COUNCIL OF THE EUROPEAN UNION

Brussels, 7 May 2014 (OR. en)

9298/14

LIMITE

POLGEN 60	**IND 152**
JAI 290	**COTER 24**
TELECOM 110	**ENFOPOL 129**
PROCIV 42	**DROIPEN 68**
CSC 98	**CYBER 23**
CIS 2	**COPS 113**
RELEX 382	**POLMIL 49**
JAIEX 35	**COSI 39**
RECH 183	**DATAPROTECT 67**
COMPET 264	

NOTE

From:	Presidency
To:	Delegations
Subject:	Road map development - examination

Delegations will find in the Annex a working version of the road map developed by the Presidency on the basis of the UK proposal and delegations' comments. The delivery dates mentioned therein are only indicative at this stage and would be further elaborated with the upcoming Presidency.

ANNEX

ROADMAP				
Field/ Work Strands	**ACTIONS**	**PROGRESS**	**DELIVERY DATE**	**Lead/ Other Actors**[1]
A. Values and Prosperity				
1. Defend a unified and strong position regarding the universal applicability of human rights and fundamental freedoms (para. 16)	• Update on the progress of negotiations of the Data Protection Regulation	DAPIX WG continues the examination with a view to a timely conclusion of the negotiations with the EP	**2015**	**Presidency (lead)** MS
	• Update on the progress of negotiations of the New Data Protection Directive in the law enforcement sector			**Presidency (lead)** MS
	• Timeline for implementation of the Guidelines of Freedom of expression online and update on progress	Adopted in April 2014 by COHOM	**December 2014**	**EEAS/COHOM (lead),** MS, COM
2. Promote and protect values and interests within the Union and its external policies related to cyber issues (para. 15)	• Develop (contribute to the development of) Council Conclusions on Internet Governance	June Telecom Council will hold a discussion on the IG follow-up	**Open**	**Presidency (lead)** EEAS, COM

[1] Within their competences and legal mandates.

3. Ensure that all EU citizens are able to access and enjoy benefits of the Internet (para. 19)	• Update on use made of the funds available under the Connecting Europe Facility for broadband roll-out		**Open**	**COM (lead)**
4. Cyber security is key to protecting the digital economy (para. 23.3)	• Promote and maintain a high level of network and information security		**Open**	**MS (lead)** COM
	• Update on the status of the Electronic Identification and other Trust Services Regulation, including the timetable for adoption	This has been informally agreed at the 4th trilogue	**July 2014**	**Presidency**
	• Examine whether outputs from the NIS Platform could be implemented to improve MS resilience		**December 2014**	**COM (lead)** MS

B. Achieving Cyber Resilience				
1. Proposal for a Directive laying down measures to enhance network and information security across the EU (para. 24)	• Update on the progress of negotiations	TELECOM WG continues the examination with a view to a timely concluding of the negotiation with the EP	**July 2014** **October 2014** **December 2014**	**Presidency (lead)** MS
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 (para. 29.1)	• Review the status of their own Cybersecurity Strategies and report on implementation progress, with support from ENISA, where appropriate		**September 2014**	**MS (lead)** Presidency, ENISA
	• Update on status of EU Institutions' Cyber Resilience		**September 2014**	**CERT-EU (lead)**
	• Examine whether outputs from the NIS Platform could be used to improve MS network resilience.		**December 2014**	**COM (lead)** Presidency, ENISA

3. Engagement with industry and academia to stimulate trust as a key component of national cybersecurity for instance by setting up PPP (para. 29.2)	• Report on the status of public-private partnerships, in particular involvement of industry and academia		**November 2014**	**MS (lead)** Presidency
	• Update on the work undertaken under Horizon 2020		**October 2014**	**COM (lead)** MS
	• Further development of the European Public-Private Partnership for Resilience (EP3R) as a sound and valid platform at EU level		**September 2014**	**COM (lead)** MS, ENISA
	• Identify and assess the technical obstacles to coordination			
	• Report on the EP3R future		**December 2014**	

4. Support awareness raising on the nature of the threats and the fundamentals of good digital practices, at all levels (para. 29.3)	• Organise a “Cybersecurity month” • Report on outcome	ENISA invited parties to express interest in taking part	**October 2014** **December 2014** (on outcome)	**ENISA, MS, private sector** **(joint lead)**
	• Organise a "Cybersecurity championship", where university students will compete in proposing NIS solutions • Update on progress of preparation/outcome	ENISA is organising a workshop to share ideas on 29/4/14	**September 2014** (on preparation) **December 2014** (on outcome)	**COM, ENISA (joint lead)**
5. Foster pan-European cybersecurity cooperation, in particular by enhancing pan-European cybersecurity exercises (para. 29.5)	• Present suggestions how to take this issue forward	ENISA is currently planning with MS and EFTA countries 3rd pan-European Exercise - Cyber Europe 2014	**December 2014**	**Presidency, ENISA, MS (joint lead)**
6. Cybersecurity issues in light of on-going work on the solidarity clause (para 29.8)	• Report progress on the adoption of Council Decision on arrangements for the implementation by the Union of the Solidarity Clause	Last version (doc. 18145/3/13) will be discussed in FoP IPCR/SCI	**July 2014**	**Presidency (lead)** MS

C. Cybercrime				
1. Use of EC3 as a means of strengthening cooperation between national agencies within its mandate (para. 32)	• Report progress on EC3 - MS cooperation, setting out areas that work well and those that may require further consideration		**January 2015**	**Presidency (lead)** on the basis of MS/EC3 input
2. Strengthen cooperation of Europol (EC3) and Eurojust with all relevant stakeholders (para. 33)	• Align cybercrime policy approaches with best practice on the operational side	EU Policy Cycle	**ongoing**	**Presidency (lead)** Europol/EC3, Eurojust COM
	• Identify obstacles to cooperation and means for their overcoming		**ongoing**	
	• Report progress		**October/ December 2014**	
3. Operational capability to effectively respond to cybercrime (Strategy)	• Update progress on development of adequate digital forensic tools and technologies in view of evolving cybercrime	Info will be obtained in the framework of the 7th evaluation round (GENVAL)	**July 2015**	**COM (lead)** Europol/EC3
4. Swift ratification of the Budapest Convention on Cyber Crime by all MS (para. 34)	• Work towards full ratification of the Budapest Convention		**December 2014**	**MS (lead)** Presidency based on input from MS unable to fulfil the ratification by end 2014
	• Report on Budapest Convention ratification status		**December 2014**	

5. Support training and up-skilling of MS whose governments and law enforcement authorities need to build cyber capabilities to combat cybercrime (para.35)	• Draw up a priority list of areas which require further training or up-skilling		**July 2014**	**COM (lead)** Europol/EC3, CEPOL, ENISA
	• Plan implementation and report on progress		**December 2014**	
	• Update on the progress of the 7th evaluation round	GENVAL	**July 2015**	**Presidency (lead)** MS
6. Use the Instrument for Stability (IfS) to develop the fight against cybercrime (…) in third countries from where cybercriminal organisations operate (para. 36.3)	• Present initial suggestions on the possible use of EU funding instruments, including for actions in third countries e.g. for capacity building, assisting LEA to address cyber threats, creation of policies, strategies and institutions	Cyber capacity building pilot projects have started within the IfS, further funding available from 2015	**October 2014**	**COM, EEAS (joint lead)** MS, private sector
7. Need for strong and effective legislation to tackle cybercrime (Strategy)	• Update on transposition and implementation status of Directive 2013/40/EU on Attacks Against Information Systems		**October 2014**	**COM (Contact Committee) (lead)**
	• Update on the assessment of the MS national laws compliance with Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography		**October 2014**	**COM (lead)**

D. CSDP				
1. Develop a cyber defence framework (para.37.1)	• Assess EU cyber defence operational requirements		**October 2014**	**EEAS (lead)** MS, EDA
	• Develop EU Cyber Defence Policy Framework	European Council Conclusion on 19-20 December 2013 (EUCO 217/13)	**December 2014**	**EEAS (lead)** MS, EDA
2. Enhance MS's cyber defence capabilities (para.37.2)	• Propose how to move this forward including through use of European Security and Defence College and the EDA Cyber Defence Roadmap			**EDA (lead)** MS
3. Develop cyberdefence capability concentrated on detection, response and recovery from sophisticated cyber threats (Strategy)	• Ensure projects are devoted to the protection of information networks and infrastructure in support of CSDP operations/missions			**EDA (lead)** EEAS, MS
	• Update on progress of project development			**EDA**
4. Using the existing mechanisms for pooling and sharing and utilising synergies with wider EU policies (para.37.3)	• Promote dialogue and coordination between civilian and military actors in the EU with particular emphasis on the exchange of best practices			**EDA (lead)** MS

5. Develop secure and resilient technologies for cyber defence and to strengthen cyber security aspects in EDA research projects (para.37.4)	• Develop secure and resilient technologies for cyber defence			**EDA (lead)** COM, MS, Private Sector
	• Strengthen research projects			MS, EDA
6. New cyber threats (para.37.5)	• Review, update and test early warning systems			**EDA (lead)** MS, ENISA, COM, Europol/EC3
7. EU-NATO cooperation on cyber defence (para.37.6)	• Identify priorities for continued EU-NATO cyber defence cooperation	EU-NATO informal staff to staff cybersecurity regular meetings since 2010. Common areas for further cooperation: need to raise cyber security awareness, training & capability development in terms of cyber resilience		**EDA (lead)** COM
	• Reciprocal participation in cyber defence exercises and training: identify concrete dates and events			**EDA (lead)** COM

E. Industry and Technology[2]				
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 (para.38)	• Identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies	Work is on-going in the NIS Platform including to develop a strategic research agenda to contribute to identifying future cyber security tools and technologies. Any additional work needs to take this into consideration.	**March 2015**	**Europol (lead)** ENISA
	• Identify specific strategic technological challenges for the future and support the capacity building to meet these challenges, via innovation, R&D and standardisation		**March 2015**	**MS (lead)** Private sector, COM, ENISA, EU-LISA
	• Identify actions to be financed under the Horizon 2020 Framework Programme	NIS Platform research landscape	**December 2014**	**MS (lead)**
	• Support the development of strategic sectors for the Union such as telecommunications equipment industry, trustworthy European-based cloud computing infrastructures and services			**MS, COM (joint lead)**
	• Strengthen the efforts at a European level as regards R&D support and innovation			**COM (lead)** ENISA, Private sector

[2] This part has been fully aligned with doc. 5495/3/14 REV3 which is expected to be agreed by FoP

	• Enhance synergies between "ICT programming" and "Societal and security challenge" of the Horizon 2020 Framework Programme			**COM (lead)** MS, ENISA
	• Optimize synergies between Horizon 2020, COSME, the Connecting Europe Facility and European Structural and Investment Funds (ESIF) for the benefit of the European cyber industry as well as for promotion of investment in innovation, research and technology transfer			**COM, MS (joint lead)**
	• Develop safeguards that hardware/software produced both in EU/3rd countries, as well as the relevant processes and corresponding infrastructure, meet necessary levels of security, assurance and protection of personal data	Work ongoing e.g. Technical Specifications for Interoperability standards for software.		**Private Sector (lead)**
	• Analyse the necessity and the impact of the establishment and promotion of an EU-wide certification scheme on the basis of, and compatible with, relevant, existing international ones			**MS (lead)**
	• Work for the further development of globally interoperable standards and to promote that they are widely used by industry			**MS (lead)** Private sector

2. Development of public-private partnerships, as a relevant instrument to enhancing cybersecurity capabilities (para. 40).	• Build a network of national digital coordinators on the basis of existing networks	This work is already underway, in part within the NIS Platform.		**Presidency, COM, MS (joint lead)**
	• Promote the strengthening of synergies between European companies, including SMEs to identify a way to improve info sharing and working together in answer to common strategic technological challenges			**MS (lead)** COM
	• Promote early involvement of industry and academia in development and coordination of cybersecurity solutions through making the most of Europe's Industrial Base and associated R&D technological innovations in coordination with research agendas of civilian and military organisations			**MS (lead)**
	• Promote tailored university and vocational trainings in order to develop ICT and cybersecurity expertise and explore the ways how to employ it for the benefit of the European market			**MS (lead)** ENISA

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 (para.45.2)	• Monitor the implementation of the first set of CBMs at the OSCE and development of second set of CBMs	OSCE Permanent Council Decision 1106/3.12 2013 set CBM to reduce risks of conflict stemming from the ICT use		**MS (lead)**
	• Hold a follow up Conference of "London process"	To be held in NL	**Spring 2015**	**MS (NL)**
2. Budapest Convention as a model for drafting national cyber crime legislation (para.44.1.a)	• Ensure that Budapest Convention is consistently presented as the instrument of choice and a model for national cyber crime legislation in all relevant fora			**COM (lead)** EEAS
3. Develop common EU messages on cyberspace issues (para.44.2)	• Develop messages by seeking MS' cyber policy expertise and experience from bilateral engagements and cooperation			**COM (lead)** EEAS, MS
	• Council conclusions on Cyber diplomacy	To be based on the EEAS paper	**June 2014**	

	• Develop a coherent EU International cyberspace policy to increase engagement with key international partners and organisations and ensuring that all MS can benefit fully from such cooperation • Update on progress	High level cyber dialogues with the EU are ongoing and potential cooperation with a number of third countries is being examined		**EEAS (lead)** MS, COM
4. Strengthen CIIP cooperation networks (Strategy)	• Increase policy coordination and information sharing e.g. the Meridian network			**COM (lead)** EEAS, MS
	• Update on progress		Once per Pcy	**Presidency (lead)**
5. Developing capacity building on cyber security and resilient information infrastructures in third countries (Strategy)	• Identify EU funding instruments which can be used in support of cyber security capacity building projects in third countries			**MS, COM**, **EEAS (joint lead)**