147992/EU XXV. GP
Eingelangt am 20/06/17

Council of the
European Union

Brussels, 20 June 2017
(OR. en)

15233/1/16
REV 1 EXT 2

JAI 1056
COSI 221
ENFOPOL 475
CRIMORG 177
ENFOCUSTOM 226
COPS 374
RELEX 1040
JAIEX 115
GENVAL 139
CYBER 149

PARTIAL DECLASSIFICATION

of document:	15233/1/16 REV 1 RESTREINT UE/EU RESTRICTED
new status:	Public
Subject:	Operational Action Plan 2017 related to the EU crime priority G3: "Cyber Attacks"

Delegations will find attached the partially declassified version of the above-mentioned document.

www.parlament.gv.at

Council of the European Union

Brussels, 12 January 2017
(OR. en)

15233/1/16
REV 1

RESTREINT UE/EU RESTRICTED

JAI 1056
COSI 221
ENFOPOL 475
CRIMORG 177
ENFOCUSTOM 226
COPS 374
RELEX 1040
JAIEX 115
GENVAL 139
CYBER 149

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	15219/16, 12759/3/13 REV 3, 14857/1/15 REV 1
Subject:	Operational Action Plan 2017 related to the EU crime priority G3: "Cyber Attacks"

Delegations will find in annex the Operational Action Plan 2017 regarding the EU crime priority G3: "Cyber Attacks", **NOT DECLASSIFIED**, which was agreed by COSI on 19 December 2016.

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

Operational action plan 2017

Cybercrime-cyber attacks

1. Aim

This Operational Action Plan (OAP) has been created within the framework of the EU Policy Cycle for organised and serious international crime[1]. This OAP corresponds to the following priority:

"To combat cybercrimes committed by OCGs and generating large criminal profits such as on-line and payment card fraud, cybercrimes which cause serious harm to their victims such as online Child Sexual Exploitation, and cyber-attacks which affect critical infrastructure and information systems in the EU".

This OAP contains a breakdown of all the operational actions that will be carried out during the year 2017 as the way to reach the various strategic goals chosen during the "MASP" workshop. It also gives a general overview of the tasks and responsibilities of the Member States and the Agencies involved in the delivery of the plan.

2. Context

Some of the operational actions (OA) of this OAP have potential for overlaps with several other OA in other OAPs.

Any overlaps identified between OAPs will be the subject of careful management attention and coordination as described below (see end of paragraph 5.1).

[1] 15358/10

www.parlament.gv.at

3. Structure

The plan is essentially a coordination overview presenting the general outline of operational activities, rather than the specific detail of each. That detail will be found in the related activity documentation which is referenced within this plan. The activity documentation should include a description of the break down of the activity in “What, When, Where, Who and How” the activity will be carried out.

The Annex to the plan contains a table with all operational activities. The table will facilitate:

- Cross-reference between different, but related, activities within the same priority
- Cross-reference between activities which also contribute to a different priority
- Reference to detailed project documentation for a given activity
- Cumulative progress reporting.

4. Management & Project Support

4.1 Management

Overall management responsibility for this OAP lies with the Drivers and Co-Drivers of each crime priority as identified by COSI. Every individual operational activity of this OAP has a designated leader duly tasked and empowered for this role. Management responsibility for each activity is clearly shown in the list of operational activities. The management approach shall be in line with the EMPACT Terms of Reference[2].

4.2. Project support

In order to allow the Driver to focus on project management (of the common actions), and to reduce the national responsibility for overall EU coordination, Europol shall provide the project support for this OAP in line with the EMPACT Terms of Reference.

[2] 14518/12

www.parlament.gv.at

4.3 Information management

The Europol Analysis Work File for Serious and Organised Crime (AWF SOC) shall be the primary means by which operational data emanating from the activities within this plan shall be processed. The Europol Information System may also be used where appropriate.

It is recommended that all operational information exchange and progress reporting within the OAP shall be done using the SIENA (Secure Information Exchange Network Application) system which provides a quick, secure and auditable means of communication between all competent authorities and Europol.

5. Methodology

5.1 Planning

NOT DECLASSIFIED

When available, the actions should also include administrative measures. Wherever possible, due use will be made of opportunities and processes for a wider inter-agency approach. The MS are invited to integrate actions developed in the plan at the appropriate level into the MS national planning and dedicated resources should be allocated to ensure full support to the common EU approach. Similarly, the Agencies should reflect the actions developed into their yearly work programmes.

www.parlament.gv.at

The OAP was validated by COSI on 19 December 2016 and the tasking responsibilities contained in the plan confirmed. That process has also identified actions contained in this plan which may be related to other plans, and vice versa. These issues will be included into the agenda of the OAP kick-off meeting in early 2017 and will be addressed by the Driver in conjunction with the Action Leaders, participants and Europol, in cooperation with the Drivers of the other OAPs involved.

5.2 Implementation

The activity will be implemented according to the breakdown of actions and timescales contained in the activity plan. The Driver will be the authority to execute or delegate the management/leadership of a specific action to the Action Leader, who then has the responsibility for initiating and reporting on each action to the Driver.

The Action Leaders will report to the Driver and Co-Driver on a quarterly basis, and include information on MS participation. This will allow the Driver and Co-Driver to monitor the progress through 2017, acknowledge the successes and identify the challenges. It is expected that learning from this reporting process will influence the OAP's throughout the policy cycle.

5.3 Monitoring and reporting

The templates include the means for recording results. Monitoring and reporting shall be done in line with the regime established by the Commission and using the template provided for the policy cycle reporting.

This regime for on-going monitoring & periodical reporting[3] should include:

- Progress and results within the individual operational activities, including targets and key performance indicators (KPIs).
- Progress and results within the overall operational action plan, including the measurement of achievement as agreed at the MASPs meetings.
- Cross reporting between different strategic goals/OAP's as appropriate.

[3] Including possible reference to resources allocated and their use.

www.parlament.gv.at

5.4. Good practices

Experiences within the delivery of the OAP which provide examples of good (and bad) practice will be duly recorded. This will be a responsibility of the Driver to report them to the attention of the EMPACT Support Team and of the National EMPACT Coordinators for wider sharing.

www.parlament.gv.at

Crime Priority G3 - Cyber Attacks – OAP 2017 – List of actions

Strategic goal 1: To build a comprehensive intelligence picture in order to jointly prioritise common threats and key targets.

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

<u>Strategic goal 2</u>: To tackle the prioritised threats and targets through joint operational activities, including disruptive actions, joint investigations and coordinated prosecutions.

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

<u>Strategic goal 3</u>: To improve operational and judicial cooperation and coordination with third countries on the prioritised threats and targets.

NOT DECLASSIFIED

www.parlament.gv.at

<u>Strategic goal 4</u>: To maximise collaboration with non-law enforcement actors including CERTs and private sector, stepping up coordination of efforts, exchange of information and building prevention and detection capacities.

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

Strategic goal 5: To contribute to the establishment of a coordinated multidisciplinary mechanism for response in case of a serious cyber-attack with a cross-border dimension with well-defined roles, responsibilities and procedures.

NOT DECLASSIFIED

www.parlament.gv.at

Strategic goal 6: **To build and strengthen cyber capabilities i.e. by developing adequate resources and tools and improving expertise, knowledge and skills available to law enforcement, judiciary and key partners such as academia.**

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

<u>Strategic goal 7</u>: To strengthen cyber security awareness, responsibility, resilience and agility of private users and professionals, in particular operators of critical infrastructure and information systems, in order to minimise threats to victims and damages of cybercrime.

NOT DECLASSIFIED

www.parlament.gv.at

<u>Strategic goal 8</u>: To identify opportunities for updating the legal framework for effective prevention, detection, disruption, investigation and prosecution of cybercrimes and to actively contribute to the debate on the related jurisdictional issues.

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

www.parlament.gv.at

NOT DECLASSIFIED

_____

www.parlament.gv.at