13 April 2011

EU-US WORKING GROUP ON CYBER-SECURITY AND CYBER-CRIME

- CONCEPT PAPER -

1. POLICY CONTEXT

The **EU-US Working Group on Cyber-security and Cyber-crime (EU-US WG)** was established in the context of the EU-US summit of 20 November 2010 held in Lisbon to "*tackle new threats to the global networks upon which the security and prosperity of our free societies increasingly depend*". The EU-US WG "*will address a number of specific priority areas and will report progress within a year*"[1].

2. POLICY AREAS AND OBJECTIVES

The objectives and priority areas of the EU-US Working Group are at Annex I. It will work on the basis of an overall roadmap (Annex II) and specific deliverables as stated below:

(1) **<u>Cyber Incident Management</u>:** develop a cooperation programme and a roadmap, including joint activities, towards synchronized and coordinated cyber incident exercises in the EU and the US (starting with desk-top exercise) in 2012-2013.

Scope of the activity:

– develop broad scenarios;

– share good practices for promoting the resilience and stability of networks;

– exchange good practice on how to work and cooperate across sectors; engage with other countries; exchange information between Governments.

Expected Deliverables:

– In anticipation of a joint US-EU cyber exercise, develop and conduct a cyber exercise workshop to convey past experiences and technical expertise with all phases of large-scale cybersecurity exercise;

– A cooperation programme providing for synchronized and coordinated cyber exercises in the EU and US, culminating in a joint cyber exercise in the timeframe 2012-2013;

– Alignment plan for developing country capacity-building on cybersecurity incident management.

[1] Joint Statement of the EU-U.S. Summit - 20 November 2010 - Lisbon: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597&type=HTML

The activity may also produce technical briefings/reports on specific topics such as best practises and standards to support cyber incident management; guidelines for information exchange between Governments as well as between Governments and the private sector, etc.

(2) **Public – Private Partnerships (PPP):** develop compatible approaches to public-private partnerships based on:

(a) key assets, resources and functions needed to ensure the continuity of electronic communications services;

(b) good practises (including baseline requirements, if appropriate) for the security and resilience of vital ICT infrastructures based on risk management;

(c) shared coordination and cooperation mechanisms to prevent, mitigate and react to cyber-disruptions and cyber-attacks.

While PPP represents a specific priority area, it also cuts across all other priority areas, and thus may be included in work in those areas as well.

In addition, the engagement of the private sector in collaborative efforts will be sought as appropriate.

Scope of the activity:

- Examining issues related to the resilience and stability of the Internet[2];
- Review and analyse good practice/initiatives and models for national PPPs (Analysis: Summer 2011);

Priority areas of focus for joint activities would include: fighting botnets, on-going information sharing with industry (including how to quickly inform businesses of ongoing threats) and control systems security including SCADA for smart grids. Additionally, exploratory discussion may address security of DNS, BGP, routing tables and undersea cables.

Expected Deliverables:

- Briefings/reports on specific topics of mutual interest including best practices and models to engage with the private sector; national approaches/programs for addressing botnets; private sector cybersecurity good practices; legislative developments; and others, as identified.
- A strategy and an action plan to engage the private sector in cooperative activities with governments, on selected areas, including development of agreed guidelines, principles, best practices, and/or standards.
- Common principles and guidelines on the resilience and stability of the Internet as well as on a reliable access to it. [3]

[2] *European Principles and Guidelines for Internet Resilience and Stability*, version of March 2011.

[3] Building on *European Principles and Guidelines for Internet Resilience and Stability*, version of March 2011.

(3) **Awareness Raising:** coordinate awareness raising activities to enhance efficacy and increase impact.

Scope of the activity:

- Share government awareness raising messages and models;
- Exchange experience on awareness models and mechanisms, in particular on how best to involve intermediaries (e.g. Internet Service Providers, technology providers, etc.) in the delivery of messages to users about on-line behaviour and in the development and delivery of awareness-raising materials;
- Exchange expertise and materials for joint events across the Atlantic.

Expected Deliverables:

- A programme for immediate joint awareness raising activities;
- A roadmap towards synchronized annual awareness efforts, to include a month by month calendar of messaging opportunities.

(4) **Cybercrime:**

- **Develop cooperation toward removing Child Pornography from the Internet, including a Roadmap for improving effectiveness of these efforts. The roadmap would identify:**

  - Channels and their effectiveness for notice and take-down of websites containing apparent child pornography images, and how they relate to channels for prosecution; solutions to improve the functioning of notice and take-down procedures including setting minimum standards (time limits for the takedown since receiving the notice);
  - Technological solutions to detect previously identified child pornography images from all locations on the Internet.

Expected deliverables:

- Summer 2011experts meeting, for first steps and overview of existing channels and technological solutions.

- **Programme for eliminating illegal use of Internet resources,** such as Internet Protocol (IP) addresses and DNS (domain names):

  - Coordination of EU/US efforts to get law enforcement recommendations endorsed by the Internet Corporation for Assigned Names and Numbers (ICANN's) Governmental Advisory Committee (GAC) in June 2010 and included in the 2011 GAC Scorecard of outstanding issues related to the introduction of new generic Top Level Domain names (gTLDs) approved by ICANN Board of Directors.

- Collaborate, directly and through the GAC, with ICANN on roadmap for implementation of law enforcement recommendations, to include alternative tools to more effectively implement specified recommendations; (implementation by DNS registrars and registries of Top Level Domain names).
- Highlights of critical issues discussed and conclusions on the follow-up after each EU-US expert meeting to be disseminated to law enforcement and industry in order to raise awareness of problems related to the abuse of Internet resources.
- Coordinate EU/US efforts with the EU/US Regional Internet Registries, ARIN and RIPE NCC, to ensure IP addresses are allocated, assigned and recorded in the most secure and stable manner.

Expected deliverables:

- Expert meeting with the US, held in February 2011;
- Participation in GAC/ICANN meetings in 2011;

- **Advancing the Council of Europe (COE) Convention on Cybercrime**, to strengthen global cybercrime response and attract an even broader group of nations to become parties to the Convention :

  - Encourage EU and CoE Member States to rapidly become parties (if possible before the 10th anniversary celebration of the Convention in November, 2011);[4]
  - Encourage pending non-European countries rapidly to become parties (in advance of November, 2011)[5].

Expected deliverables:

- Non-party EU states to produce statements of positions and plans for becoming parties;
- Plan for statements by ministers to secure EU and non-EU parties.

(5) Outreach

In addition, the Working Group will consider options for outreach to other regions, countries or organisations which are addressing similar issues, in order to share approaches and related activities and avoid duplication of effort.

[4] Andorra, Austria, Belgium, Czech Republic, Georgia, Greece, Ireland, Lichtenstein, Luxembourg, Malta, Monaco, Poland, Russia, San Marino, Sweden, Switzerland, Turkey, the United Kingdom.

[5] Canada, Japan and South Africa (all three countries participated in the drafting of the Convention and have an Observer status), and countries formally invited to accede: Argentina, Australia, Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines

This external dimension will be added to the agenda of the WG and of the Expert Sub Groups[6] (ESGs) meetings to examine options.

The EU and US take coordinated positions in some international fora, such as the UNODC expert group on cybercrime. Consideration should also be given to facilitating joint approaches in other international fora.

(6) Further objectives and priorities

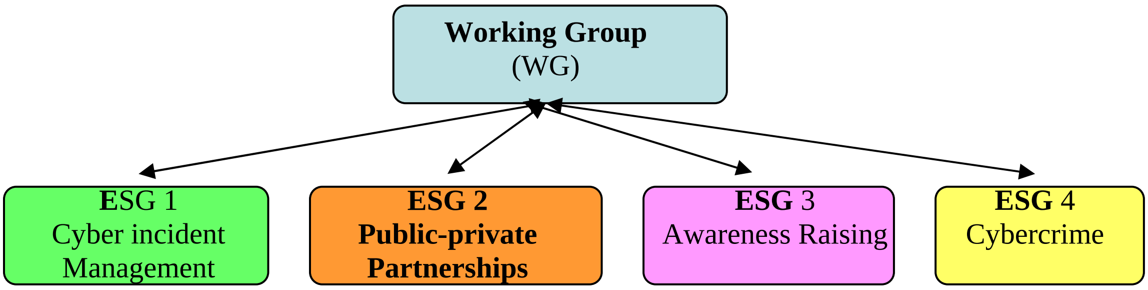
Further objectives and priorities can be added to the remit of the Working Group, and further ESGs created if necessary, by mutual agreement at any time.

In this regard, candidate areas could include foreign policy and security aspects, complementarity with NATO, and capacity-building assistance to improve the institutional and infrastructural resilience of third countries.

3. Working Method

3.1. Governance and composition of the Working Group (WG)

Below is the overall structure of **EU-US Working Group** based on the activities listed in Annex I. The activities in specific areas will be conducted primarily via **Expert Sub-Groups (ESGs)**.



The Working Group (WG) takes stock of the progress of the ESGs. It meets in ad hoc formats to manage the activity (at the senior officials' level). As well, as appropriate, it gets the necessary political steering and guidance on the political level[7]. The WG may decide to combine the ESGs as appropriate.

The WG meets according to the provisional roadmap provided in Annex II.

[6] See Section 3

[7] Guidance will be provided on the US side by: Secretary of State; Attorney General; Secretary of Homeland Security; and the Special Assistant to the President and Cybersecurity Coordinator; and, on the EU side by European Commission Vice-President for the Digital Agenda; Commissioner for Home Affairs; the Presidency of the Council; the High Representative of the Union for Foreign Affairs and Security Policy; and, the offices of the President of the European Council and of the President of the European Commission.

All configurations (WG, ESG) get their political guidance and high-level decisions formally approved from their respective political authorities, who shall in parallel maintain their EU-US bilateral contacts as appropriate.

3.2. Governance and composition of the Expert Sub-Groups (ESG)

Each ESG is composed of officials from relevant EU and US Departments/Agencies/ Services as well as experts selected on an *ad hoc* basis. They are co-chaired by EU and US officials[8]. They organize and steer the work of the ESG as well as report progress to the WG level. It is anticipated that each ESG would:

- define its own working methods and detailed agenda, and roadmap;
- meet physically at least 2-3 times and/or use appropriate communication means (video/phone conference calls, etc.).

Participation in ESGs would include:

– **EU side**: European Commission relevant Directorates General (INFSO, HOME), the European External Action Service - EEAS (former European Commission Directorate General RELEX), the Presidency of the Council, the EU Counter-Terrorism Coordinator, the EU representation office to the US, the EU relevant agencies (ENISA, EUROPOL, EUROJUST). In addition, experts from the EU Member States' competent national authorities may also participate[9].

– **US side**: the Department of Homeland Security (DHS), including the US Secret Service (USSS) and Immigration and Customs Enforcement (ICE); the Department of Commerce (DoC), including National Telecommunications and Information Administration (NTIA) and National Institute of Standards and Technology (NIST); the Department of State (DoS); the White House / National Security Council (NSC); the Department of Justice (DoJ), including the Federal Bureau of Investigation (FBI).

[8] The ESG co-chairs are A. Servida (DG INFSO) and [US counterpart] for ESG 1-3, and J.Boratynski (DG HOME) and B. Shave for ESG 4.

[9] EU Member States are also regularly informed of the developments either at COREPER or, if appropriate, in the Working Group via the Transatlantic Relations Working Group (COTRA), via the European Forum for Member States (EFMS) for what concerns the cybersecurity aspects, and via the Task Force of heads of cybercrime units (ECTF) for what concerns the cybercrime aspects.

ANNEX I

EU-US SUMMIT: COOPERATION ON CYBERSECURITY AND CYBERCRIME

The EU and the U.S. are establishing a *Working Group* on Cybersecurity and Cybercrime to evaluate and coordinate opportunities for enhanced collaboration and to focus on outcomes in the following priority areas:

- **Public – Private Partnerships**

  This area would focus on providing a coherent environment for cooperation between the public and private sector in the EU and the U.S.

  This area would also include a focus on the protection and resilience of critical information infrastructures from a cybersecurity perspective including enhancing the security of and reducing the cyber risk to networked industrial control systems.

- **Cyber Incident Management**

  This area would focus on cyber incident response and enhanced collaboration between national/governmental computer security incident response teams (CSIRT) in Europe and the US. Cybersecurity exercises, to include regional exercises and a possible synchronized trans-continental exercise in 2012/2013, would also be included to evaluate incident management processes.

- **Awareness Raising**

  This area would focus on a sustained effort to raise awareness about cybersecurity and related cybercrime issues with key stakeholders in EU member states and in the US. This area would focus on developing coordinated activities with respect to awareness raising to enhance efficacy and increase impact.

- **Cybercrime**

  This area would also focus on continued relationship building and cooperation among law enforcement partners. In addition, this may address child exploitation online.

This Working Group may consider options for outreach to other regions or countries addressing similar issues to share approaches and related activities and avoid duplication of effort, as appropriate. It could also serve to facilitate a joint approach in international fora.