to take - outcome	9334/15 (approved COREPER) 15419/15	
	EU Priorities at the United Nations and the Seventieth United Nations General Assembly	10158/15 (adopted FAC)	

Inter-institutional Steering Board CERT-EU [2]	New mandate, service catalogue; information sharing and exchange framework	6738/15	
COM Informal groups	NIS Platform - Cooperation Group and CSIRT network H2020 - Programme Committee for Secure Societies High level group on Internet Governance High level group on Cybercrime and cybersecurity High Level Group on combating racism, xenophobia and other forms of intolerance		

[2] Not a formal Council preparatory body.