Council of the European Union

Brussels, 4 March 2015
(OR. en)

6183/1/15
REV 1

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 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, the discussions at the Friends of the Presidency Group on Cyber Issues meeting held on 23 February 2015 and subsequent comments received.

ROADMAP				
Field/ Work Strands	**ACTIONS**	**PROGRESS**	**DUE 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~~reaching a general approach on both files. ECJ decisions C-293/12, C-594/12, and C-131/12	**June ~~2014~~2015** **~~December 2014~~**	**Presidency (lead)** MS
	• Update on the progress of negotiations of the New Data Protection Directive in the law enforcement sector		**~~June 2014~~** **December ~~2014~~2015**	**Presidency (lead)** MS
	• ~~Timeline for implementation of the~~Adoption of Guidelines of Freedom of expression online • ~~and~~ Update on progress of implementation	Adopted on 12 May 2014 by FAC	**COMPLETED** **~~Open~~** **July 2015**	**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)	• ~~Follow-up~~Adoption of Council Conclusions on Internet Governance • Update on the follow-up and implementation	Council Conclusions on Internet Governance were adopted on 27/11/14 (16200/14)	**COMPLETED** **Open~~November 2014~~**	**Presidency (lead)** EEAS, COM, FoP Cyber

[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 ~~made~~ of ~~the~~ funds available under the Connecting Europe Facility for broadband roll-out		**~~December 2014~~July 2015**	**COM (lead)**
4. Cybersecurity is key to protecting the digital economy (para. 23.3)	• ~~Promote and maintain a high level of network and information security~~	~~Discussed by FOP on 22/09/2014 - EU institutions aspects~~	**~~Open~~**	**~~MS (lead)~~** ~~COM, eu-LISA~~
	• ~~Update on the status~~Adoption of the Electronic Identification and other Trust Services Regulation~~, including the timetable for adoption~~ • Update on the status of implementation	OJ L 257/73, 28.8.2014	**COMPLETED** **July ~~2014~~2015**	**Presidency** **COM, 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. The third informal trilogue is in preparation (doc. 16224/14 and 5257/15)	~~**October 2014**~~ ~~**December 2014**~~**July 2015**	**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 update on implementation progress, with support from ENISA, where appropriate	Ongoing work by ENISA on cybersecurity strategies.	**Open**	**MS (lead)** Presidency, ENISA
	• 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 plenary meeting was held on 25 November 2014 in Brussels	**Open**~~**December 2014**~~	**COM (lead)** Presidency, ENISA, eu-LISA

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	First call in industrial leadership in ICT security has retained 8 projects in the area of security-by-design and cryptography. The first 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. ~~EP3R has been subsumed into the NIS Platform and does not exist anymore.~~	**November ~~2014~~2015**	**MS (lead)** Presidency, eu-LISA
	• Update on the work undertaken under Horizon 2020		**October ~~2014~~ 2015**	**COM (lead)** MS
	• ~~•~~ Identify and assess the technical obstacles to coordination		**September ~~2014~~ 2015**	**COM (lead)** 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" • Update on outcome	ENISA invited parties to express interest in taking part	**October ~~2014~~ 2015 December ~~2014~~2015** (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's workshop to share ideas took place on 29/4/14	**September ~~2014~~2015** (on preparation) **December ~~2014~~2015** (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	The 3rd pan-European Exercise - Cyber Europe 2014 was carried out. Update was provided to FOP on 22/09/14. 1st IPCR Exercise "Crisis Response 2014", (Based on Cyber Europe 2014), was held in Brussels on 27 November 2014 (15776/14)	**~~December 2014~~July 2015**	**Presidency, ENISA, MS (joint lead)**
6. Cybersecurity issues in light of ongoing work on the solidarity clause (para 29.8)	• ~~Update on progress on the~~ Adoption of Council Decision on arrangements for the implementation by the Union of the Solidarity Clause • Update on progress of implementation	~~Adopted~~ (9937/14). GAC adopted a decision on the arrangements for the implementation by the Union of the solidarity clause	**~~GAC June 2014~~ ~~Open~~COMPLETED** **March 2015**	**Presidency (lead)** MS

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)	• ~~Examine weaknesses and~~ search for ~~ways to remedy them in the face of the growing threats towards EU institutions' information systems~~; • Identify the weaknesses and undertake actions to strengthen the EU institutions' information systems network security and resilience;		**Open**	**MS, EU institutions, agencies and bodies (lead)**
	• 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 2014~~ February 2015** **October 2015**	**MS, EU institutions, agencies and bodies (lead)** CERT-EU, ENISA COM, eu-LISA
	• Update on the developments of the inter-institutional NIS cooperation at technical and political level ~~(the inter-institutional committee for informatics (CII))~~ regarding the NIS policies, ~~and~~ guidelines and practices of EU institutions, agencies and bodies		**October 2015**	**EU institutions, agencies and bodies**
	• 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

	• Assist the EU institutions, agencies and bodies in their effort of reinforcing their NIS and bringing coherence in their NIS policies and capabilities		**Open**	**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		**~~January~~ July 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, eu-LISA COM
	• Identify obstacles to cooperation and means for their overcoming		**Ongoing**	
	• Update on progress		**October/ December ~~2014~~2015**	
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 • to address the terrorist use of the internet, most notably through the cooperation with internet companies and the civil society,	Info will be obtained in the framework of the 7th evaluation round (GENVAL) At JHA Council on 9 October 2014, the Commission was invited to present a set of recommendations on how the EU should engage with Internet companies on countering the use of the Internet for terrorist purposes. Commission updated TWP on 16/1/15 on the process	**July 2015**	**COM (lead)** Europol/EC3, eu-LISA

		of establishment of a Forum with Internet service providers community.		
	• Update on the JHA Agencies network work in the areas of ICT and cybersecurity	Among the priorities of the JHA Agencies network for 2015 (5946/15) is further strengthening their cooperation, exploring the use of ICT solutions and related economies of scale and joint projects in line with their respective mandates. The 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 ~~full~~ ratification of the Budapest Convention by all MS	4 MS still need to ratify the Budapest Convention	**December ~~2014~~2015**	**MS (lead)** Presidency based on input from MS unable to fulfil the ratification by end 2014
	• Update on Budapest Convention ratification status	Provided in FOP on 22/09/14	**~~December 2014~~July 2015**	

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	~~**November 2014**~~**July 2015**	**COM (lead)** Europol/EC3, CEPOL, ENISA, eu-LISA
	• Plan implementation and update on progress		~~**December 2014**~~**July 2015**	
	• Update on the progress of the 7th evaluation round	GENVAL FR (Oct 2014) NL (Nov 2014) UK (Jan 2015) RO (Jan 2015) SK (Feb 2015) EE (March 2015)	**July 2015**	**Presidency (lead)** 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 ~~Cyber~~ capacity building of third countries to fight cybercrime ~~pilot projects have~~ started in November 2013 under ~~within the IfS,~~ IcSP (in partnership with the Council of Europe). ~~f~~Further funding available from 2015. One example was presented by COM in FOP on 22/09/14 (C(2014) 5651 final)	~~**October 2014**~~**July 2015**	**COM (lead)** 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**~~**June 2015**	**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**~~**June 2015**	**COM (lead)**

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	~~**October 2014**~~**Open**	**EEAS (lead)** MS, EDA
	• Develop EU Cyber Defence Policy Framework • Update on the implementation	European Council Conclusion on 19-20 December 2013 (EUCO 217/13). Adopted at the FAC on 17 November 2014 (15585/14)	**COMPLETED** **July 2015**	**EEAS (lead),** 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		~~**October 2014**~~ **December 2015~~4~~**	**EDA (lead)** 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 exercises			**EEAS (lead)** EDA, 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			**EEAS (lead)** 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 (lead)** 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 (lead)** 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 (lead)** 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 (lead)** COM, EDA
	• Reciprocal participation in cyber defence exercises and training, in accordance with the EU Cyber Defence Policy Framework and the EU exercise policy~~: identify concrete dates and events~~ • 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 (lead)** 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	**~~March~~ May 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~~ May 2015**	**MS (lead)** Private sector, COM, ENISA, EU-LISA
	• Identify actions to be financed under the Horizon 2020 Framework Programme	Programme Committee	**~~December 2014~~July 2015**	**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
	• 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),** 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 (lead),** eu-LISA
	• Work for the further development of globally interoperable standards and to promote that they are widely used by industry			**MS (lead)** 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.	**Open**	**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			**MS (lead)**

	trainings in order to develop ICT and cybersecurity expertise and explore the ways how to employ it for the benefit of the European market			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 (lead)**
	• Hold a follow up Conference of "London process"	The next follow-up Conference will be held in the Hague, NL in 2015	**16-17 April 2015**	**MS (NL)**
	• 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	**~~March~~ 2015~~4~~**	**EEAS, MS**
	• Support the work of the EU-Japan Cyber Dialogue	The EU-Japan Cyber Dialogue meeting was held on 6/10/14. COASI was briefed on 15/10/2014 and a COREU 1140/14 was issued on the1st meeting which will cover the application of international law, cyber norms and confidence building measures (CBM), capacity	**~~6 October 2014~~ Open**	**EEAS (lead)** COM, MS

		building and cybercrime.		
	• Support the work of the EU-China Cyber Taskforce	The EU-China Cyber Taskforce meeting was held on 21/11/14. ~~COASI and FoP briefed 29/10/2014 about the 3rd meeting at which International security l□Й□ □0 x□ x x□ x□ x□ confidence building measures), Internet governance, economic growth and cyber security and cybercrime were discussed.~~ ~~MS, EEAS and COM held a preparation meeting 06/11/2014~~	~~**21 November 2014**~~**open**	**EEAS (lead)** COM, MS
	• Support the EU-US Cyber Dialogue	The EU-US Cyber Dialogue meeting was held on 5/12/14. ~~COTRA briefed on 14/10/2014.~~ At its 1st meeting the international security in	~~5~~ **December 2015~~4~~**	**EEAS (lead)** COM, MS

		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 will be discussed.		
	• Support the EU-India Cyber Dialogue	Terms of Reference presented in COASI on 11/02/2015 in preparation for the upcoming dialogue.	**21 May 2015**	
	• Support the EU-Republic of Korea Cyber Dialogue	Terms of Reference presented in COASI on 11/02/2015 in preparation for the upcoming dialogue.	**30 April 2015**	
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 the Budapest Convention as a blueprint for national cybercrime legislation	**Ongoing**	**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
	• Develop the Cyber diplomacy policy ~~and Evaluate the ways for follow-up~~	The Council Conclusion on Cyber Diplomacy were adopted by GAC on 10/2/15 (doc. 6122/15)	**COMPLETED ~~September~~ December 2014 ~~Open~~**	**Pcy (lead)** EEAS, MS
	• Follow-up the Council Conclusions on Cyber Diplomacy implementation and reporting		**2015**	**MS, EEAS, COM**
	• 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. Update on the already launched cyber dialogues was provided in FOP on 22/09/14.		**EEAS (lead)** 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 (lead)** EEAS, COM
	• Update on progress		**Once per Pcy**	**Presidency (lead)**

5. Developing capacity building on cybersecurity and resilient information infrastructures in third countries (Strategy)	• Identify EU external financing~~funding~~ instruments which can be used in support of cybersecurity capacity building projects in third countries	Work has started on 23/07/14 at the cyber attaches meeting, (COM + EU ISS presentations).National cyber capacity building initiatives-were presented at the cyber attaches meeting on 29/1/15.	**Ongoing**	**MS, COM~~,~~ ~~EEAS~~ (joint lead)** EEAS
	• Implement ongoing and launch new EU Capacity building programmes on cybersecurity and cybercrime	Two ongoing programmes under the Instrument contributing to Stability and ~~of~~ Peace and Stability (IcSP) on cybercrime and cybersecurity respectively, and one under the Eastern Partnership Instrument on cybercrime.	**2014-2016**	**COM (lead)~~,~~** EEAS