Council of the
European Union

Brussels, 2 July 2019
(OR. en)

13668/2/18
REV 2 EXT 1

JAI 1071
COSI 240
ENFOPOL 526
ENFOCUSTOM 222
COPS 389
RELEX 908
JAIEX 147
CYBER 255

PARTIAL DECLASSIFICATION

of document:	13668/2/18 REV 2
dated:	7 May 2019
new status:	Public
Subject:	Operational Action Plan 2019 related to the EU crime priority: "Attacks against information systems"

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

Council of the European Union

Brussels, 7 May 2019
(OR. en)

13668/2/18
REV 2

RESTREINT UE/EU RESTRICTED

JAI 1071
COSI 240
ENFOPOL 526
CRIMORG 148
ENFOCUSTOM 222
COPS 389
RELEX 908
JAIEX 147
CYBER 255

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	15700/17 + COR 1, 9450/17
Subject:	Operational Action Plan 2019 related to the EU crime priority: "Attacks against information systems"

Delegations will find attached the draft OAP 2019 regarding the EU crime priority: "Attacks against information systems", developed under the overall responsibility of the **NOT DECLASSIFIED** driver, as agreed by COSI Support Group on 16 November 2018.

The OAP 2019 consists of 19 actions, of which 8 are classified as operational.

The Driver and Co-Drivers lead 4 of these actions.

23 Member States participate in this OAP, as well as CH, IS, NO, Interpol, COM, EUROJUST, EUROPOL, CEPOL and GSC. Member States are leading 17 actions **NOT DECLASSIFIED** and the other actions are led by COM (1) and CEPOL (1).

This OAP aims to identify intelligence gaps within the criminal business model with an operational plan to target vulnerabilities.

NOT DECLASSIFIED

ANNEX

Operational Action Plan:

ATTACKS AGAINST INFORMATION SYSTEMS

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:

1) To fight cybercrime, by (1) disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime, by (2) combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, and by (3) targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities.

This OAP contains a breakdown of all the operational actions that will be carried out during the year 2019 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, the EU institutions, agencies and other possible entities 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 7704/17

3. Structure

The plan is essentially a coordination overview presenting the general outline of operational actions, 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 actions.

The table will facilitate:

- Cross-reference between different, but related, operational actions within the same priority
- Cross-reference between operational actions which also contribute to a different priority
- Reference to detailed project documentation for a given operational actions
- Identification of possible JADs.

4. Management & Project Support

4.1. Management

Overall management responsibility for this OAP lies with the Driver and Co-Drivers as identified by COSI and set out in the list of relevant actors regularly issued.

Every individual operational action of this OAP has a designated Action Leader duly tasked and empowered for this role, assisted if required by a Co-Action Leader.

Management responsibility for each operational action is clearly shown in the list of operational actions.

The management approach shall be in line with the EU Policy Cycle Terms of Reference[2].

[2] 10544/2/17 REV 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 EU Policy Cycle Terms of Reference.

4.3. Information management

The Europol Analysis Projects shall be the primary means by which operational data emanating from the operational actions within this plan shall be processed. Other Europol 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 SIENA (Secure Information Exchange Network Application), which provides a quick, secure and auditable means of communication between all competent authorities and Europol.

5. Methodology

5.1. Planning

This OAP has been developed by experts from **NOT DECLASSIFIED** are registered as Relevant Actors for this OAP, however were not in attendance. **NOT DECLASSIFIED** also attended the drafting meeting.

The scope of operational actions included in the plan corresponds to the conclusions and recommendations emanating from the specific assessment of the problem which is central to the priority crime area.

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 the relevant actions developed in the plan at the appropriate level into their national planning and to allocate resources to support a common EU approach. Similarly, the agencies should commit the actions developed into their annual work programmes pursuant to the Council conclusions on the continuation of the of the EU Policy Cycle for organised and serious international crime for the period 2018-2021 and the EU Policy Cycle Terms of Reference.

The OAP was agreed by COSI Support Group and the tasking responsibilities contained in the plan were 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 2019 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 OAP will be implemented according to the breakdown of operational actions and timescales contained in the OAP. The Driver, assisted by the Co-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.

5.3. Monitoring and reporting

Monitoring and reporting shall be done in line with and using the template set out in the reporting collection mechanism. This mechanism will be established following Action 15 of the Council conclusions on the continuation of the EU Policy Cycle for organised and serious international crime for the period 2018-2021[3].

[3] 7704/17

This regime for on-going monitoring and periodical reporting[4] should include:

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

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.

[4] Including possible reference to resources allocated and their use

Operational Action Plan (OAP)

ATTACKS AGAINST INFORMATION SYSTEMS

EU Crime Priority: Attacks against information system OAP 2019

List of actions

Strategic Goal 1: Intelligence Picture

Objective: Develop and update the intelligence picture on criminal activities related to attacks against information systems in the EU, through the detection of intelligence gaps, the monitoring of trends and new developments, the identification of links to other crime areas, and to integrate it in the strategic and operational planning of the relevant stakeholders.

NOT DECLASSIFIED

NOT DECLASSIFIED

Strategic Goal 2: Operational activities

Objective: Prepare and coordinate operations, investigations and prosecutions to detect, disrupt and deter organised crime groups and suspects active in criminal activities related to attacks against information systems in the EU.

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

Strategic Goal 3: Prevention and Capacity building

Objective: Increase prevention against threats relating to attacks against information systems in the EU, including through awareness-raising amongst relevant public and private actors, and build the law enforcement capacity to tackle criminal activities related to attacks against information systems in the EU by improving knowledge, skills and expertise of relevant public and private actors based on cooperation, training and the sharing of best practices.

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

Strategic Goal 6: Financial Investigations

Objective: Combat criminal finances, money laundering, and facilitate asset recovery and confiscation as part of investigations of criminal activities related to attacks against information systems in the EU.

NOT DECLASSIFIED

NOT DECLASSIFIED