Council of the European Union

Brussels, 23 September 2014
(OR. en)

9967/4/14
REV 4

LIMITE

CYBER 29
RELEX 443
JAIEX 39
TELECOM 121

NOTE

From:	Presidency
To:	Friends of the Presidency Group on Cyber Issues
Subject:	**An outline for European Cyber Diplomacy Engagement**

Following the last discussion and negotiations within the meeting of the FOP Group on Cyber issues held on 22 September, the Presidency prepared a final version of the Cyber Diplomacy paper, preliminarily agreed by delegations, as set out in the Annex.

The text is put under silence procedure until **Friday 26 September 12.00** - Brussels time.

The present paper addresses neither the procedures for the establishment of the Union position in the EU's external relations on cyber matters in each context, nor the issues of external representation of the Union, and is thus without prejudice to the allocation of powers between the EU institutions. Furthermore, the use of the terms EU and/or Member States in this paper is without prejudice to the distribution of competences between the EU and the Member States.

ANNEX

An outline for European Cyber Diplomacy Engagement

Cyberspace issues became central to the EU's external agenda as a growing number of international fora address various issues related, inter alia, to cyberspace engagement and norms of behaviour, applicability of rule of law and human rights law in cyberspace, cybersecurity capacity building and Internet Governance. The EU and its MS have played a key role and brought an added value in many of these international cyber policy debates and achievements to date. In order to continue being a valuable player and contributor in the relevant fora shaping the cyberspace policy, the EU and its MS should, with a sense of urgency, focus their efforts on formulating a coherent and comprehensive cyber diplomacy policy.

As the EU is moving towards a global, networked, knowledge, industry & service-based economic model, it is important to ensure that the prospects for wider economic and social benefits of the digital domain are not undermined. Conscious of the huge potential for progress, growth, development and transformation of new digital technologies, but also of the constantly evolving challenges they pose to the various spheres of life, the EU must commit to put in place efforts to a sustainable and focused co-ordination process with a view to formulating appropriate and coherent policy responses. The latter should not only seek to tackle successfully these challenges, but also to attain the strategic goals of the EU, in particular those of its foreign policy, keeping pace with the ever shifting international landscape and mindful of the divergent positions and interests of the other players.

Information and Communications Technologies (ICTs) are becoming the fabric of our economy and societies, so in a way all public policies, including their international dimension, become more or less connected to cyberspace. This makes it more than necessary to establish a coherent and global EU diplomacy policy related to cyberspace (EU cyber diplomacy policy). Therefore the present paper aims to outline the key elements for an international cyber diplomacy engagement of the EU and its MS as well as to provide political guidance for their future bilateral and multilateral contacts on various cyber issues ranging from security, capacity-building and human rights to industry, growth and prosperity.

Such outline builds upon the existing policy documents, in particular the EU Cyber Security Strategy and the Council Conclusions on it, the EU Strategic Framework on Human Rights and Democracy and relate, inter alia, to Commission's Communication on Internet policy and governance of 12 February 2014[1]. In practice it also strives to further one of the foreign policy priorities set out by the European Council at its meeting on 26-27 June 2014 in the Strategic Agenda for the next five years[2], namely of the EU as a strong global actor to engage with its global strategic partners.

[1] COM(2014) 72 final.
[2] EUCO 79/14 CO EUR 4, CONCL 2 (Annex I).

The building blocks of the EU's cyber diplomacy engagement, as set out in the paragraphs below, have to fully reflect, respect and guarantee the core EU values of democracy, human rights and the rule of law as well as to ensure and protect its political, economic and strategic interests.

1. Applicability of rule of law and human rights law in cyberspace

The EU and its MS must defend the rule of law as a founding principle fully valid in cyberspace. They should also maintain that the universal applicability of the rights enshrined in international law, in particular the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), the EU Charter of Fundamental Rights and other relevant international human rights instruments extends also to cyberspace as affirmed by the UN Human Rights Council.

The EU and its MS should make further efforts to uphold the rule of law principle and human rights law and to ensure that they are fully respected and enforced in cyberspace and should further reflect on the activities necessary in this regard at regional and global level.

The EU Human Rights Guidelines on Freedom of Expression Online and Offline adopted recently by the Council[3] reiterate the support for the promotion and protection of all human rights online, including the freedom of expression. Some major elements are the development of best practices with regard to exports of technologies that could be used for censorship or mass surveillance online by authoritarian regimes; development of measures and tools to increase and improve Internet access; and the use of media and ICT by stakeholders to promote and protect human rights.

The EU Guidelines on Human Rights Defenders of 2008 are seeking to enhance the ability of journalists, other media representatives and human rights defenders to operate effectively, without undue constraints in the online environment. The tools provided therein might be useful in contacts with third countries as well as in multilateral human rights fora, in order to support and strengthen on-going efforts by the EU to promote and encourage respect for the right to defend human rights.

The EU and its MS, in their external relations, should:
- encourage the participation of civil society, including NGOs, the private sector and academia in the international decision-making procedures on issues which affect the applicability of human rights law in cyberspace;
- promote, and make better use of, the tools provided in the EU Human Rights Guidelines on Freedom of Expression Online and Offline and the EU Guidelines on Human Rights Defenders.

The rights to privacy and to protection of personal data are enshrined in a number of human rights instruments, in particular the UDHR, ICCPR, ECHR and the EU Charter of Fundamental Rights and their application concerns personal data both provided by an individual or obtained as a result of profiling technologies use. Some elements related to the application of these rights in cyberspace have been addressed in recent ECJ case-law and its consequences on the future of the European personal data protection framework should be fully considered.

[3] doc. 9647/14.

The EU and its MS should further reflect on how unlawful invasions of privacy and unlawful and arbitrary access to personal data enabled by new technologies could be further combatted, thus supporting a high standard of protection of our fundamental rights and freedoms.

2. Norms of behavior in cyberspace

Mindful that new technologies can be used for both legitimate and malicious purposes, the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the context of International Security noted in its 2013 report that the absence of common understandings on acceptable state behaviour with regard to the use of ICTs increases the risks to international peace and security[4]. The report further stated that international law, especially the UN Charter, is applicable and is an essential measure to reduce those risks as well as to maintain peace and stability and promote an open, secure, peaceful and accessible ICT environment. GGE also agreed that States should intensify cooperation against criminal or terrorist use of ICTs, assume obligations regarding internationally wrongful acts attributable to them, and strengthen practical collaboration between respective law enforcement and judicial authorities. However, improved security should not come at the expense of fundamental human rights. The upcoming GGE meetings are expected to continue the discussions on these issues.

The EU and its MS should seek to contribute to the achievement of common understandings on how to apply existing international law, including in cyberspace, and develop norms for state behaviour in cyberspace.

Where possible the norms of behavior should derive from current international law and pave the way for its wider application.

International dialogue on norms of behavior in cyberspace was held during the G8 Summit in Deauville in 2011 and in the so-called London process of the same year. The latter establishes an important narrative that EU supports in promoting open, free and accessible cyberspace, with a free flow of information, where freedom of expression, privacy, property and other core EU values are respected and protected and governments act proportionately in accordance with national and international law. The follow-up Conferences on Cyberspace held in Budapest, 2012 and Seoul, 2013 clearly outlined and recognized the driving force of cyberspace in accelerating progress towards political and economic development worldwide. A consolidated EU approach in particular on norms of behaviour, which brings closer MS positions within the various fora dealing with cyberspace issues, is desirable and would bring an added value to EU's active participation.

[4] UN document A/68/98 available at http://www.mofa.go.jp/files/000016407.pdf

Looking forward to the follow-up Global Conference on Cyberspace in the Netherlands, in April 2015, the EU and its MS should seek to contribute to the positive development and progress of that process as well as to ensure consistency of the messages delivered from the EU side regarding the norms of behaviour in cyberspace.

The EU Cybersecurity Strategy outlines that existing international legal instruments, in particular the Budapest Convention on cybercrime, International Humanitarian Law and Human Rights Law provide a legal framework that is applicable also in cyberspace.

The EU and its MS should make efforts to ensure that the existing legal instruments are upheld in cyberspace and should continue reaffirming their position of not calling for the creation of new international legal instruments for cyber issues. In this regard, they should continue promoting the universalisation of the Budapest Convention.

The adoption of an initial set of Confidence Building Measures (CBMs) to reduce the risks of conflicts stemming from cyberspace in the framework of the Organisation for Security and Cooperation in Europe (OSCE) was another notable development in 2013, where the EU played a substantial coordination role among the OSCE participating states. The EU and its MS are already engaging other regional forums such as the UNASUR and ASEAN Regional Forum with a view to supporting the development of initial set of cyber CBMs among their respective countries.

Mindful that these processes are still in an early stage of their development and substantial deliberations are expected in the years to come, the EU and the MS should on the basis of a coherent cyber policy support these processes as well as the implementation of the initial set of CBMs and the development of an additional one in the framework of the OSCE.

3. Cyber capacity building

Confirmed by the EU Cybersecurity Strategy, capacity building should feature prominently in the EU's evolving cyber diplomacy engagement. A broad capacity building effort is strategically important to strengthen the positive narrative of promoting and safeguarding freedom and security, growth and development in cyberspace. Efforts for cyber capacity building need to go hand in hand with a broader development aid component.

In this regard, the EU and its MS should:
- maintain a coherent holistic approach, drawing together technology, policy and skills development, which is to be integrated within the EU's broader development and security agenda;
- emphasise the importance of access to and use of unhindered, uncensored and non-discriminatory, open and secure ICTs for fostering open societies and enabling economic growth and social development;
- make cybersecurity capacity building an integral part of wider global approaches in all cyberspace domains notably through close cooperation with academia and private sector as well as further development and use of ENISA and EC3/EUROPOL potential;

- *support new initiatives on cybersecurity capacity building that take stock of, build on, and complement current initiatives and increase global commitment to promoting sustainable cyber capacity building, as well as provide a stimulus for streamlining and expanding funding for cybersecurity capacity building;*

- *develop priorities for selection of recipient third countries.*

The EU has started already its first cybersecurity capacity building projects, engaging with global partners in its cybersecurity capacity building efforts. In 2014, an EU cybersecurity project "Enhancing cybersecurity: protecting information and communication networks" was launched with the aim of enhancing the resilience of critical ICT infrastructures in selected countries in South-East Europe and Western Balkans. In November 2013, the "Global Action on Cybercrime (GLACY) project" was launched to serve as a global facility that will respond to the need for capacity building initiatives in the area of fighting cybercrime in developing countries. Both projects are financed by the long-term component of the EU Instrument contributing to Stability and Peace whereas the second one is co-funded by the Council of Europe.

The EU and its MS should continue promoting the Budapest Convention as a model for drafting national cybercrime legislation and as a basis for international cooperation. They should strongly encourage its application as an important element of the cybersecurity capacity building effort in the various countries world-wide and should put further efforts in designing an effective EU model for cybersecurity capacity building.

4. Internet Governance (IG)

In 2014, major IG events are being held. The Global Multi-stakeholder Meeting on the Future of Internet Governance (NetMundial) in April adopted a set of principles and a roadmap for the further evolution of the IG ecosystem. In October, the ITU's Plenipotentiary Conference will further deliberate on the future potential role of the organisation in areas related to IG.

In the course of the WSIS+10 process, stakeholders are reviewing the WSIS outcomes. In the framework of the UN Commission of Science and Technology for Development, proposals for new IG mechanisms have been debated. In deliberations at the UN General Assembly, the Resolution on the modalities for the overall review of the implementation of the outcomes of the WSIS has been adopted[5].

It is expected that the definitions of IG models and existing policy frameworks will be further discussed focusing primarily on the authority, participation and potential primacy of the different stakeholders and that those actors preferring a top-down, government controlled scheme of IG will try to challenge the current multi-stakeholder model. This model, supported by the EU and its MS, is expected to include both public and private actors as well as to duly take into account legitimate public interests.

[5] Resolution No A/RES/68/302.

The EU and its MS should continue working on IG issues in order to:
- present their coherent voice in these ongoing debates and continue promoting, supporting and further strengthening a multi-stakeholder model, which is more accountable, transparent, inclusive and balanced without undermining the strengths and flexibility of the existing Internet organisations that have built an easily accessible, free and open Internet which is crucial for economic growth and social empowerment;
- maintain the view that no single entity, company, organisation or government should seek to control the digital domain or dominate activities in the cyberspace;
- argue that IG debates on the technical questions of assigning names and numbers may be successfully dealt with, at least at the technical level, within private organisations, provided that they ensure a fair multi-stakeholder representation and that public interests are being addressed effectively whenever relevant (such as security, intellectual property, geographic indications, protection of individuals and of children, etc.).

5. Enhancing the competitiveness and promoting EU economic interests

ICTs have become the backbone of the economic growth of the EU internal market and are a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport while many business models are built on the uninterrupted availability of Internet and the smooth functioning of information systems. Enhancing openness, connectivity and trustworthy solutions, while making most use of the borderless Internet, will create a dynamic competitive environment to ensure that the EU stands out as a location.

While considerable progress has been made, there are still elements of lack of trust between consumers and companies in relation to commercial transactions online or in the digital domain in general. This regards the identity of the other party, the trustworthiness of an online offer, the security of ICT products, the means of redress or the way their data will be used, processed and stored. This adds to the problems deriving from software or ICT systems vulnerability or linked to users exposure to viruses, cyber attacks, spyware, malware and the related thereto data loss or identity theft.

The EU and its MS should continue their commitment towards the development and maintenance of competitive and sustainable cyber-related industries and services. In this respect, they should:
- place specific emphasis on further promoting the digital single market and take related issues forward within international fora supporting market access in a spirit of reciprocity and mutual benefits as well as when negotiating free trade area agreements with third countries;
- put efforts to increase the digital trust as precondition for greater use of ICTs and ICT driven growth;
- support the inclusion of the digital economy in the World Trade Organisation agenda and the process for revision and expansion of the Information Technology Agreement.

New standards in the digital domain should promote competition, cross-border online trade and new business models also taking into account the ongoing work in the OECD framework, including on taxation-related issues.

The EU and its MS should aim for an active role in standard setting, pursuing as far as possible the development of global standards through competitive, bottom-up processes.

For the digital economy to truly reach its potential, improving the safety of data is a key requirement. The EU must be able to fully seize the increasing opportunities, but also to face the serious challenges entailed by such innovative technologies as cloud, mobile and social computing, free movement of data through physical borders, Big Data and associated analytical tools.

The EU and its MS should systematically consider addressing the serious challenges related to the protection of data in cooperation with key international partners and countries.

6. Strategic engagement with key partners and international organisations

In view of the global nature, scope and reach of the digital domain, most policy decisions on cyberspace related issues have international implications, necessitating active international engagement and collaboration. Structured EU cyber consultations have already been launched with the US, China and India. Discussions on opening up cyber dialogues with Japan, South Korea, Brazil and a number of other countries are taking place. In this regard, careful consideration should be given to avoiding overlaps with any on-going dialogues in which cyber issues are already being discussed.

This cooperation is expected to build trust and confidence, as well as to provide platforms to exchange best practices, improve security and tackle issues of common concern. This would allow the EU to further promote its core values in the cyber domain as well as to refine and retool its development, security and capacity building agenda.

The EU and its MS should:
- prepare all cyber dialogues within a framework of effective policy coordination;
- play a coordination role with regard to "ad hoc" dialogues with key partners (e.g. Sino-European Track 1,5 dialogue);
- share information on bilateral cyber consultations; and
- engage key partners in bilateral, regional or global settings and maintain close relations with other relevant international organisations where recent cyber developments are taking place (e.g. Council of Europe, OSCE, OECD, UN, NATO, AU, OAS, ASEAN, ARF and others).