Council of the
European Union

Brussels, 4 February 2015
(OR. en)

5610/15

CYBER 3
RELEX 58
JAIEX 2
TELECOM 20
COPS 15

"I/A" ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. prev. doc.:	5223/1/15 REV 1
Subject:	Draft Council Conclusions on Cyber diplomacy

1. At the meeting of the Friends of the Presidency on Cyber Issues held on 24 February 2014, the EEAS presented a food-for-thought paper (doc. DS 1081/14) entitled “Further Strengthening European Cyber Diplomacy”. The debates that followed clearly indicated the need of raising awareness on the importance of this newly emerging issue and more importantly on the need of elaborating an appropriate strategic guidance for the EU and Member States' positioning thereon.

2. As requested by a number of delegations and with a view to facilitating further discussions, the Hellenic Presidency presented an "Outline for European Cyber Diplomacy engagement" (doc. 9967/14), building to a large extent upon the EEAS food-for-thought paper and reflecting as much as possible Member States' views and concerns expressed during its examination.

3. The subsequent discussions examined both the content and the form to take forward the issued of cyber diplomacy. An agreement on the Presidency paper was preliminary reached on 22 September 2014 within the FOP and confirmed on 26 September 2014 by silence procedure (doc. 9967/4/14 REV 4). Given the strong preference expressed by Member States, the Presidency decided to prepare draft Council conclusions on Cyber Diplomacy.

4. The complexity of the matter led to difficult and lengthy debates on the draft Council conclusions in search for a balance between the various aspects and the respective roles and competences of the various players. Additionally, account had to be taken of the parallel discussion and subsequent adoption of the Council Conclusions on Internet Governance, which is one of the subsets of cyber diplomacy, as well as of the reactions following terrorist attack in Paris.

5. Following a discussion at the meeting of the FOP on 8 December 2014, the compromise document (doc. 5223/1/15 REV 1) was submitted to delegations by silence procedure.

6. On this basis, COREPER is requested to invite the Council to approve the draft Council conclusions on Cyber Diplomacy, as set out in the Annex.

ANNEX

Draft Council Conclusions on Cyber Diplomacy

The Council of the European Union,

RECOGNISING that cyberspace issues, in particular cyber security, the promotion and protection of human rights in cyberspace, the application of existing international law, rule of law and norms of behaviour in cyberspace, Internet governance, the digital economy, cyber capacity building and development, and strategic cyber relations offer significant opportunities, but also pose continuously evolving challenges for EU external policies, including the Common Foreign and Security Policy,

AFFIRMING that the EU and its Member States should address these cross-cutting multifaceted issues with a coherent international cyberspace policy that promotes EU political, economic and strategic interests and continue to engage with key international partners and organisations as well as with civil society and the private sector,

UNDERLINING that such policy should build on existing policy documents, in particular the Council Conclusions on the Digital Agenda for Europe[1], on the first anniversary of the EU Strategic Framework and Action Plan on Human Rights and Democracy[2], on the EU Cyber Security Strategy[3], and on Internet governance[4],

---

1 doc. 10130/10 and doc. 9981/10 (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Agenda for Europe (COM(2010) 245 final)).

~~2~~ doc. 12559/13 and doc. 11855/12 (the EU Strategic Framework and Action Plan on Human Rights and Democracy).

3 doc. 12109/13 and doc. 6225/13 (Joint Communication to European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (COM JOIN (2013) 1 final)).

4 doc. 16200/14 and doc. 6460/14 (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Internet Policy and Governance Europe's role in shaping the future of Internet Governance (COM(2014) 72 final)).

BEARING IN MIND the recent terrorist attacks in France and AFFIRMING the need for a comprehensive approach in the fight against terrorism that includes various actions in different policies, including in the area of transport, finance, information technologies and in relations with third countries, as stipulated in the joint statement of the Justice and Home Affairs Ministers at their informal meeting held in Riga on 29 and 30 January 2015,

REAFFIRMING the EU's position that the same norms, principles and values that the EU upholds offline, notably the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention on the Rights of the Child and the EU Charter of Fundamental Rights, should also apply and receive protection in cyberspace,

RECALLING the crucial importance of promoting and protecting a single, open, free and secure cyberspace which fully reflects and respects the core EU values of democracy, human rights and the rule of law,

EMPHASISING the importance of trust through enhanced availability, security, reliability and interoperability of online communications and noting that the secure flow and handling of data is contributing to economic growth,

CONSIDERING that the growing number of international fora, bilateral and multilateral meetings and processes on cyberspace issues poses challenges to all stakeholders in ensuring appropriate participation,

ACKNOWLEDGING that developing an overarching and coherent narrative on EU cyber issues is crucial in the face of expanding and complex international discussions,

HEREBY

REGARDS as essential and crucial the further development and implementation of a common and comprehensive EU approach for cyber diplomacy at global level that:

- promotes and protects human rights and is grounded on the fundamental EU values of democracy, human rights and the rule of law, including the right to freedom of expression; access to information and right to privacy,

- ensures that the Internet is not abused to fuel hatred and violence and safeguards that the Internet remains, in scrupulous observance of fundamental freedoms, a forum for free expression in full respect of law,

- promotes a cyber policy informed by gender equality,

- advances European growth, prosperity and competitiveness and protects EU core values, inter alia, by strengthening cybersecurity and improving cooperation in fighting cybercrime,

- contributes to mitigation of cybersecurity threats, conflict prevention and greater stability in international relations through the use of diplomatic and legal instruments,

- promotes the efforts to strengthen the multi-stakeholder model of Internet governance,

- fosters open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures,

- promotes the sharing of responsibilities among relevant stakeholders, including through cooperation between the public and private sectors as well as research and academic institutions on cyber issues,

NOTES that these Council Conclusions are without prejudice to the distribution of competences between the EU and its Member States and the allocation of powers between the EU institutions,

AND

INVITES the EU and its Member States to work together, respecting each other's areas of competence and the principle of subsidiarity, in response to the strategic objectives set out in these Conclusions,

Promotion and Protection of Human Rights in Cyberspace

UNDERLINES that individuals' human rights and fundamental freedoms as enshrined in the relevant international instruments must be respected and upheld equally online and offline and WELCOMES the fact that this principle has been also affirmed by the UN Human Rights Council[5] and General Assembly,

CALLS UPON the EU and its Member States:

- to promote and protect human rights and fundamental freedoms in cyberspace, including freedom of expression, access to information, assembly and association, privacy, effective remedy and a fair trial and to strongly uphold and firmly defend their common positions in the relevant regional and global fora,

- to actively contribute to the enforcement of international human rights obligations in cyberspace,

- to protect human rights of victims of serious and organised crime in cyberspace by ~~to~~ promoting effective investigations and prosecutions, allowing competent authorities to gain timely access to electronic evidence, with full respect to international law and fundamental rights including the protection of personal data,

- to encourage exchanges of good practices on the promotion and protection of fundamental rights in cyberspace with all relevant stakeholders, in particular the freedom of opinion and expression and the right to privacy,

- to promote a universal, affordable and equal access to the Internet and in particular the empowerment of women and girls in policy development and use of Internet,

[5] A/HRC/RES/20/8.

INVITES the EU and its Member States to promote the implementation and make better use of the EU Guidelines on the Freedom of Expression online and offline and of the EU Guidelines on Human Rights Defenders, namely by:

- developing and promoting best practices to ensure respect for human rights online, including in the framework of the export of technologies that could be used for surveillance or censorship by authoritarian regimes,

- supporting the efforts of third countries to increase and improve their citizens' access to and secure use of information and communication technology (ICT) and the Internet,

- raising awareness and empowering stakeholders to use ICT and the Internet to promote human rights and fundamental freedoms in cyberspace,

Norms of behaviour and application of existing international law in the field of international security

WELCOMES the work done within the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, notably its 2013 report[6], and the consensus achieved that international law, in particular the Charter of the United Nations, is applicable to cyberspace and is essential to reduce risks and maintain peace and stability,

WELCOMES the adoption of a first set of Cyber Security Confidence Building Measures in the OSCE[7] framework and LOOKS FORWARD to their implementation as well as to the development of measures aimed at enhancing confidence and cooperation,

REITERATES the EU's and its Member States' commitment to actively support the development of such measures, through a consolidated and coordinated approach and including in other regional fora such as the ASEAN Regional Forum to reduce the risk of misperceptions in their relations and encourages greater Member States' engagement to this end,

---

6 A/68/98.

7 Permanent Council Decision No. 1106 on the initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies of 3 December 2013.

ENCOURAGES the EU and its Member States:

- to focus efforts in a coherent and coordinated manner and contribute actively to the achievement of a global common understanding on how to apply existing international law in cyberspace and to the development of norms for responsible state behaviour in cyberspace with a view to increasing transparency and trust, consistent with existing international law provisions,

- to strongly uphold the principles regarding State responsibility for internationally wrongful acts and to take the initiatives necessary at national, regional and international level to ensure that they are fully respected and enforced in cyberspace,

- to strongly uphold the position that existing international law is applicable in cyberspace,

EMPHASISES the key role played by the EU and its Member States in international cyberspace policy debates and events, such as the "London process" and its follow-up conferences in Budapest and Seoul, and ENCOURAGES them to continue their efforts to support the next Global Conference on Cyber Space in the Hague in 2015, by contributing to the positive development and progress of that process while ensuring consistency of the messages delivered from the EU side,

Internet Governance

RECALLS its recently adopted Conclusions on Internet Governance[8] which contain the EU's position on this issue and STRESSES the importance of those Conclusions given that Internet governance is an integral part of the common and comprehensive EU approach for cyber diplomacy,

Enhancing competitiveness and the prosperity of the EU

RECOGNISES that Internet and digital technology have become the backbone of economic growth of the EU internal market and a critical source which all economic sectors rely on,

UNDERLINES the need for the EU to advance the digital single market and to promote its regulatory framework in order to further develop competitive and sustainable European digital enterprises and e-commerce,

[8] doc. 16200/14.

EMPHASISES that the digital economy can only reach its true potential by ensuring the protection of data online as well as of the underlying infrastructure and areas that face increasing opportunities and challenges with innovative technologies such as cloud, mobile and social computing and analytical tools applied to Big Data,

ACKNOWLEDGES the importance of cross-border data flows for promoting growth and economic development and of ensuring trust through the availability, security, reliability and interoperability of online communications,

ACKNOWLEDGES the importance of the EU in playing an active role in ICT standard setting, pursuing as far as possible the development of global or globally interoperable standards ensuring a high level of security, promoting competitive, cross-border online trade and new business models through inclusive and bottom-up processes and taking into account the on-going work in the OECD framework, including on taxation-related issues,

ENCOURAGES the EU and Member States together with the private sector, technical and academic communities and civil society to work towards the enhancement of open, interconnected and trustworthy solutions to create a dynamic, competitive and conducive environment for European industries and services ensuring that the EU stands out as a global player and as a market for investment and innovation,

INVITES the EU and its MS:

– to place specific emphasis on further promoting the EU digital single market and enhancing IT security, promoting digital trust and enabling greater use of ICTs and ICT driven growth;

– to move forward the relevant negotiations within the respective international and multilateral fora as well as to support the inclusion of the digital economy in their respective agendas;

– to systematically consider addressing challenges related to data protection in cooperation with key international partners and countries, and to maintain a high level of IT-security, including relevant standards, and in doing so, to explore the avenues to promote the interoperability and portability of users' content and data between different digital platforms;

– to promote the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as a minimum standard for data protection in third countries,

– to support market access in a spirit of reciprocal and mutual benefit with third countries when negotiating free trade agreements taking into account EU values and norms, including data protection,

Cyber capacity building and development

REITERATES the importance of cyber capacity building in third countries as a strategic building block of the evolving cyber diplomacy efforts of the EU towards the promotion and protection of human rights, rule of law, security, growth and development,

EMPHASISES the importance of access to and use of open and secure ICTs for enabling economic growth and innovation, accelerating progress and driving political, social and economic development worldwide,

RECOGNISES the need to promote the rule of law and to combat the increase in organised crime and unlawful acts in cyberspace, in line with human rights law and international mutual legal assistance agreements,

CONTINUES promoting the Council of Europe Convention on Cybercrime as a framework for international cooperation,

STRONGLY ENCOURAGES the EU and its Member States to:

– develop a coherent and global approach to cyber capacity building, which on one side brings together technology, policy and skills development within a broader and overreaching EU development and security agenda, and on other side facilitates the design of an effective EU model for cyber capacity building;

– make cyber capacity building an integral part of wider global approaches in all cyberspace domains, including through close cooperation with academia and the private sector as well as European Union Network and Information Security Agency (ENISA), the European Cybercrime Centre within Europol and the EU Institute for Security Studies[9]

[9] Within their respective mandates.

– support new initiatives on cyber capacity building that take stock of, build on, and complement existing initiatives emphasising the importance of access to and use of unhindered, uncensored and non-discriminatory use of open and secure ICT for fostering open societies and enabling economic growth and social development;

– promote sustainable cyber capacity building, when appropriate, together with international partners, as well as streamlining and prioritising funding, including by making full use of the relevant EU external financial instruments and programmes;

– promote the Council of Europe Convention on Cybercrime internationally as the legal framework of reference for international cooperation in fighting cybercrime at a global level and support third countries to accede to the Convention and to introduce a minimum national legal framework to combat cybercrime as well as to develop the necessary investigation and prosecution capacities;

– tackle growing cyber threats and challenges by increasing resilience of critical information infrastructure and by reinforcing close cooperation and coordination among international stakeholders through initiatives such as the development of confidence building, common standards, international cyber exercises, awareness-raising, training, research and education, incident response mechanisms,

– leverage the expertise of national cyber organisations, including computer security incident response teams, high-tech crime units and other competent national bodies,

Strategic engagement with key partners and international organisations

RECOGNISES that due to the global cross-cutting nature, scope and reach of the digital realm, most of the policy decisions on cyberspace-related issues have international implications that necessitate active international engagement, collaboration and coordination in the EU,

EMPHASISES that many recent cyberspace developments have taken place in different international organisations, in particular the UN, Council of Europe, OSCE, OECD, NATO, AU, OAS, ASEAN, ARF, etc.,

ENCOURAGES the EU and its Member States to prepare cyber dialogues within the framework of effective policy coordination, avoiding duplication of efforts and taking into account the broader EU political and economic interests, collectively promoted by all EU actors,

RECALLS that structured and overarching EU strategic cyber consultations have already been launched with the US, China, Japan, India, South Korea and Brazil, and that negotiations to launch such discussions are currently on-going with other partners; in addition numerous sectorial dialogues are on-going on ICT, organised crime and human rights, with the aim of building trust and confidence as well as providing platforms for exchanging best practices, promoting human rights and the rule of law, improving security and tackling issues of common concern,

REAFFIRMS the call in the EU Cybersecurity strategy:

- to seek Member States' cyber policy expertise and their experience from bilateral engagements/cooperation to develop common EU messages on cyberspace issues,

- to work towards achieving a coherent EU international cyberspace policy by increasing engagement with key international partners and organisations, by improving coordination of global cyber issues, mainstreaming the strategic external relations and improving internal consultations;

- to support the creation of relevant national policies, strategies and institutions in third countries with the aim of enabling the full economic and social potential of ICT, developing resilient systems and mitigating cyber risks for the EU;

INVITES the EU and its Member States:

– to ensure that the European activities in cyberspace and national policies, law and initiatives are designed in a way to allow for a coherent approach and avoid duplication;

– to improve coordination of dialogues with partners and to engage them in bilateral, regional or global settings;

– to maintain close relations with the relevant international organisations where the major cyber developments are taking place;

– to engage civil society organisations, the private sector, technical and academic communities, where appropriate, in shaping and implementing EU cyberspace policy;

– to share information on their bilateral cyber consultations,

AND

ENCOURAGES the EU and its Member States to support on-going implementation of these Conclusions by keeping EU strategic objectives under constant review and by setting up EU cyber diplomacy policy priorities,

INVITES the Member States, the Commission and the High Representative to regularly report to the Council on the implementation of these conclusions and ENCOURAGES the regular collaboration between the competent Council preparatory bodies, in particular with the Friends of the Presidency Group on Cyber Issues which should continue serving as a comprehensive cross-cutting forum for EU cyber policy coordination and cooperation.