COUNCIL OF
THE EUROPEAN UNION

Brussels, 6 November 2012

15686/12

LIMITE

POLGEN 183
JAI 750
TELECOM 198
PROCIV 170
CSC 72
CIS 6
RELEX 988
JAIEX 91
RECH 398
COMPET 659
IND 181
COTER 107

NOTE

from:	Presidency
to:	COREPER (part 2)
Subject:	Better coordination in the Council on cyber policy issues

I. CURRENT STATE OF AFFAIRS

1. The term "cyber issues" covers a multi-faceted range of issues involving different policy areas, e.g. criminal justice, law-enforcement cooperation, the internal market, the Internet economy, research and development, industrial policy, cyber-security, protection of critical information infrastructure, aspects of anti-terrorism policies, international cyberspace policy, external relations, military planning and operations, etc. The number of initiatives and activities in the field at EU level is growing. A non-exhaustive list of some recent and upcoming initiatives is set out in Annex II, along with an indication, where possible, of the Council preparatory body leading work on each of them.

2. The multidisciplinary nature of the subject is mirrored in a complex institutional construction at the EU and national level, where many different working formats and entities are competent on cyber issues.

3. It appears that work in the area faces some difficulties due to a certain level of fragmentation, compartmentalised sectoral development and lack of a coherent overview of the policy area in its entirety. Organising the coordination and exchange of information among the various activities and players in a comprehensive policy framework remains a challenge that has to be addressed.

4. Coordination would become even more important in view of the upcoming European Strategy for Cyber-Security that will be jointly presented in the coming months by the Commission and the High Representative for Foreign and Security Policy.

II. A Friends of Presidency Group (FoP) on Cyber Issues

5. In order to enhance internal coordination and help develop an EU integrated approach on cyber policy issues, a recognised horizontal forum could be established within the Council. Such a group could provide a comprehensive cross-cutting forum for coordination and cooperation and exchange of information encompassing various fields of expertise to ensure coherence, when required, on general policy issues taking into due account existing interlinkages and interdependencies.

6. One possible working format could be to use the Friends of the Presidency Group (FoP), an existing Council preparatory body, activated by the Presidency to address specific policy issues[1]. Activating the FoP to address specifically cyber policy issues would offer the necessary flexibility for considering interlinked issues in a holistic manner, would ensure effective guidance and better organisation. Council formations currently dealing with different aspects of cyber issues would maintain ownership of their respective items. The FoP group would also provide a forum which could flag to COREPER and to the Council general issues requiring their guidance. Draft terms of reference of the Group are set out in Annex I.

7. In order for this FoP, to operate in an efficient manner, Member States should identify national focal point(s) through which all relevant communication would be channeled and who would also provide national coordination among the competent entities at the national level.

8. Against this background, COREPER is invited to:

- consider whether it is opportune to activate the Friends of Presidency Group for the purpose of providing guidance and input on horizontal aspects of cyber issues and for exchanging information on these matters ;

- if so,
  - to endorse the terms of reference for this FoP as set out in Annex I; and
  - invite Member States to designate national focal point(s) on cyber policy issues and communicate their contact details to the Council General Secretariat (cyber@consilium.europa.eu)

[1] FoP Group (Integrated Maritime Policy), for example, is the main expert level working format within the Council responsible, *inter alia*, for preparing Council conclusions on EU Integrated Maritime Policy, which are adopted regularly. In its conclusions of 8 December 2008 (doc. 16503/1/08) the Council has not only recognised the IMP's cross-cutting nature by dealing with it through the General Affairs and External Relations Council, but also "confirm(ed) that an integrated approach to maritime issues constitutes a major objective, since the synergies, the coherence and the added value of sectoral action undertaken by the European Union need to be reinforced (…)".

ANNEX I

Terms of Reference for a Friends of Presidency Group on Cyber Issues

1. A formation of the Friends of the Presidency Working Group (hereinafter: the Group) is activated to ensure horizontal coordination of cyber policy issues in the Council.

   The objectives of the Group will be to:

   - ensure a cross-cutting working platform to support an integrated approach on cyber policy issues, by providing a horizontal overview of the cross cutting, transversal issues, and thus avoiding compartmentalised policy developments and decision-making;
   - identify and further exploit synergies;
   - enhance the exchange of information sharing between the various strands of work, both among Member States, as well as between the EU and the national level;
   - assist in setting EU cyber priorities and strategic objectives as part of a comprehensive policy framework;
   - support effective external representation of the EU in conformity with strategic EU cyber policy objectives;

2. The Group is activated in order to speed up the process in this particular domain, where there is an evident need to act expeditiously to keep pace with rising threats and to allow citizens to reap the opportunities offered by the digital environment.

3. The Group should address relevant cyber issues in a comprehensive manner. In view of the implementation of the European Strategy for Cyber Security, the various aspects of cyber policy, which are related, among others, to the security and resilience of networks and information systems, the fight against cybercrime, cyber defence, as well as the EU international cyberspace policy could be addressed.

4. In this context, the Group will examine any relevant horizontal issues, without prejudice to the existing mandate of other Working Parties, and could focus, *inter alia,* on policies to improve EU-wide cyber resilience, on industrial, R&D and trade developments, security dimension of internet governance issues, Human Rights online, intellectual property protection in cyberspace etc. It could be also used as a forum to coordinate the EU cyber policy initiatives relating to third countries or international organisations, and to develop EU positions for international cyber fora (e.g. the London process on cyberspace);

5. The Group will not be involved in legislative activities, but will bring issues to the attention of COREPER and Council in order for the latter to ensure coherence. The activities of the Group will be without prejudice to the work carried out in other relevant Working Parties, which shall remain responsible for the specific legislative and other non-legislative files.

6. The Group, which will be chaired by the rotating Presidency of the Council, is expected to meet at the outset of each Council rotating Presidency to take stock of the state of play in the field and identify the key issues of relevance to its work. This will be on the basis of an overall report on the various strands of on-going work and on future activities and priorities. The rotating Presidency of the Council may call for additional meetings, if deemed necessary.

7. The Group is initially set up for a period of one year. Its efficiency and effectiveness as well as its mandate, will be reviewed at the end of this period.

____

ANNEX II

RECENT INITIATIVES AND ACTIVITIES IN THE CYBER FIELD

1. The **Digital Agenda for Europe** of 26 August 2010 (doc. 9981/1/10) is one of the seven flagship initiatives of the Europe 2020 Strategy. The Digital Agenda builds its key actions around seven problematic areas, where "more comprehensive and united policy response at EU level" is needed in order to boost Europe's social and economic performance trough Information and Communication technologies (ICT). In the course of 2012 the Commission should submit a mid-term review looking at strategic priorities for the remaining two years of the Digital Agenda for Europe lifecycle - **Digital Agenda for Europe – Next steps** (measure 25 in the Commission Work Programme 2012 (doc. 17394/11 ADD 1)).

   (Working Party on Telecommunications and Information Society)

2. On 11 December 2009 the European Council adopted **The Stockholm Programme - an open and Secure Europe serving and protecting citizens** - the multiannual programme setting out the strategic guidelines for legislative and operational planning within the area of Justice, Security and Freedom for the period 2010 -2014 (doc. 17024/09, OJ 2010/C 115/01 of 4.5.2010). Section 4.4.4. of the Programme includes a number of measures to counteract Cybercrime in the context of the fight against organised and serious crime.

   The Commission Communication **"Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme"** of 20 April 2010 (doc. 8895/10) envisages concrete actions in that respect.

   (Standing Committee on Operational Cooperation on Internal Security (COSI), Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS))

3. The **Internal Security Strategy for the European Union: "Towards a European Security Model"**(ISS) was adopted by the Council of the EU on 23 February 2010 (doc. 5842/2/10). It sets out a European security model identifying common threats and challenges and strategic guidelines for action, while calling for EU-wide approach to internal security. Raising levels of security for citizens and businesses in cyberspace is among the five main priority areas for action until 2014 outlined in the **Commission Communication "EU Internal Security Strategy in Action: Five steps towards a more secure Europe"** of 22 November 2010 (doc. 16797/10).

   The **First Annual Report** providing an assessment of the implementation of the ISS in Action in 2011 was submitted on 25 November 2011 (doc. 17790/11). It outlines the state of EU internal security in each of the ISS's priority areas and provides a forward look for actions in 2012.

   (COSI, CATS)

4. The **European Security Strategy**, adopted by the European Council on 13 December 2003, included a section on Cyber security [1], which stressed the need for a comprehensive EU approach, to raise awareness and to enhance international cooperation.

5. In the coming months, the Commission and the High Representative of the Union for Foreign and Security Policy should present **a European Strategy for Cyber-security.** The initiative will aim to ensure a secure and trustworthy digital environment, articulating EU international cyberspace policy and aiming to protect fundamental rights and EU core values.

   (among others Working party on Telecommunications and Information Society)

[1] "Cyber security: Modern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, but also the internet. The EU Strategy for a Secure Information Society, adopted in 2006 addresses internet-based crime. However, attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon. More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation."

6. In December 2011 the Council took note of a progress report on the Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA) (doc. 18156/11). The proposal is intended to strengthen and modernise the ENISA and to establish a new mandate for a period of five years. The current mandate of the ENISA will expire on 13 September 2013.

New features in the tasks of ENISA in principle agreed at the Council consist of the following:

- ENISA should have the additional task of supporting and promoting voluntary co-operation between relevant organisations e.g. CSIRTs/CERTs and regularly share best practices with the aim to arrive at an advanced level of network and information security
- ENISA should support the Member States, at their request, and the Union's institutions to organise awareness raising and other outreach activities to increase network and information security and its visibility
- On international cooperation, the ENISA should contribute to the Union's efforts to cooperate with third countries and international organisations, for instance by supporting cooperation with the relevant organisations e.g. CSIRTs/CERTs and promoting involvement in international network and information security exercises.
- ENISA should provide Member States, at their request with the necessary knowledge and other resources available to strengthen their network and information security capability.

(Working Party on Telecommunications and Information Society)

7. **COM Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security** of 31 March 2011 (doc. 8548/11). The HU Presidency organised a ministerial conference on this issue and an exchange of views followed by adoption of Council conclusions took place at the May Council (doc. 10299/11).

   The Communication is a follow-up of **COM Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" of** 30.03.2009.

8. As envisaged by the 2012 Commission work programme, a cross sectoral CIP policy package will be presented to the Council in the end of 2012. This package follows up the completed review of Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (doc. 15827/08, OJ 2008/L 345/75 of 23.12.2008), covering transport and energy sectors. The forthcoming CIP policy package will also propose an updated European Programme for Critical Infrastructure Protection (EPCIP) to further reinforce protection of critical infrastructure. In addition, Critical Infrastructure Information Warning Network (CIWIN) (doc COM (2008) 676 final - not published in OJ) will be completed in early 2013. CIWIN will allow the European CIP community to share any relevant information on the protection of critical infrastructure.

   (among others, Working Party on Telecommunications and Information Society, Working Party on Civil Protection (PROCIV))

9. A **joint EU-US Cyber incident table top exercise "Cyber Atlantic 2011"** took place in November 2011.

10. A **Pan-European Cyber incident exercise** with the participation of all Member States took place in 2010 (Cyber Europe 2010) and in 2012 (Cyber Europe 2012).

11. The Commission on 27 September adopted its **Communication on "Unleashing the potential of cloud computing in Europe (COM(2012)529 final).** The Communication includes key actions concerning technical standards, certification measures, contract terms and public procurement. In particular, this Cloud computing strategy includes aspects of standards for interoperability, data portability and reversibility; the development of model contract terms to address issues not covered by the Common European Sales Law; and the establishment of a European Cloud Partnership

(Working Party on Telecommunications and Information Society)

12. **In the framework of its exchange of views on nuclear security, the Ad hoc Group on Nuclear Security** discussed and elaborated on the issue of Computer Security / Cyber Security. The key role of Information and Communication Technology (ICT) systems and Instrumentation and Control (IC) systems was identified and relevant good practices were included in the AHGNS Report which was adopted in May 2012.

(Ad hoc Group on Nuclear Security)

13. **The next Framework Programme for Research and Innovation, Horizon 2020, is curren**tly under discussion in the Council and in the Parliament. The Council's partial general approach (doc. 10663/12) from May 2012 includes a specific research objective for Secure Societies in which the focus of activities shall be to:

a. fight crime, illegal trafficking and terrorism, including under*standing and tackling terrorist ide*as and beliefs;

b. protect and improve the resilience of critical infrastructures, supply chains and transport modes;

c. strengthen security through border management;

d. improve cyber security;

e. increase Europe's resilience to crises and disasters;

f. ensure privacy and freedom, including in the Internet and enhance the societal legal and ethical understanding of all areas of security, risk and management;

g. Enhance standardisation and interoperability of systems, including for emergency purposes.

(Working Party on Research)

Over and above the internal measures taken by each EU institution and body to protect its own IT infrastructure, as well as improved cooperation at technical level (particularly between the GSC, the European Commission, and the EEAS), the following activities merit specific mention in this context:

14. Establishment in June 2010 of a **Network Security Incident Alert Mechanism** in the Council (doc. 8184/2/10)

    (Council Security Committee)

15. **A CERT-EU for EU institutions, bodies and agencies** has been set up on September 11th 2012, following a pilot phase of one year (doc. 13737/12) and successful assessment of its role and effectiveness.

    (Council Security Committee, Coordination Committee for CIS)

16. A **Network Defence Policy and Guidelines** which will apply to the Council and Council members. The policy was approved by the Council on 30.03.12 and the Guidelines were approved by the Security Committee on 30.05.12.

    (Council Security Committee)

17. The Council adopted a general approach on the proposal for a **Directive on attacks against information systems** on 10 June 2011 (doc. 11566/11). In June 2012 the negotiations with the European Parliament with a view to a first reading agreement were successfully concluded. The Council will adopt the Directive once the plenary vote in the EP takes place. The directive aims to set up minimum rules by means of criminal law for the definitions and sanctions for Cybercrime offences, while addressing inter alia some new challenges in view of the growing number of large-scale attacks across Europe conducted through advanced technological tools, such as "botnets".

    (Working Party on Substantive Criminal Law (DROIPEN))

18. Following a first reading agreement with the EP, on 13 December 2011 the Council adopted **the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA** (PE-CONS 51/1/11) . The Directive addresses *inter alia* the issue of removal of or blocking the access to web pages containing or disseminating child pornography materials.

    (DROIPEN)

19. **Council conclusions on a Concerted Work Strategy and Practical Measures against Cybercrime** of 28 November 2008 (doc. 15569/08)

    (Law Enforcement Working Party)

20. **Council Conclusions on an Action Plan to implement the Concerted Strategy to combat Cybercrime** of 26 April 2010 (doc. 5957/2/10)

    (Law Enforcement Working Party)

21. In the framework of the **EU policy cycle for organised and serious international crime**, seven strategic goals (doc. 14452/2/11) and an **Operational Action Plan** (doc. 17809/11) covering the years 2012 -2013 were agreed in the autumn of 2011 for the EU crime priority "Step up the fight against cybercrime and the criminal misuse of the Internet by organised crime groups".

    (COSI)

22. **Commission Communication "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre"** (doc. 8543/12) was submitted on 28 March 2012.**Council conclusions** on the establishment of a European Cybercrime Centre (10603/12) were respectively adopted.

    (LEWP)

23. A revision of **the EU framework for data retention** is envisaged under measure 63 of the COM Work Programme 2012.

    (DROIPEN)

24. **The Council of Europe Convention on Cybercrime (ETS No185)**, which entered into force on 1 July 2004, is the only international legal instrument up to date providing a comprehensive framework to fight Cybercrime. In conformity with the Stockholm Programme, the EU and its Member States should promote the Council of Europe Convention on Cybercrime as "the legal framework of reference for fighting cybercrime at global level"

25. **An Open-ended intergovernmental expert group on Cybercrime** to conduct a comprehensive study of the problem of cybercrime was established with UNODC in Vienna in the beginning of 2011. A regular update on the activities of the group should be presented in an appropriate Council preparatory body.
    (partially GENVAL, EU coordination process is taking place on spot)

26. **An International Conference on Cyberspace,** exploring inter alia the possible adoption of norms of behaviour in cyberspace was held on 1-2 November 2011 in London. On 13-14 December 2011 an **International Conference on Challenges in Cyber-security – Risks, Strategies, and Confidence-Building** took place in Berlin. On 4-5 October 2012 Hungary **hosted a first follow-up conference to the 2011 Conference on Cyberspace in London.** The conference aims to promote norms of behaviour in cyberspace, capacity building, security and the free use of cyberspace through close and practical cooperation between the private sector, civil society and government, as well as through more efficient cooperation between regional organisations.

27. **EU Cyber Security Conference** was organised jointly by the Commission and the External Action Service on 6 July 2012 in Brussels, where Member States were invited to exchange views on the major focus areas of the upcoming EU Strategy for Cyberspace. At the conference 5 Member States presented a non-paper calling inter alia for the establishment of a *"cross-cutting high level group on cyber security and wider related cyber policy and strategy issues".*

28. **OSCE** (Organisation for Security and Cooperation in Europe, in which the EU participates) Security Committee has launched an informal working group on Confidence Building Measures in Cyber security in June 2012. The Working Group aims at developing the transparency and cooperation measures to reduce the risk of escalation and mis-perception in state behaviour, and to build trust between state actors on cyber security issues.

    (Political and Security Committee)

29. The **EU-US Working Group on Cyber-security and Cyber-crime** was established in the context of the EU-US Summit held in Lisbon on 20 November 2010 to *"address a number of specific priority areas"* where coordinated approaches would add value to both regions, and would bring benefits to relevant public and private stakeholders - (i) Cyber Incident Management, (ii) Public-Private partnership, (iii) Awareness raising and (iv) Cybercrime. [1] The first progress Report was submitted to the EU-US Summit held in Washington on 28 November 2011. The WG continues its activities.

    (COTRA, JAIEX)

30. **EU-NATO contacts on Cyber-security issues**. Informal contacts take place between the EU and NATO on cyber defence and cyber security aspects, most recently in the margins of the Council's Politico-Military Working Group.

    (Politico-Military Working Group)

31. In the end of 2011 **the International Atomic Energy Agency (**IAEA**)** released its Technical Guidance on Computer Security at Nuclear Facilities. It is relevant to all computer-based critical infrastructure.

    (Ad hoc Group on Nuclear Security)

[1] The US Department of Defense announced a new cyber security strategy in July 2011. The strategy treats cyber space as an operational domain and is centered around five pillars (which include cooperation with international partners). In addition to working with the EU and with NATO countries, the US has a dedicated cyber cooperation agreement with Australia and cooperates with Japan in this domain, within the wider framework of the Japan-US Security Arrangements.

32. ASEAN (Association of South East Asian Nations which has dialogue relations with the EU) has been very active in the Cyber field. Already back in 2003 the ASEAN-China Plan of Action was signed and in 2004, the statement from the ASEAN Ministerial on Transnational Crime held in Bangkok addressed cybercrime and recognised the need for an effective legal cooperation to fight transnational crime. Most recently, in October 2011, the ASEAN ministerial on Transnational Crime in Bali noted that cybercrime had been growing very rapidly and that they should step up efforts and cooperation in that area. The cooperation with ASEAN in this respect **might** require a follow-up at EU level **in view of EU-ASEAN meetings**.

33. **ARF** (ASEAN Regional Forum, in which the EU is a full participant). The statement from the ARF Ministerial held in Bali in July 2011 registered a disagreement over Russia's proposed draft statement by the ARF ministers on "Cooperation in Ensuring International Information Security".

34. **China** and **Russia (**members of ARF and SCO, ASEAN dialogue partners). Whether bilaterally with the EU or in international fora, both promote the notion of "information security", which is wider than "cybersecurity". In September 2011, China and Russia, together with Tajikstan and Uzbekistan, addressed a letter to the UN Secretary General, suggesting an "international code of conduct for information security", which would focus on threats to international stability, fighting cybercrime and preventing the use of cyberspace for terrorism activities. The proposal can be misused to strengthen censorship and violation of Human Rights in cyberspace, and has not received wide-spread support in the international community.

35. At the EU-China Summit held in Beijing in February 2012, the two sides recognized the importance of deepening understanding and trust on cyber issues, and were committed to enhancing exchanges and cooperation in tackling obstacles and threats, in order to maximize the positive role of secure ICT and Internet in promoting economic and social development, as well as to exchanging views on shared risks. In this regard, the two sides agreed to set up a **EU-China Cyber Taskforce**.

(*possibly CONUN and PSC, regarding the code of conduct)*
(COASI and PSC, regarding the EU-China cyber issues)

36. **India (**ARF member**,** observer at the SCO, ASEAN dialogue partner). Since the EU-India Summit in December 2010, cyber-security was identified as a promising area of cooperation. At the Delhi Summit in February 2012, where cyber security and cyber crime were discussed, "leaders expressed satisfaction with bilateral consultations on cyber security and cyber crime as a result of which some concrete areas for mutual cooperation were identified [and] called for continuation of these consultations stressing the importance of further dialogue."
(*COASI, PSC)*

37. **Japan.** Cyber security was identified in the August 2011 Defence White Paper as one of Japan's five key security concerns**.** At the EU-Japan Summit in 2008, it was stated that "Japan and the EU will work together to strengthen the security of networks and ICT usages, by coping with threats such as cyber attacks and computer incidents, fraud, illegal, unsolicited e-mail and phishing, and the risks faced by younger users deriving from the use of internet and other communication technologies and by improving security of critical information infrastructure, in particular of telecommunications. In this regard and building on the 2004 EU-Japan Joint Statement on cooperation on ICT, they will promote exchange of information and discussions on relevant policies and cooperation, at the bilateral level and in the relevant international organizations and frameworks."
(*COASI, PSC)*