Council of the European Union

Brussels, 30 June 2016
(OR. en)

8732/1/16
REV 1

LIMITE

CYBER 47
RELEX 367
JAIEX 38
TELECOM 72
COPS 139
POLMIL 45

NOTE

From:	Presidency
To:	Delegations
Subject:	Cyber capacity building: towards a strategic European approach

In the Cyber Attaches meeting of 20 May 2016 and the Friends of the Presidency (FOP) Group on Cyber Issues meeting of 27 May 2016, delegations expressed support for developing a more coherent, strategic European approach on cyber capacity building.

Introduction

A secure and safe digital environment is a necessary condition for reaping the benefits of ubiquitous access to the Internet and the positive effect it has on economic and social development. The number of Internet users has more than tripled in a decade and the numbers of devices connected to the Internet has reached 15 billion in 2015.

As societies globally become increasingly digitized, it is of growing importance for states, private companies and international organizations to address the threats posed by malicious cyber activities and promote secure digital services and infrastructure. Cyber offers immense opportunities, which can only be used to their full potential if capacities to deal with these challenges are continuously strengthened, improved and shared among actors in the digital domain.

The EU is a strong supporter of the vision of a free, open and secure Internet as the basis for economic and social development. At the moment, not all parts of the world benefit from the positive effects of the Internet, in particular due to a lack of open, secure, ,interoperable and reliable access. The EU will therefore provide third states with necessary capacities to implement this vision for the Internet and will continue to support third countries' efforts in their quest to ensure access and use of the Internet for their people, guaranteeing its integrity and security and effectively fighting cybercrime.

Cyber capacity building is aimed at building functioning and accountable institutions in third countries which are a prerequisite for responding effectively to security threats and for enhancing resilience. It is an essential component of international cooperation; fostering international solidarity with a common vision and a common purpose − to secure a free, open and secure cyberspace for everyone − while ensuring compliance with human rights and the rule of law.

The EU and its Member States have made and are making substantial efforts to provide both the technical, organizational and financial means to build cyber in third countries. They should continue to approach cyber capacity building in a strategic manner and the EU should further integrate it in its diplomatic cyber strategy.

Cyber capacity building actions: EU policy framework

In line with the EU Cybersecurity Strategy of 2013, the EU and its Member States support cyber resilience – the capacity to withstand, stress and recover strengthened from challenges – of third countries with less developed cyber capacities to reap the potential of the Internet and close the digital divide. The Strategy stresses that Member States should step up their efforts to support cyber capacity building in third countries and foster international cooperation in cyberspace issues. This international cooperation includes exchanging best practices, sharing information, early warning joint incident management exercise and so on.

Furthermore, the Council Conclusions on Cyber Diplomacy of 2015: "*reiterate 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"*. The importance of cyber capacity building is repeated once more in the Joint Communication on Hybrid Threats of 2016, which highlights that capacity building actions to enhance partner countries' cyber-resilience and their abilities to detect and respond to cyber-attacks and cybercrime can also contribute to their overall capacity in countering hybrid threats.

Reflecting on cybercrime's borderless nature, the European Agenda on Security also foresees a specific action on "enh*ancing cyber capacity building action under external assistance instruments*". Capacity building in the fight against cybercrime and in support of cyber resilience is also linked to the EU's commitments under the 2030 Agenda for Sustainable Development which applies to all countries at all levels of development, and, inter alia, foresees the facilitation of "*sustainable and resilient infrastructure development in developing countries"* (target 9a) and the "*strengthening of relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime"* (target 16a).

There is a general consensus among the Member States that the EU should continue strengthening its role in providing cyber capacity building assistance to partner countries. Following the adoption of the EU Cybersecurity Strategy the Commission started pursuing a more comprehensive cyber-specific capacity building engagement globally, especially by utilising the Instrument contributing to Stability and Peace.

The need for cyber capacity building is also reflected in the Roadmap of the FoP Group on Cyber issues where capacity building on cybersecurity and resilient information infrastructures in third countries is one of the priority actions. The Member States actively contribute to policy debates on cyber capacity building within the FoP and other fora such as the WSIS +10 review and the UN GGE which examines cyber capacity building issues and the development of concrete and demand driven solutions.

Global Forum on Cyber Expertise

In addition to EU instruments, other initiatives have been undertaken in order to strengthen global commitment to cyber capacity building. One of these is the Global Forum on Cyber Expertise (GFCE), launched at the Global Conference on Cyber Space 2015 in The Hague. The GFCE, of which several Member States as well as the European Union are founding partners, is a platform to coordinate cyber capacity building efforts. Working within its vision and mandate, the GFCE recognizes the need to leverage knowledge, expertise and (scarce) resources to meet capacity building needs. The GFCE has a unique position to support and strengthen cyber capacity building efforts in countries, complementing to what countries undertake with their own resources and on bilateral level. It connects key actors globally and stimulates those actors to take up the responsibility for their own actions within their own field of expertise, thereby ensuring a broad representation of interests. The GFCE also has a long-term ambition to become agenda setting in the field of cyber capacity building.

Although not all Member States are partners of the GFCE, it is an instrument that is closely aligned with EU goals and strategies in the cyber domain and could be used to broaden the support of EU policies, especially in this area.

Leveraging cyber capacity building initiatives: towards a strategic EU approach

Cyber capacity building serves both short-term and long-term objectives important to the EU and its Member States:

- In the short-term, cyber capacity building helps to improve resilience of the cyber domain in third countries and inter alia improves access to information and to an open Internet, prevents and counter cyber threats, develops donor coordination for steering capacity-building efforts and supports their ability to benefit of the digital economy.
- In the short-term stronger cyber capabilities in third countries also strengthen the resilience of the cyber domain as a whole and help to mitigate threats at its place of origin. For example, stronger cybercrime legislation in countries where cybercrime originates from, provides opportunities to deal with cyber criminals in these jurisdictions and avoid impunity.
- In the long-term, investment by the EU in cyber capacity building helps to build strategic alliances aimed at supporting a free, open and secure Internet, reduce harm to Member States of cyber incidents and promote European norms and values as well as related EU policy objectives in the digital domain.

In light of this analysis, the Presidency would like to encourage a strategic approach of the EU and its Member States on the issue of external cyber capacity building and to fully integrate this approach in the next version of the EU Cyber Diplomacy Strategy. We believe the FoP could play an important role in strengthening the impact of cyber capacity building by bringing together the efforts of the Commission, the EAAS, other relevant EU bodies (in particular EC3 at Europol and ENISA), as well as efforts of Member States, both their bilateral programs as well as multistakeholder platforms like the GFCE.

As a starting point the EU and its Member States could consider the following short-term actions:

- Share information on their various initiatives to provide cyber capacity building to third countries and/or regional organizations.

- Explore options for improved coordination to steer cyber capacity building efforts, including by mapping of the various cyber capacity building initiatives of Member States as an action in the FoP Roadmap.

- Get better knowledge and make full use of EU financial instruments and programmes for cyber capacity building activities.

In order to support the strategic goals, the EU and its Member States could consider the following long-term actions:

- Consider using the mapping of existing cyber capacity building programs in the FoP as basis for enhanced coordination among EU and its Member States with a view to complement their efforts, to explore opportunities for joint actions as well as broaden their outreach in this field, and eventually serve as a clearing-house mechanism.

- Link various ongoing cyber capacity building efforts and different EU aid instruments for cybersecurity capacity building in different thematic areas (development, peace and security) and 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 ENISA, the EC3 within Europol and EUISS.

- Consider establishing a framework for exchange of best practices / internationally accepted recommendations for cyber capacity building based on lessons learnt from relevant policy areas, including, inter alia, from the EU's own internal cyber capacity building efforts and from long-established development cooperation principles. The GFCE, in collaboration with its members and partners, could help broaden the consensus for the development of internationally agreed upon and voluntary recommendations on cyber capacity building.

- Consider developing a methodological approach by setting criteria for the prioritisation of cyber capacity building actions, in terms of geographical focus and intervention areas, as well as providing technical expertise and funding for implementing these priorities. Such an effort could position the EU as a strategic player in this field.

Follow up

The Presidency considers important to bring this initiative further turning it into a strong component of the implementation of the relevant cyber policy instruments, in particular the EU Cybersecurity Strategy and the Council Conclusions on Cyber Diplomacy. The following steps could be taken in this regard:

1. Regular update on the issue in the FoP Group on Cyber Issues meetings by the relevant EU actors and Member States and inclusion of this initiative as action in the Roadmap.
2. Launch of a stock-taking and mapping exercise on the basis of the overview available in the GFCE (Annex).
3. Start of discussion on the possible way of defining what constitutes a cyber capacity building activity or project.
4. Launch a comparison exercise of the Member States' methodologies with the aim to define common grounds and/or ensure, to the extent possible, synergies among the various national approaches.

The Presidency encourages the FoP to address the issue of cyber capacity building as described above by dedicating time on its agenda and by regularly reviewing developments in this field.

FoP mapping list of cyber capacity building initiatives				
Initiators	**Name initiative**	**Target country**	**Target regio**	**Internal/External**
Hungary Hewlett Packard Netherlands Romania	GFCE: Coordinated Vulnerability Disclosure	Inapplicable	World	Internal
Netherlands Senegal UNODC	GFCE: Cyber Security Awareness	Senegal/Whole West-African region	West-Africa	External
ITU Microsoft Netherlands OAS	GFCE: CSIRT Maturity	Inapplicable	World	Internal/External
Netherlands Norway Spain Switzerland	GFCE: Critical Information Infrastructure Protection	Inapplicable	World	Internal/External
Kosciuzko Inst.Poland Netherlands Platform Internetstandards NL	GFCE: Internet Infrastructure	Inapplicable	World	Internal/External
Global Partners Digital Netherlands	Civil Society Capacity Building	Chile India Indonesia Kenya	South-America South-Asia Southeast-Asia East-Africa	External