Council of the European Union

Brussels, 5 June 2015
(OR. en)

6183/2/15
REV 2

LIMITE

POLGEN 15	**IND 19**
JAI 90	**COTER 34**
TELECOM 35	**ENFOPOL 40**
PROCIV 7	**DROIPEN 17**
CSC 33	**CYBER 7**
CIS 2	**COPS 46**
RELEX 125	**POLMIL 20**
JAIEX 8	**COSI 24**
RECH 23	**DATAPROTECT 16**
COMPET 37	**CSDP/PSDC 88**

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	9298/5/14
Subject:	EU Cybersecurity Strategy: Road map development

Delegations will find in Annex an updated and reshaped version of the road map on the implementation of the Council conclusions on the EU Cybersecurity Strategy taking into account the progress made on the respective already agreed actions, outcome of the 2nd High-Level Conference on the EU Cybersecurity Strategy held in Brussels on 28 May 2015, which seeked "to ensure that the strategy is being implemented promptly and assessed in the face of possible developments".

In order to provide some input to the upcoming Presidencies agenda, the LV Presidency added a new column entitled "Notes for reflexion" encompassing suggestions for possible way forward of the actions left behind or where no real progress has been made so far or new tasks or challenges that … during the implementation.

Delegations are invited to consider these suggestions and form a position thereon.

ROADMAP					
Field/ Work Strands	**ACTIONS**	**PROGRESS**	**DUE DATE**	**Lead/ Other Actors**[1]	**Notes for reflexion**
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	General approach on both files expected in mid-June 2015. (ECJ decisions C-293/12, C-594/12, and C-131/12)	**July 2015** **December 2015**	**Presidency (DAPIX)** MS	
	Update on the progress of negotiations of the New Data Protection Directive in the law enforcement sector				
	Adoption of EU Human Rights Guidelines on Freedom of Expression Online and Offline	Adopted on 12 May 2014 by FAC (9647/14)	**completed**	**EEAS (COHOM)** MS, COM	Update on progress of implementation
2. Promote and protect values and interests within the Union and its external policies related to cyber issues (para. 15)	Adoption of Council Conclusions on Internet Governance	Adopted on 27/11/14 by TTE Council (16200/14)	**completed**	**Presidency (TELECOM FoP)** EEAS, COM	Update on progress of implementation

[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 the use of funds available under the Connecting Europe Facility for broadband roll-out		**July 2015**	**COM**	An overall overview of funding available for cybersecurity could be prepared with goals/amounts/ requirements
4. Cybersecurity is key to protecting the digital economy (para. 23.3)	Adoption of the Electronic Identification and other Trust Services Regulation	OJ L 257/73, 28.8.2014	**completed**	**Presidency, COM, MS**	Update on progress of implementation

B. chieving 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	3rd trilogue on 30/4/15 (no date for next one). Written input by COM on 27/05. Technical meeting on 1/06.	**July 2015**	**Presidency (TELECOM)** 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 Cybersecurity Strategies and update on implementation progress, with support from ENISA, where appropriate.	ENISA support focused on the development, analysis and implementation of existing strategies, raising awareness of good practice and practical tools for evaluation. 2nd Workshop of ENISA on National Cyber Security Strategies took place in Riga on 13/5/2015.	**On-going**	**MS** Presidency, ENISA	Explore ways to support MS without strategy, using experience of MS with a revised Strategy in place. Examine and draw conclusions from more focussed updated/ revised strategies, including on the common policy priorities across the EU.
	Examine whether outputs from European Public private partnerships such as the NIS Platform could be used to improve the network resilience of MS and of EU institutions, agencies and bodies	NIS platform 5th plenary meeting was held on 27/5/2015 in Brussels. Report on progress by the 3 WGs (strategic research agenda, risk management structure and requirements, voluntary information sharing).	**On-going**	**COM** Presidency, ENISA, eu-LISA MS	Considering the existence of multiple fora (fragmentation and confusion vs. possibility for a permanent lead) prepare an overview of the different platforms in the EU.

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)	Update on the status of public-private partnerships, in particular involvement of industry and academia	1st call in industrial leadership in ICT security has retained 8 projects in the area of security-by-design and cryptography. 1st call on digital security in societal challenge has retained 7 secure societies proposals in the area of privacy, access control, and risk management and assurance models. Projects are expected to start in the first half of 2015.	**November 2015**	**MS** Presidency, eu-LISA	**?**
	Update on the work undertaken under Horizon 2020		**October 2015**	**COM** MS	**?**
	Identify and assess the technical obstacles to coordination		**September 2015**	**COM** MS, ENISA, eu-LISA	**?**

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” 2015	ENISA invited parties to express interest in taking part (call open till 09/2015). Also is organising with MS seminars/trainings to build up a coalition (04-09/2015). A report with PPP best practices from MSs is currently being drafted. A NIS quiz is under preparation. An interactive map with NIS educational programmes is refined. A pledge to mitigate human-related risks in the cyber space was signed on May 18, 2015 by LV, LT, EE, FI, AT, NL and a Cyber Hygiene Initiative was launched.	**October 2015**	**ENISA, MS, private sector**	How to ensure more involvement of MS**?** Lessons learned & good practices. Encourage MS to introduce NIS training in schools; NIS, personal data protection & secure software development in the universities; and basic NIS training for public administration. Update on outcome
	Organise a "Cybersecurity championship", university students will compete in proposing NIS solutions. Update on progress of preparation	ENISA's workshop to share ideas took place on 29/4/14	**September 2015**	**COM, ENISA**	Update on the outcome
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	The 3rd pan-European Exercise - Cyber Europe 2014 was carried out. Update was provided to FOP on 22/09/14. A Pan European Exercises Workshop was organised on 12-13/5/2015 in Rome to discuss the After	**July 2015**	**Presidency, ENISA, MS**	What is the level of preparedness of the cyber exercises calendar? Application of the solidarity clause for cyber crises (IPCR) Will be worth to

		Action Report from Cyber Europe 2014. The Cyber Europe 2016 concept brief will be ready in summer 2015, planning will start in early Autumn 2015; MS will be invited to participate. EU cooperation procedures (EU-SOPs) to be refined before end of 2015. The cyber exercises survey project is ongoing. MS will be asked to contribute (summer 2015). Results are expected to be available by November 2015. 1st IPCR Exercise- "Crisis Response 2014", (Based on Cyber Europe 2014), was held in Brussels on 27 November 2014 (15776/14)			organise a cyber exercise in FoP similar to IPCR?
6. Cybersecurity issues in light of ongoing work on the solidarity clause (para 29.8)	Adoption of Council Decision on arrangements for the implementation by the Union of the Solidarity Clause	GAC adopted on 24/6/2014. a decision on the arrangements for the implementation by the Union of the solidarity clause (9937/14)	**completed**	**Presidency** MS	Clarify the application of the Solidarity Clause and it's mechanisms for cyber crises Update on progress of implementation

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 (para 25)	Identify weaknesses and undertake actions to strengthen EU institutions' information systems network security and resilience		**On-going**	**MS, EU institutions, agencies and bodies**	
	Regular update on status of EU Institutions' Cyber Resilience	Discussed in FOP on 22/09/14 (12992/14) and on 23/02/15 On 25/2/15, the inter-institutional CERT-EU Steering Board agreed on a new mandate for CERT-EU; its service catalogue and its information sharing and exchange framework (doc. 6738/15)	**September 2015**	**MS, EU institutions, Agencies and bodies** CERT-EU, ENISA COM, eu-LISA	MS/EU institutions to consider the implementation of the cyber hygiene project
	Update on the developments of the inter-institutional NIS cooperation at technical and political level regarding the NIS policies guidelines and practices of EU institutions, agencies and bodies		**September 2015**	**EU institutions, agencies and bodies**	Consider regular updates on the outcome of the inter-intitutional cooperation
	Provide support to CERT-EU as the shared security and incident response capacity of the EU institutions, agencies and bodies		**October 2015**	**EU institutions, agencies and bodies** ENISA, MS	See with CERT-EU what support might be needed? Network of EU CERTs
	Assist the EU institutions, agencies and bodies in their effort of reinforcing their NIS and bringing coherence in their NIS policies and capabilities		**On-going**	**ENISA, MS**	

C. Cybercrime					
1. Use of EC3 as a means of strengthening cooperation between national agencies within its mandate (para. 32)	Update on progress on EC3 - MS cooperation, setting out areas that work well and those that may require further consideration		**July 2015**	**Presidency** 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	**On-going**	**Presidency** Europol/EC3, Eurojust, eu-LISA COM	Consider involvement of FOP in the preparation of OAPs 2016. Establishment of closer links between the various cyber communities Update on progress
	Identify obstacles to cooperation and means for their overcoming		**On-going**		
3. Operational capability to effectively respond to cybercrime (Strategy)	Update on progress on the development of adequate digital forensic tools and technologies in view of evolving cybercrime	Info will be obtained in the framework of the 7th mutual evaluation round (GENVAL)	**July 2015**	**COM** Europol/EC3, eu-LISA	
	Address the terrorist use of the internet, most notably through the cooperation with internet companies and the civil society,	COM's European Agenda on Security provides for launch in 215 of EU Internetl Forum in 2015 to bring IT companies together with LEA and civil society. The Forum will focus on deploying the best tools to counter terrorist propaganda on Internet and in social		**Europol, COM, MS**	

		media and will explore concerns of LEA on new encryption technologies. JHA Council agreed on setting up an EU Internet Referral Unit at Europol on 12/03/15 (6891/15). It is expected to become operational by 1/7/2015. Exchange of good practices on the use of Internet for terrorist purposes at FOP on 8/6/2015 (FR, UK).			
	Update on the JHA Agencies network work in the areas of ICT and cyber security	JHA Agencies network priorities for 2015 (5946/15) include further strengthening their cooperation, exploring use of ICT solutions and related economies of scale and joint projects in line with their respective mandates. 3rd meeting of the network and a meeting with the industry on ICT solutions are in preparation.		**JHA Agencies network (**CEPOL, EASO, EIGE, EMCDDA, eu-LISA, Eurojust, Europol, FRA and Frontex**)**	
4. Swift ratification of the Budapest Convention on Cyber Crime by all MS (para. 34)	Work towards ratification of the Budapest Convention by all MS	3 MS still need to ratify the Budapest Convention. Update on the ratification status by MS was provided in FoP on 22/09/2014	**December 2015**	**MS** Presidency	To check with the remaining 3 MS how to speed up the process

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	COM is evaluating the national programmes through which 70% of the funding available under ISF would be spent	**July 2015**	**COM** Europol/EC3, CEPOL, ENISA, eu-LISA	
	Plan implementation and update on progress		**July 2015**		
	Update on the progress of the 7th evaluation round	GENVAL FR (Oct 2014) and NL (Nov 2014) reports presented at GENVAL on 29/4/15 UK (Jan 2015) RO (Jan 2015) SK (Feb 2015) EE (March 2015) SI (May 2015) IT (May 2015 tbc) ES (June 2015)	**July 2015**	**Presidency** MS	
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 (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	A pilot project on capacity building of third countries to fight cybercrime started in November 2013 under-IcSP (in partnership with the Council of Europe). Further funding available from 2015. One example was presented by COM in FOP on 22/09/14 (C(2014) 5651 final)	**July 2015**	**COM** EEAS, MS, private sector	COM to present in details all funding possibilities for MS

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	On 28 April 2015, the Commission adopted the European Agenda on Security (8293/15), setting out key priorities and actions for the period 2015-2020. Its three main priorities will be the fight against terrorism, organised crime and cybercrime	**September 2015**	**COM (Contact Committee)**	
	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 2015**	**COM**	

D. CSDP					
1. Develop a cyber defence framework (para.37.1)	Assess EU cyber defence operational requirements	The EUMS and the EDA briefed the Military Committee on 24/09/2014 on the Assessment of the EU Cyber defence operational requirements	**On-going**	**EEAS** MS, EDA	
	Develop EU Cyber Defence Policy Framework	European Council Conclusion on 19-20 December 2013 (EUCO 217/13). Adopted by FAC on 17/11/14 (15585/14).	**completed**		Update on progress of implementation
	Update on the progress report on the implementation	An oral update on the implementation was provided to the cyber attaches on 22 May 2015. A report will be officially presented and discussed in the PMG in June (in the perspective of an endorsement by the PSC)	**July 2015**	**EEAS** PMG, 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		**December 2015**	**EDA** MS	
	Utilization of NATO CCDCOE platform for exchange of best practices			**EEAS**	**?**
	Take part in the organisation of the multilayer exercise (cyber elements) and update on the outcome Develop common standards, training and education, organise cyber defence			**EEAS** EDA, MS	

	exercises				
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			**EEAS** EDA, MS	
	Update on progress of EDA cyber defence 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			**EEAS** EDA, MS	
5. Develop secure and resilient technologies for cyber defence and to strengthen cybersecurity aspects in EDA research projects (para.37.4)	Develop secure and resilient technologies for cyber defence			**EDA** COM, MS, Private Sector	
	Strengthen research projects			MS, EDA	
6. New cyber threats (para.37.5)	Test, review and update early warning and response systems in the light of new cyber threats			**EEAS** EDA, MS, ENISA, COM,Europol/EC3	

7. EU-NATO cooperation on cyber defence (para.37.6)	Identify priorities for continued EU-NATO cyber defence cooperation, with due respect to the institutional framework and the EU's decision-making autonomy	EU-NATO informal staff to staff cybersecurity regular meetings since 2010. Common areas for further cooperation: need to raise cybersecurity awareness, training & capability development in terms of cyber resilience		**EEAS** COM, EDA	
	Reciprocal participation in cyber defence exercises and training, in accordance with the EU Cyber Defence Policy Framework and the EU exercise policy Ensure a dialogue with international partners, specifically NATO and other international organisations in order to contribute to the development of effective cyber defence capabilities			**EEAS** COM, EDA	

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 (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 ongoing in the NIS Platform	**May 2015**	**COM** Europol,ENISA	What will be the link with NIS Directive network
	Identify specific strategic technological challenges for the future and support the capacity building to meet these challenges, via innovation, R&D and standardisation		**May 2015**	**MS** Private sector, COM, ENISA, EU-LISA	
	Identify actions to be financed under the Horizon 2020 Framework Programme	Programme Committee	**July 2015**	**MS**	
	Support the development of strategic sectors for the Union such as telecommunications equipment industry, trustworthy European-based cloud computing infrastructures and services	The Competitiveness Council adopted conclusions on 2 March 2015 on the "Single Market Policy" (6197/15)		**MS, COM**	
	Strengthen the efforts at a European level as regards R&D support and innovation	The Council (Competitiveness) adopted conclusions on open, data-intensive and networked research as a driver for faster and wider innovation.		**COM** ENISA, Private sector	
	Enhance synergies between “ICT programming” and “Societal and security challenge” of the Horizon 2020 Framework Programme			**COM** 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	The Commission presented in		**COM, MS**	Consider involvement in DSM actions (establishment of a PPP on cyber security in the area of

	as for promotion of investment in innovation, research and technology transfer	July 2014 its Communication on "Towards a thriving data-driven economy (11603/14 + COR 1) The Commission issued its communication "A digital single market strategy for Europe" on 6 May 2015, (8672/15). On 28-29 May 2015, the Council (Competitiveness) exchanged views on digital single market policy and adopted conclusions on the digital transformation of European industry (8993/15). The outcome of the exchange of views and the conclusions will be a valuable contribution to the discussions on digital single market policy planned at the European Council on 25-26 June 2015.			technologies and solutions for online network security)
	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** eu-LISA	

	Analyse the necessity and the global impact of the establishment of an EU-wide security certification framework compatible with, relevant, existing international, national and European standards			**MS** eu-LISA	
	Work for the further development of globally interoperable standards and to promote that they are widely used by industry			**MS** Private sector, eu-LISA	

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 3 events took place in November 2014.	**On-going**	**Presidency, COM, MS**	
	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** 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**	
	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** 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 contribute to the implementation as well as the 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**	
	Hold a follow up Conference of "London process"	The follow-up Conference was held in the Hague, NL on 16-17/4/2015. Next one will be held in Mexico in 2017	**completed**	**MS (NL)**	Information on Mexico preparation. EU/MS Position(s)?
	Participate as observer in the cybersecurity confidence building measures discussion held in the framework of Asean Regional Forum	An ARF seminar supported by the EU on CBMs will be held in 2015.	**2015**	**EEAS, MS**	
	Support the work of the EU-Japan Cyber Dialogue	The EU-Japan Cyber Dialogue meeting was held on 6/10/14. The second rounds of the new space and cyber dialogues take place in 2015 as set out in the orientation debate for the next EU-Japan Summit on 29/5/15. (7589/15)	**On-going**	**EEAS** COM, MS	
	Support the work of the EU-China Cyber Taskforce	The EU-China Cyber Taskforce meeting was held on 21/11/14.	**On-going**	**EEAS** COM, MS	

	Support the EU-US Cyber Dialogue	The EU-US Cyber Dialogue meeting was held on 5/12/14. The international security in cyberspace, promotion and protection of human rights online, Internet governance developments in 2015, capacity building, US-EU cyber related work streams and upcoming events in 2015 were discussed.	**December 2015**	**EEAS** COM, MS	
	Support the EU-India Cyber Dialogue	The EU- India Cyber Dialogue was held on 21/5/15.	**On-going**	**EEAS** COM, MS	
	Support the EU-Republic of Korea Cyber Dialogue	The EU- Republic of Korea Cyber Dialogue was held on 30/4/15.	**On-going**	**EEAS** COM, MS	
2. Budapest Convention as a model for drafting national cybercrime legislation (para.44.1.a)	Ensure that the Budapest Convention is consistently presented as the instrument of choice and a model for national cyber crime legislation in all relevant fora	EU capacity building programmes use Budapest Convention as a blueprint for national legislation	**On-going**	**COM** 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	Telecom WP and CONUN are drafting LTT to guide the EU and its MS in the preparatory process of the WSIS+10 Review Process	**December 2015**	**COM, EEAS MS**	How to ensure better involvement of cyber attaches in similar occasions in the future
	Develop Cyber diplomacy policy	The Council Conclusion on Cyber Diplomacy were adopted by GAC on 10/2/15 (doc. 6122/15)	**completed**	**Pcy** EEAS, MS	Update on progress of implementation
	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 and provide regular update on progress	High level cyber dialogues with the EU are on-going and potential cooperation with a number of third countries is being examined. Update on the already launched cyber dialogues was provided in FOP on 22/09/14.		**EEAS** MS, COM	
4. Strengthen CIIP cooperation networks (Strategy)	Increase policy coordination and information sharing e.g. the Meridian network	DE delegation updated on the Meridian network and upcoming conference in FOP on 22/09/14.Next meeting will be held in Madrid.	**October 2015**	**MS** EEAS, COM	Explore what other mechanisms for info sharing and policy coordination exist? How they interact? Invite relevant delegation to provide info on outcome & progress

5. Developing capacity building on cybersecurity and resilient information infrastructures in third countries (Strategy)	Identify EU external financing instruments which can be used in support of cybersecurity capacity building projects in third countries	Work started - presentations of COM + EU ISS - 23/07/14 and of national cyber capacity building initiatives - 29/1/15 at cyber attaches meetings.	**On-going**	**MS, COM** EEAS	COM to present in details all funding possibilities for MS
	Implement ongoing and launch new EU Capacity building programmes on cybersecurity and cybercrime	Two ongoing programmes under the Instrument contributing to Stability and Peace and Stability (IcSP) on cybercrime and cybersecurity respectively, and one under the Eastern Partnership Instrument on cybercrime.	2014-2016	**COM** EEAS	What is in the pipeline?