Council of the European Union

Brussels, 16 December 2022
(OR. en)

13747/1/22
REV 1

LIMITE

JAI 1340
COSI 253
ENFOPOL 513
CRIMORG 132
ENFOCUSTOM 143
COPS 468
RELEX 1370
JAIEX 88
CYBER 331

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	13590/2/21 REV 2
Subject:	Operational Action Plan 2023: Cyber attacks

EMPACT
Fighting crime together

Delegations will find attached the Operational Action Plan 2023 on Cyber-attacks developed under the responsibility of the DE driver. The draft OAP was shared with National EMPACT Coordinators (NEC) and brought to the NEC meeting for discussion on 25-26 October 2022 and COSI Support Group (COSI SG) on 14 November 2022.

In line with the agreed OAPs template set out in 10595/22, the participation in operational actions is set out in document 14407/1/22 REV 1.

Pursuant to the COSI SG meeting, delegations submitted some further changes to be introduced into the Operational Action Plan.[1]

[1] Changes compared to the previous version are marked in ~~strikethrough~~ or **bold and underlined**. See page 9.

Cyber-attacks Operational Action Plan

1. Aim

This Operational Action Plan (OAP) has been created within the EMPACT framework and corresponds to the following priority:

Cyber-attacks

The aim of this priority is "to target the criminal offenders orchestrating cyber-attacks, particularly those offering specialised criminal services online."

This OAP outlines a list of all the operational actions that will be carried out during the year 2023 as means to implement the following strategic goals:

- CHSG 1 - Criminal intelligence picture
- CHSG 2 - Investigations and judicial response, with a specific focus on high-risk criminal networks (HRCN) and key individuals
- CHSG 4 - Criminal finances, money laundering and asset recovery
- CHSG 6 - Capacity building through training, networking and innovation
- CHSG 7 - Prevention and harm reduction, assistance to victims, awareness raising
- CHSG 8 - External dimension: cooperation with non-EU partners

2. Context

2.1. EU Intelligence contributions

Definition of criminal activity/crime area:

Cyber-dependent crime is any criminal activity that can only be committed using computers, computer networks or other forms of information communication technology (ICT). Such crimes are typically directed at computers, networks or other ICT resources. It includes the creation and spread of malware, hacking to steal sensitive personal or industry data including trade secrets and proprietary knowledge, denial of service attacks to cause financial and/or reputational damage and other criminal activities.

Key threats:

- The availability of cybercrime services online as part of a crime-as-a-service business model makes cybercrime more accessible by lowering the technological expertise required to carry out these crimes.
- While cyber threats continuously evolve, 'traditional enablers' remain a constant factor: criminal infrastructure (e.g. botnets) are used to spread malware through 'traditional' methods (e.g. phishing). Data breaches continue to result in personal information being made available to criminal organisations that in turn use it to commit cybercrime and fraud.[2]
- Businesses are increasingly the targets of cyberattacks. Public institutions, including critical infrastructure such as health services, continue to be targeted by cybercriminals.
- Malware constantly evolves and is highly diverse existing in hundreds of thousands of variants. Mobile devices continue to be the targets of mobile cyberattacks relying on mobile malware.

[2] Europol 2020, Internet Organised Crime Threat Assessment (IOCTA) 2020, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

- Ransomware has been acknowledged as a key cybercrime threat for some years now. Their sophistication continues to increase and number of attacks on public institutions and large companies is particularly notable.
- DDoS attacks are a well-known and persistent threat, affecting not only smaller organisations with lower security standards as well as public institutions and critical infrastructure.
- Cybercriminals are highly adaptable and quickly integrate technological developments and new security measures into their modi operandi.
- Cyber industrial and economic espionage (theft of trade secrets) cost EUR 60 billion to the EU economy.[3]

Key developments:

- The threat from cyber-dependent crime has been increasing over the last years not only in terms of the number of attacks reported but also in terms of the sophistication of attacks.
- The impact of cyber-attacks is extremely high. Cyber-dependent crime causes significant financial loss to businesses, private citizens and the public sector each year through payments for ransomware, incident recovery costs and costs for enhanced cyber-security measures. Regular citizens are affected by publication of their personal data and disruptions caused by attacks to critical infrastructure.
- Businesses are increasingly the targets of cyberattacks due to a higher profitability. Data commodification, extortion and ransom are some of the means to obtain profits from cyber-attacks. Businesses are more prone to pay as they might be covered by insurances or in order to avoid regulatory sanctions and reputational damages.

[3] European Commission 2019, The scale and impact of industrial espionage and theft of trade secrets through cyber, accessible at https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en

- Innovative SMEs in particular display lower levels of resiliency to the threat of industrial espionage due to cybersecurity and IP management awareness and preparedness.[4]
- The use of cryptocurrencies and proliferation of anonymisation techniques, including encryption, continues to grow.
- Bullet proof hosting of criminal activities remains a major concern in the EU and beyond.[5]
- Developments in the modus operandi related to ransomware, where the information is not only encrypted, but also leaked online, pose new threats to victims and new challenges to law enforcement.
- The number of ransomware attacks and the level of their sophistication continues to increase, particularly in the area of public institutions and large companies.
- Cybercriminals orchestrating DDoS attacks increasingly target smaller organisations with lower security standards.
- During 2020, the COVID-19 pandemic has led to a surge in connections from private to corporate systems as telework became the norm in many sectors and industries, making many corporate networks more vulnerable to cyberattacks.
- Developments such as the expansion of Internet of Things (IoT), the increased use of artificial intelligence (AI), more applications for biometrics data or the availability of autonomous vehicles create criminal opportunities.

[4] Europol 2020, Internet Organised Crime Threat Assessment (IOCTA) 2020, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[5] Europol 2020, Internet Organised Crime Threat Assessment (IOCTA) 2020, accessible at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Intelligence gaps:

- Cyber-dependent crime is likely significantly underreported.
- Knowledge on criminal actors, criminal networks and their geographical location is limited.

Key locations:

- Non-EU eastern European countries
- East Asia

Enabling factors/enablers:

- Online service providers
- Cryptocurrencies, especially the ones with more privacy focus
- Existing payment infrastructures
- The use of network infrastructures (bulletproof hosting and/or VPN services)

Most relevant (non-EU) partners/countries of interest:

- Online service providers
- Cybersecurity practitioners (e.g. CSIRTs)
- Financial sector (Banks, exchanges and online payment infrastructure operators)
- Private sector (Internet security companies and network operators)
- Public sector (public institutions and critical infrastructure operators)
- Belarus, Brazil, China, Georgia*, Israel^, Japan^, Moldova*, Russia, South Korea, Ukraine*, United States*

* Operational Agreement with Europol

 Strategic Agreement with Europol

^ Working arrangement

Key areas to target:

- Focus on criminal networks and lone offenders involved in cybercrime activities.
- Focus on cybercrime enablers and criminal infrastructure.
- Develop countermeasures to prevent, identify or hinder money-laundering activities by means of cryptocurrencies.
- Improve the awareness of industry actors.

Additional elements to the intelligence picture from Driver & OAP participants: none.

2.2. Potential overlaps or synergies with other OAPs

The priority crime area which this OAP addresses, could potentially overlap or have synergies with the following other OAPs:

- OAP Online Fraud Schemes OA 2.3 (phishing attacks) and OA 4.1 (virtual currency exchangers and mixing platforms and any other related financial instruments)
- OAP Criminal Finances, Money Laundering and Assets Recovery: –OA 2.3 (phishing attacks) and OA 4.1 (virtual currency exchangers and mixing platforms and any other related financial instruments)

This potential overlap/synergy with other OAPs will be subject to the Driver's attention. The coordination with other OAPs will be facilitated by the EMPACT Support Team.

3. Structure

The OAP is essentially a coordination overview presenting the general outline of OAs, rather than the specific detail of each OA and does not include sensitive nor classified information. These details will be found in the related OA planned implementation document based on the Planning and reporting template[6].

An overview of the OAs within this OAP, that should be updated whenever relevant, can be seen below.

Overview of OAs

No	OA	AL	Short title
1	1.1	NL	Development of tools for the intelligence process to identify High Value Targets (HVT), current and emerging major cyber threat
2	1.2	~~DE~~ **EUNAT**	Continuing development of tactical concepts in connection with Cyber-Extortion cases Payment of ransom and tactical concepts
3	2.1	RO	Disruption of organised crime groups and suspects engaged in criminal activities related to attacks against information systems in the EU
4	2.2	EL	Focusing on the phishing attacks to report, disrupt and take operational action
5	2.3	DE	Disruption activities against high value cybercrime group(s) involved in the criminal facilitation of cybercrime, in particular by means of offering forums and other means of criminal communication channels
6	2.4	FR	Targeting a bulletproof VPN service to access and exploit data in order to identify HVT
7	4.1	FR	Tackling money-laundering services using virtual currencies and key financial facilitators

[6] 5002/1/20 REV 1 section II. Planned implementation

No	OA	AL	Short title
8	4.2	EUROPOL	Bitcoin clusterization
9	6.1	CEPOL	Implementation of multidisciplinary training activities related to cyberattacks
10	6.2	DE	Organization of an International Cybercrime Conference
11	7.1	NL	Prevention and deterrence from engaging in a career as a cybercriminal
12	7.2	FR	Ransomware Integrated Investigation Process (R2IP)
13	8.1	CEPOL	Carry out and implement multidisciplinary training activities related to cyber-attacks in order to build capacities for law enforcement, judicial authorities and other relevant bodies
14	8.2	Albania	strengthening cooperation and real-time information exchange between LEAs and CERTs

Action leaders – relevant actors: DE, EL, FR, NL, CEPOL, EUROPOL

Action leaders – partners: Albania

4. Management, Coordination & Support

4.1. OAP Management

Overall management responsibility for this OAP lies with the Driver, supported by the Co-Driver(s) of the OAP as identified by COSI and set out in the list of relevant actors.

Each OA 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 outlined in the list of operational actions.

The management of the OAP shall be in line with the EMPACT Terms of Reference[7].

4.2. OAP support

In order to allow the Driver to focus on OAP management, Europol shall provide the support to the OAP in line with the EMPACT Terms of Reference.

Furthermore, the Coordinator(s) of CHSGs, in line with the tasks and responsibilities set out in the EMPACT Terms of Reference, will support the various Drivers/Co-Drivers with all issues related to the successful implementation of CHSGs, together with the Action Leaders and the OAP group.

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 tools may also be used where appropriate.

It is recommended that all operational information exchange within the OAP shall be done using the Secure Information Exchange Network Application (SIENA), which provides a quick, secure and auditable means of communication between all competent authorities and Europol. Proper access to SIENA should be ensured as necessary for the implementation of OAs.

[7] 8436/1/21 REV 1 (will be updated following the final version of ToR)

5. Methodology

5.1. OAP drafting process

The OAP drafting process has recently been modified to adapt to changing circumstances and a continuous increase in the number of participants. The details on the OAP drafting process for EMPACT 2022+, including the engagement of the Partners in the drafting and implementation, the release of the OAP to the Partners as well as the specific steps of the OAP development can be found in the EMPACT Terms of Reference[8].

The scope of the OAs included in the OAP corresponds to the EU SOCTA 2021 and additional intelligence contribution gathered by the OAP groups.

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 OAP will be validated by COSI SG/COSI.

5.2. Implementation

The OAP will be implemented via the set of OAs and timescales contained in the OAP. The Driver, assisted by the Co-Drivers, will be the authority to execute or delegate the management/leadership of a specific OA to the Action Leader, who then has the responsibility for initiating and reporting on each action to the Driver.

Member States are invited to integrate the relevant OAs developed in the OAP at the appropriate level into their national planning and to allocate resources to support a common EU approach. Similarly, the agencies and relevant EU networks, should commit the actions developed into their annual work programmes pursuant to the Council conclusions on the permanent continuation of the EU Policy Cycle for organised and serious international crime: EMPACT 2022+ and the EMPACT Terms of Reference.

5.3. Monitoring and reporting

The reporting is composed of three steps: 1. Light reporting on the progress of the OAP, 2. Comprehensive reporting on the results of the OAP and 3. Annual fact sheets on the results of OAP.

[8] 8436/1/21 REV 1 (will be updated following the final version of ToR)

Monitoring and reporting shall be done in line with and using the template set out in the reporting mechanism[9].

[9] 5002/1/20 REV 1 - Reporting mechanism

Operational Action Plan 2023

Cyber- Attacks

EU crime priority/OAP: Cyber-attacks - OAP 2023

List of actions

Strategic Goal 1: Criminal intelligence picture

Objective: develop or keep updated, through the detection of intelligence gaps, the monitoring of threats (including from high-risk criminal networks – HRCN), trends and new developments (e.g. the use of new technologies), and the identification of links to other crime areas, the strategic and operational intelligence picture relating to each EU crime priority, and to integrate it in the strategic and operational planning of the relevant stakeholders.

Ref.: OA 1.1	**Leader: NL (Police Forces)**

Activity summary of the Operational Action:

Development of tools for the intelligence process to identify High Value Targets (HVT), current and emerging major cyber threat, in order to continuously enhance the intelligence picture of threats.
The identified targets can be further handled in one or more of the OAs under SG 2, SG 6 or SG 7.

Key Performance Indicators (KPIs) and targets

a) Number of co-developed tools for processing and analysis. Target: 5-10.
b) Number of countries implementing/using tool-box and potential HVT identified. HVT identified target: 5-10.
c) 2 workshops to present the outcome activity.

Type of Operational Action

2-Data collection/data exchange, 3-Strategic

Activities under the Operational Action and timing

Activity	Timing
1) International co-development of tools for the data intelligence process in which data is processed and analysed in a standardised structural manner.	Q1-Q3
2) The output of this data intelligence process should provide a substantial insight in the prioritised threats and potential HVT.	Q4
3) Workshops to present the tool, funding mechanisms and the outcome of the activity	Q1; Q4

Links to other Operational Action Plans (OAP)

Horizontal activities / Joint Action Days (JAD)

Ref.: OA 1.2	**Leader: European Network of Advisory Teams –EuNAT- (Other non- law enforcement)**

Activity summary of the Operational Action *(Short description– 10 lines maximum)*:

As current situations show, the discussion of a possibly necessary fulfilment of perpetrator demands will arise more and more frequently in cyber extortion cases. A follow-up assignment to examine and develop new tactics, methods and possibilities for identifying perpetrators in the cyber space is therefore necessary.

State prohibitions on paying ransom sometimes come to nothing and companies work around the police instead of together. Often, the ransom is paid despite the prohibition because the focus is on economic interest. Therefore, approaches should be optimized and police tactics established that can lead to investigative success.

During the EU project EuNAT (European Network of Advisory Teams), guidelines regarding cyber extortion have been successfully created. In order to combat cybercrime on an international level, the continuation of a project for the further development of police tactical concepts concerning the possibilities of action with ransom would therefore be of great importance.

Key Performance Indicators (KPIs) and target values

a) Number of exchanges of best practices and tactical approaches to solve cyber extortion cases (Target 6)
b) Number of Recommendations on the topic of continuing development of tactical concepts in connection with cyber-extortion cases, especially under the aspect of international cooperation (Target 7)
c) Workshop to present the outcome activity (Target 1)

Type of Operational Action (*indicate the main ones - maximum 2)*

Strategic, Knowledge/training

Activities under the Operational Action and timing *(Short description– 5 lines maximum per activity)*

Activity	Timing
1) Evaluation of relevant operational cases and best practises	Q1-Q4
2) Workshops on the topic continuing development of tactical concepts in connection with Cyber Extortion cases	Q1-Q4
3) Summary of the results and recommendations	Q1-Q4
4) Workshop to present the outcome activity	Q1-Q4
5) International trainings	Q1-Q4

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)

Strategic Goal 2: Investigations and judicial response, with a specific focus on high-risk criminal networks (HRCN) and key individuals.

Objective: prepare and conduct investigations, coordinated actions, and prosecutions, in each EU crime priority, to detect, identify and disrupt criminal networks active in the EU, and individuals with key roles in these networks, with a special emphasis on high-risk criminal networks (HRCN) undermining the rule of law by using corruption and intimidating power in order to infiltrate a Country's legal economy and administrative management system, those who commit acts of violence and use firearms to further their criminal goals and take advantage of vulnerable groups, as well as those who launder their criminal proceeds through a parallel underground financial system.

Ref.: OA 2.1	**Leader: RO (Police Forces)**

Activity summary of the Operational Action:

To pursue enforcement and disruption activities against high value cybercrime group(s) e.g. to include (but not confined to) CaaS involved in the deployment of malware (e.g. ransomware, mobile malware and other forms of malware), operating botnets, data breaches, malicious hacking collectives, cash-out services related to malware usage,DDOs attacks, CAV services, encrypted services that are facilitating cybercriminal communication) and cryptors.

Key Performance Indicators (KPIs) and targets

a) Number of investigations/ operations and prosecutions. Target 5
b) Number of HVTs disrupted. Target 3
c) Number of distributed reports (e.g. operational analysis reports, cross-matches, intelligence notifications). Target 20
d) Number of operational meetings and technical sprints. Target 5
e) Number of workshops organised. Target 1

Type of Operational Action

1-Operational

Activities under the Operational Action and timing

Activity	Timing
1) Intelligence gathering	Q1–Q2
2) Investigation, takedown, remediation and depending on possibilities the prosecution of criminals and criminal facilitators	Q1–Q4
3) Technical mitigation in collaboration with private partners	Q1–Q4
4) Exchange best practices and expertise on investigative measures and dedicated tooling	Q1–Q4
5) Organising a workshop dedicated to malware analysis	Q2–Q3

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)

Ref.: OA 2.2	Leader: EL (Police Forces)

Activity summary of the Operational Action:

Infrastructures/phishing as a service:

Cybercriminals heavily rely on phishing attacks to steal users' data. The fake websites used for phishing purposes are, in several cases, hosted in infrastructure of legitimate providers, and they are taken down, shortly after the provider is notified for the illegal content (either by the victims or by the LEAs). This action is crucial, as it protects any other potential victims. The goal of the OA is to develop a pilot mechanism for: (a) fast reporting of the phishing websites from LEAs to the hosting providers (report & takedown – without disrupting any ongoing investigations), and (b) identify targets and coordinate actions against administrators of phishing websites. Additionally, awareness raising campaign on phishing attacks will take place within MS.

Key Performance Indicators (KPIs) and targets
a) Number of phishing websites identified. (300)
b) Number of phishing websites taken down. (100)
c) Number of criminal actors administering phishing websites identified and related investigations (10)
d) Number of prevention activities/campaigns. (1 on every participant MS)

Type of Operational Action

1-Operational, 5-Prevention

Activities under the Operational Action and timing

Activity	Timing
1) Development of a pilot mechanism/procedure for fast reporting of phishing websites from LEAs to hosting providers.	Q1-Q2
2) Identification of targets and coordination of (joint) actions against administrators of phishing websites.	Q2-Q4
3) Awareness campaigns in MS to inform the public about phishing.	Q2-Q4

Links to other Operational Action Plans (OAP)/priority

OFS; CFMLAR

Horizontal activities / Joint Action Days (JAD)

JAD or EAD

Ref.: OA 2.3	Leader: DE (Police Forces)

Activity summary of the Operational Action:

To pursue enforcement and disruption activities against high value cybercrime group(s) involved in the criminal facilitation of cybercrime, in particular by means of offering forums and other means of criminal communication channels.

Key Performance Indicators (KPIs) and targets

a) Number of criminal contributed platforms. (35).
b) Number of cross-match reports. (30).
c) Operational workshop to improve data collection, cooperation and knowledge. (1)

Type of Operational Action

1-Operational, 2-Data collection/data exchange

Activities under the Operational Action and timing *per activity)*

Activity	Timing
1) Investigation and, depending on possibilities, takedown, remediation, prosecution of criminals and criminal facilitators operating via Internet-based communication technologies. To include identification, prosecution and disruption activities against high value cyber criminals, groups and/or the infrastructure.	Q1–Q4
1) Improvement of the knowledge base of the relevant cybercriminal-groups, their criminal activities and the means of communication used.	Q1–Q4
2) Discovering proactive and investigative methods for proxy/backend detection and data seizure.	Q1–Q4
3) Explore possibilities for policy and regulatory action.	Q1–Q4
4) Improving technical knowledge, equipment and IT-infrastructure of Member States (Hardware, Software) in order to process, store and analyse data gained from operational outcome. This may include external outsourcing.	Q1–Q4
5) Operational workshop to improve data collection, cooperation and knowledge.	Q1-Q4

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)

Ref.: OA 2.4	Leader: FR (Police Forces)

Activity summary of the Operational Action *(Short description– 10 lines maximum)***:**

One of the top priority of criminals online is to obfuscate any information that could allow Law Enforcement Agencies to identify them. Using a VPN to hide their IP address is the first step they take.

However, they tend to avoid “commercial” VPN services that may comply with legal request and tend to use “bullet proof” services that rely on their refusal to comply with legal requests as well as deleting all personal information to attract business. These services are often advertised on online criminal forums or other communication means dedicated to criminal activities.

Investigation lead on bulletproof services lead in the past to relevant information on ransomwares, botnets and helped prevent further attacks.

The goal of this OA would be to identify a bulletproof VPN service and set up technical investigation tools to gather information that would be shared with the relevant partners as well as live data collection.

Key Performance Indicators (KPIs) and targets

a) Targeting a bulletproof VPN service used by criminals. 1
b) Setting up NetFlow interception and analysing data connected to criminal activities
c) Creating packages for active ongoing investigations: 5-10.
d) Organising sprint meetings to share and work on intelligence and data 7

Type of Operational Action (*indicate the main one - maximum 2)*

(1-Operational, 2-Data collection/data exchange, 3-Strategic,)

Activities under the Operational Action and timing *(Short description– 5 lines maximum per activity)*

Activity	Timing
1) Targeting a criminal VPN service and meeting with prosecutors and countries on extracting data who will be stored in specialized equipment such as servers	Q1-Q2
2) Identifying HVT, creating and sharing intelligence packages	Q2-Q3
3) Gather actionable intelligence to allow the relevant Member States and third parties to take further actions	Q4

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)

Strategic Goal 3: Coordinated controls and operations targeting the online and offline trade in illicit goods & services

Objective: target – notably through coordinated controls and operations – criminal networks, individual criminal entrepreneurs, high impacts vendors and facilitators, their business models and other actors involved in the online and offline trade in illicit goods and services, with a special attention to those active in the markets that are related to an EU crime priority.

Targeting the Organised Criminal Groups, other actors and the infrastructures used to prepare and launch cyber-attacks related products and services are key objectives in this OAP.

A number of operational actions proposed in this OAP, such as OA 2.1 (RO) and OA 4.1 (FR), have directly links and activities that target the disruption of criminal services and aim to achieve some of the objectives of this Common Horizontal Strategic Goal-CHSG.

Strategic Goal 4: Objective: Combat the criminal use of financial structures including money laundering, facilitate asset recovery an confiscate proceeds of crime, disrupt criminal infiltration by involving specialised financial investigators, where relevant, as part of investigations in the EU crime priorities, and develop a culture of asset recovery through training and financial intelligence sharing.

Ref.: **OA 4.1**	**Leader: France (Police Forces)**

Activity summary of the Operational Action *(Short description– 10 lines maximum)***:**

Bitcoin and other specific cryptocurrencies are the default payment methods when it comes to online trade in illicit goods and services and in the cybercrime underworld. They should therefore handle as an asset, in the same way that fiat currency, cash or gold. Mixer and tumbler services as well as privacy coins impede criminal finance analysis using forensics block chain analysis or other relevant sources and tools. Alongside other measures, identifying and tackling those obfuscating financial services can be one of the most effective way to identify suspected criminals. The goal of this OA is to directly disrupt services that facilitate criminal finance through effective joint operations and discourage potential new offenders from providing criminal financial services via the publicity thereof; Improve baseline intelligence on criminal infrastructure including criminally complicit virtual currency exchanges mixers and related financial instruments.

Key Performance Indicators (KPIs) and target values

a) Number of criminal facilitators or services: identified (5)/ disrupted (1)
b) Number of money laundering-financial investigations carried out (3).
c) Value of assets seized/frozen/confiscated in crypto (20.000 Euros)
d) Tactical sprint against ransomware financial facilitators (1)
e) International workshop on money laundering proceeding from cybercrime using virtual currencies (1)

Type of Operational Action (*indicate the main ones - maximum 2)*

(1-Operational, 2-Data collection/data exchange, 3-Strategic, 4-Knowledge/training,

Activities under the Operational Action and timing *(Short description– 5 lines maximum per activity)*

Activity	Timing
1) Identification and/or update of the criminal financial services and deconfliction	Q1-Q2
2) Prioritization of the High Value target per category	Q2-Q3
3) Joint investigation and crypto sprint targeting prioritized HVT	Q2-Q4
3) Sharing of best practices and improvement of tools, methods and technics used by LE crypto specialists. Incorporate money laundering investigations and asset recovery techniques within operational activities.	Q3-Q4
4) Disruption of the targeted services and intelligence gathering	Q2-Q4
5) Sharing of financial intelligence with the affected countries and reporting	Q3-Q4

Links to other Operational Action Plans (OAP)/priority

OAP Financial crime, money laundering and assets recovery

Horizontal activities / Joint Action Days (JAD)

Ref.: OA 4.2	Leader: EUROPOL

Activity summary of the Operational Action *(Short description– 10 lines maximum)*:

Bitcoin and other specific cryptocurrencies are the default payment methods when it comes to online trade in illicit goods and services and the cybercrime underworld. Alongside other measures, high quality cryptocurrency analysis can be one of the most effective tools to identify suspected criminals in this field.

Clusterisation of addresses is a key element to successful virtual currency analysis. Commercial tools endeavour to present identified clusters but often there is an incomplete picture. LEA need to address this to raise the quality of their cryptocurrency analysis and, as such, their ability to identify suspected criminals operating in the criminal underworld.

The solution is to deliver a real-time coordinated approach to acquiring and sharing attributable information concerning unidentified or underdeveloped clusters. The primary aim of this operational action would be to deliver a collective Member State and selected Third Party effort to proactively withdraw and deposit from selected target services. These addresses will be compiled to a central database to maximise the benefit for law enforcement. The specific mechanism for the database element will be determined during the course of the project.

Key Performance Indicators (KPIs) and target values

a) Number of high value clusters identified. Target 10.

Type of Operational Action (*indicate the main ones - maximum 2)*

(1-Operational, 2-Data collection/data exchange, 3-Strategic, 4-Knowledge/training, 5-Prevention)

Activities under the Operational Action and timing *(Short description– 5 lines maximum per activity)*

Activity	Timing
1) Co-ordination of data collectors	Q1-Q3
2) Establishing and maintaining a central document with all the contributions.	Q2-Q4
3) Data collection/ validation/ de-confliction/ exchange.	Q3-Q4
4) VC Workshop for Clustering improvement and Big data analysis with 27 MS.	Q3–Q4

Links to other Operational Action Plans (OAP)/priority

OAP Financial crime, money laundering and assets recovery

Horizontal activities / Joint Action Days (JAD)

Strategic Goal 5:

Objective: target criminal networks or criminal individual entrepreneurs active in the production and provision of fraudulent and false documents or identification marks by involving specialised investigators, where relevant, as part of investigations in the EU crime priorities.

The use of fraudulent and false documents does not appear as a key aspect for the facilitation of cyber-attacks related crimes. Therefore, the relevant actors in this OAP have opted for not to include this CHSG, as in the previous EMPACT cycle.

Strategic Goal 6: Capacity building through training, networking and innovation

Objective: build the law enforcement and judicial authorities' capacities and capabilities to tackle serious and organised crime by improving knowledge, skills and expertise based on training, networking, the sharing of good practices, and the development of innovative approaches.

Ref.: **OA 6.1**	**Leader: CEPOL**

Activity summary of the Operational Action:
Carry out and implement multidisciplinary training activities related to cyberattacks.

Key Performance Indicators (KPIs) and targets

a) Number of training events organised. Target: 14 onsite training activities, 3 online training activities.
b) Number of trained/exchanged officers. Target: minimum 26 participants per onsite training; 5 exchanges.
c) Level of satisfaction with training activities. Target: Satisfaction rate: >80%.

Type of Operational Action
4-Knowledge/training

Activities under the Operational Action and timing

Activity	Timing
1) 2 onsite courses "Open Source Intelligence (OSINT) and IT Solutions"	Q1-Q4
2) 1 onsite course "Darkweb and Cryptocurrency - basic"	Q2-Q4
3) 1 onsite course "Darkweb and Cryptocurrency - advanced"	Q2-Q4
4) 1 onsite course "Conducting Forensic Searches in Various IT Devices"	Q2-Q4
5) 1 onsite course "Cybercrime - Advanced Windows File System Forensics"	Q2-Q4
6) 1 onsite course "cross-border exchange of e-evidence	Q2-Q4
7) 1 onsite course "Digital Forensic Investigator Training"	Q2-Q4
8) 1 onsite course "First Responders and Cyber-forensics"	Q2-Q4
9) 1 onsite course "cyber intelligence"	Q2-Q4
10) 1 onsite course "Malware Investigation"	Q2-Q4
11) 1 onsite "Live Data Forensics"	Q2-Q4
12) 1 onsite course "Mac Forensics"	Q2-Q4
13) 1 onsite course "Linux Forensics"	Q2-Q4
14) 1 online course "Open Source Intelligence (OSINT) and IT Solutions"	Q1-Q3
15) 3 webinars related to cyber attacks	Q1-Q4
16) Participation in the CEPOL Exchange Program with a focus on cyber-attacks	Q1-Q4

Links to other Operational Action Plans (OAP) / priority
Horizontal activities / Joint Action Days (JAD)

Ref.: OA 6.3	Leader: DE (Police Forces)

Activity summary of the Operational Action

To improve the international cooperation and to close ranks in the field of cybercrime, the German Federal Police Office (BKA) is increasing its efforts to share knowledge, built capacities, raise awareness by bringing together public and private partners in their efforts to fight against cybercrime. Therefore, an international conference will be the frame to invite experts from several disciplines, to inform about developments, to provide a general overview, to share good practises and to build up an interdisciplinary network. The BKA plans to organise the conference every year.

Previously, the German Federal Police Office (BKA) organised three cybercrime conferences (C^3), which gained positive feedback and should therefore be brought on a higher level. The conference should contain a general overview and recent developments related to cybercrime. In addition, the conference shall provide operational information on case studies, tool developments, new technical, forensic and tactical elements of law enforcement to counter cybercrime.

Key Performance Indicators (KPIs) and targets

a) Execution of an international Cybercrime conference (C^3) in May (1)
b) Participation of public and private partners (300 participants)

Type of Operational Action

4-Knowledge/training

Activities under the Operational Action and timing

Activity	Timing
1) Preparatory work for hosting the C^3	Q1, Q2
2) Execution of the C^3	Q2
3) Evaluation of the C^3	Q3

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)

Strategic Goal 7:

Objective: carry out ethically acceptable and evidence-based activities aimed at raising awareness and reducing the risk of crime occurring and its harmful consequences with the ultimate goal of working towards the improvement of the quality of life and safety of individuals, groups and communities.

Ref.: OA 7.1	**Leader: NL (Police Forces)**

Activity summary of the Operational Action:

Utilise the EU prevent network to carry out actions that will dissuade people from a criminal career path. Support MS with the generation of products that contribute to awareness campaigns.

Key Performance Indicators (KPIs) and Targets

a) Number of tactical Prevent operations and Prevent awareness/education /communication campaigns. Target: 5.
b) Successful establishment of cyber Prevent SPOC network (1)
c) Support and deliver new Prevent approaches across the EU. Target: 5.
d) Number of prevent interventions delivered and numbers diverted. Target: 3.

Type of Operational Action

1-Operational, 3-Strategic, 4-Knowledge/training, 5-Prevention

Activities under the Operational Action and timing

Activity	Timing
1) Promote best practice and concurrently understand MS capability to deliver Prevent activity. Formalise the Prevent network in order to develop and distribute best practice, guidance and training.	Q1
2) To run awareness campaigns to inform the public about the implications and consequences of hacking and malware deployment to dissuade people from becoming or progressing as a cybercriminal. Utilisation of tactical prevent messaging on forums in order to influence messaging.	Q3
3) Continuation of the development of positive alternatives that can be deployed alongside Prevent interventions enabling people to actively engage and use their skills for the greater good of a safe online environment	Q1-Q4
4) Support operational activity - by co-ordination of Prevent outcomes. Utilise de-briefing and future supported operations to evaluate effectiveness of Prevent delivery.	Q1-Q4

Links to other Operational Action Plans (OAP)

Horizontal activities / Joint Action Days (JAD)

Ref.: OA 7.2	Leader: FR (Police Forces)

Activity summary of the Operational Action *(Short description– 10 lines maximum)***:** All EU MS are facing ransomware threats and attacks. All Police forces will have to respond and not only high specialized Units. They need a Ransomware Integrated Investigation Process (R2IP) that would aim to set up pragmatic guidelines to respond to the threat as underlined:

1. Following up the previous questionnaire et re engaging non-responders' participants. And Analysing the State of the Play

2. THE HIVE incident response software has been chosen. Beta testing in French National Law Enforcement with engagement of 2 or 3 participant countries.

3: Initial incident form already set up. Engage private sector and partners countries

3. Enhance sharing capacities through standardized proceedings via Siena messages. Regarding the R2IP investigation process set up in France and vetted by Justice Department

4. Gathering Intelligence on negotiation scenarios to build on common guidelines for investigator and countermeasures to deploy during this phase.

Key Performance Indicators (KPIs) and target values

a) Statistics on surveys initially sent to MS Law Enforcement on R2IP existing framework Target: at least 12 questionnaires
b) Statistics on information sharing R2IP reports to Europol. Target: 50
c) Number of local field using R2IP integrated tools, solution, documents, reports, forms, guidelines (etc...) proposed in R2IP package. Target: (5)
d) Engagement of private companies to use the R2IP. Target: (5)

Type of Operational Action (*indicate the main ones - maximum 2)*

(1-Operational, 2-Data collection/data exchange, 3-Strategic, 4-Knowledge/training, 5-Prevention)

Activities under the Operational Action and timing *(Short description– 5 lines maximum per activity)*

Activity	Timing
1) Presentation of R2IP proceedings to country partners (4)	Q1-Q4
2) Presentation of THE HIVE digitalized environment (4)	Q1-Q4
3) Dedicated R2IP Siena message to set up with EUROPOL (3)	Q1-Q4
4) Private sector to engage with R2IP initial incident report (3)	Q1-Q4

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)

Strategic Goal 8:

Objective: expand the external dimension of EMPACT and the cooperation both with third countries and at global level to address common challenges. Enhance cooperation with relevant non-EU partners such as international organisations, regional fora, non-EU source, transit and destination countries, priority countries such as enlargement and neighbouring countries, and key crime markets for each EU crime priority.

Ref.: **OA 8.1**	**Leader: CEPOL**

Activity summary of the Operational Action *(Short description– 10 lines maximum)*:
Carry out and implement multidisciplinary training activities related to cyber-attacks in order to build capacities for law enforcement, judicial authorities and other relevant bodies.
According to the description of actions only for the projects beneficiary countries:
Eastern Partnership (EaP) countries: AM, AZ, GE, MD, UA
MENA beneficiaries: ALGERIA, EGYPT, ISRAEL, JORDAN, MOROCCO, LEBANON, LIBYA, PALESTINIAN AUTHORITY, TUNISIA, AFRIPOL, LEAGUE OF ARAB STATES

Key Performance Indicators (KPIs) and target values

a) Number of delivered training activities (Target = 5).
b) Number of trained participants (Target = 144).
c) Satisfaction rate Target = 80%

Type of Operational Action (*indicate the main ones - maximum 2)*
(1-Operational, 2-Data collection/data exchange, 3-Strategic, 4-Knowledge/training, 5-Prevention)
3-Strategic, 4-Knowledge/training

Activities under the Operational Action and timing *(Short description– 5 lines maximum per activity)*

Activity	Timing
1) To implement webinar on the subject of online gambling and phishing for EaP countries	Q3
2) To organise regional online course on cyber-attacks for MENA countries.	Q3
3) To implement webinar on cyber-attacks for MENA beneficiaries.	Q4
4) To organise regional course on covert techniques in forensics and mobile telecommunications for EaP countries	Q4
5) To implement webinar on covert techniques in forensics and mobile telecommunications for EaP countries	Q4
6) To prioritise and incorporate CEPOL Exchange Programme in cyber-attacks operations/investigations	Q2-Q4

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)

Ref.: OA 8.2	Leader: Albania (Police Forces)

Activity summary of the Operational Action *(Short description– 10 lines maximum)*:
This OA aims at strengthening cooperation and real-time information exchange between LEAs and CERTs. It also aims at identifying and sharing best practices between EU MS and Western Balkan countries on cooperation between private and public stakeholders.

Key Performance Indicators (KPIs) and target values

a) One Workshop between WB countries and EU MS.
b) Level of satisfaction of the workshop participants (target at least 80%).
c) At least 15% increase of information exchange between LEAs and CERTs (within 6 months folowing the workshop).
d)

Type of Operational Action (*indicate the main ones - maximum 2)*
(1-Operational, 2-Data collection/data exchange, 3-Strategic, 4-Knowledge/training, 5-Prevention)

Activities under the Operational Action and timing *(Short description– 5 lines maximum per activity)*

Activity	Timing
1) Identify the main issues regarding the cooperation between LEAs and CERTs through a questionnaire	Q1-Q4
2) Organize a workshop (address main issues and share best practices)	Q1-Q4
3) Issue a report following the workshop with recommendations	Q1-Q4
4) Explore possibilities for policy and regulatory actions/changes	Q1-Q4
5) Follow-up questionnaire on information exchange flow between LEA and CERTs	Q1-Q4

Links to other Operational Action Plans (OAP)/priority

Horizontal activities / Joint Action Days (JAD)