COUNCIL OF
THE EUROPEAN UNION

Brussels, 20 September 2013
(OR. en)

12759/3/13
REV 3

LIMITE

JAI 671
COSI 98
ENFOPOL 254
CRIMORG 105
ENFOCUSTOM 126
PESC 955
RELEX 708
JAIEX 62
GENVAL 53
CYBER 16

NOTE

From:	General Secretariat of the Council
To:	JHA Counsellors/COSI Support Group
No. prev. doc.:	15358/10, 12095/13
Subject:	Implementation EU Policy cycle for organised and serious international crime: Multi-Annual Strategic Plan (MASP) related to the EU crime priority "cybercrime"

Delegations will find in annex the MASP regarding the EU priority for the fight against serious and organised crime between 2014 and 2017 *"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 document is based on the outcome of the MASP workshop held in Brussels under the auspices of the Commission on 11-12 July 2013 and was agreed following the discussions in COSI on 17 September 2013.

MULTI ANNUAL STRATEGIC PLAN

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.*

1. Description of the scope of the problem

Intelligence gap. Police services in general suffer from a significant dark number in regard to cybercrime. This is caused by several factors. First of all, there are few incentives for victims to report cybercrime. Financial losses for victim are often covered by financial institutions and the latter along with victims in other industrial sectors are refrained from reporting to avoid reputational damage. Secondly, it is difficult for law enforcement to detect crimes. The use of dark net, deep web forums, closed groups, live streaming and peer-to-peer communication make it difficult to observe criminal activities and get a picture of the actual developments in cybercrime.

High-tech crimes such as the creation and deployment of botnets, intrusion and data breaches cause a significant problem for governments and businesses. Distributed denial of service (DDoS) attacks undermine the availability of public services and affect the commercial interests of companies. Especially for businesses that depend on online sales and services the DDoS attacks can serve as an effective instrument for extortion.

Data breaches can be used to undermine the authority and security of states by exposing confidential information as a form of activism. Data breaches affecting the private sector are in particular popular to obtain large quantities of financial credentials such as credit card details. Ransomware affects ten of thousands of internet users per year in the EU. By blocking the computer of a user the perpetrators demand a ransom. Often this is done by pretending to represent a law enforcement authority and claiming that the victim has to pay a fine for inappropriate conduct on the internet.

An increasing problem is the availability of Crime-as-a-Service. No longer technical skills are required to commit cybercrimes. A wide variety of cybercrime services is offered in criminal forums, including sales of hacking tools, botnet rental and tailor made malware. This reduces the threshold for other OCGs to enter the cybercrime domain.

Payment card fraud is another serious problem causing damages of around 1.5 billion Euro per year. Around 40 % of this derives from card-present-fraud where card details are copied by skimming for the production of counterfeit cards that are used to take cash from ATMs or to buy products. The introduction of the EMV chip on cards has pushed the cashing out to the Americas, where the magnetic strips are still used. The other 60 % are accounted for by card-not-present fraud (CNP). The financial details are obtained through phishing and data breaches. Such details are then either used to directly procure products and services online at the expense of the victim or traded at criminal forums on the internet.

Child Sexual Exploitation Online is predominantly non-commercial. Child abuse material is exchanged through various channels by like-minded perpetrators. This includes dark net, like TOR and the Invisible Internet Project (I2P), peer-to-peer and closed groups in social media. The production of child abuse material can take place in a family setting or by travelling sex offenders abroad. Also the live streaming of on-demand abuse is witnessed as well as online solicitation of minors.

In recent years the **virtual underground economy** has matured. It now facilitates at a large scale the cashing out and laundering of the proceeds of crime. The use of bit coins for financial transactions provides the desired level of anonymity to criminals.

2. Existing activities and policies

This chapter does not include information on standard tools and procedures (databases, contact points, meetings, etc.) that are used for cooperation in general. It only contains specific and detailed indications that are relevant for the current strategic goals.

Relevant **EU legislation** in this area is the following:

- Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography (OJ L 335, 17.12.2011), which has to be implemented into national law by December 2013. Its main features include an easier prosecution of offenders, a better victim protection and an increased prevention; more effective means of fighting child sex tourism and of reducing availability of child sexual abuse images on the Internet,

- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013).

Other relevant **EU documents** in this area are the following:

- Commission and the High Representative of the EU for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace (doc. 6225/13) and Council Conclusions on that Strategy (doc. 12109/13),

- Commission Communication "Tackling crime in our digital age: Establishing a European Cybercrime Centre" (EC3) (doc. 8543/12) and Council conclusions on the establishment of EC3 (doc.10603/12),

- Council conclusions on the Global Alliance against Child Sexual Abuse Online (doc.10607/12),

- Commission Communication on a European strategy for a Better Internet for Children (doc.9486/12) and Council conclusions on that Strategy (doc.15850/12),

- Council conclusions on combating sexual exploitation of children and child pornography on the Internet - strengthening the effectiveness of police activities in MS and third countries (doc. 15783/2/11),

- Commission Communication on Critical Information Infrastructure protection (CIIP) "Achievements and next steps: towards global cyber-security" (doc.8548/11) and Council Conclusions on CIIP (doc.10299/11),

- Commission Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (doc.8375/09),

- Council conclusions on a Concerted Work Strategy and Practical Measures against Cybercrime (doc.15569/08),

- Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cask means of payment (OJ L 149, 02.06.2001).

- Council Decision 2000/375/JHA of 29 May 2000 to combat child pornography on the Internet (OJ L 138, 09.06.2000).

Other relevant **EU existing activities and initiatives** in this area are the following:

- Activation of the Friends of Presidency Group on Cyber Issues Working Group within the Council for the purpose of providing guidance and input on horizontal aspects of cyber issues and for exchanging information on these matters (doc.15686/12),

- European Cybercrime Centres of Excellence in Research and Training,

- European Coordination Training and Education Group (ECTEG) hosted by Europol and composed of law enforcement, the private sector, international organisations and the academia for coordination of production, delivery and dissemination of accredited cybercrime investigation training for the Member States,

- European Union Cybercrime Task Force (EUCTF) hosted by Europol and formed by the Heads of EU National Cybercrime Units, Eurojust, Europol and the European Commission,

- Internet Forensic Expert Forum (IFOREX) within the Europol Platform for Experts (EPE) for the hosting and sharing of police best practices and cybercrime training.

3. Identification of potential vulnerabilities i.e. illustration of how the problem should be tackled in the time frame of the full policy cycle

The following potential vulnerabilities were identified, in no particular order:

A. With regards to **"online card fraud"** sub-priority

- lack of priority for law enforcement due to no reporting/underreporting,
- cross-border nature of the crime, with different elements of the offence being committed in different states,
- divergent legislation creating obstacles to cross-border cooperation,
- magnetic stripes being vulnerable, technically easy to obtain compromised data,
- insufficiently strong authorisation of online transactions and authentication of customers,
- low level of sanctions,
- industry lacks knowledge about the seriousness of online card fraud and its role as a facilitator of other serious organised crime,
- lack of awareness about the impact on the EU economy,
- lack of equipment (software and hardware)/resources/capacity/knowledge,
- need for continuous specialised training,
- law enforcement does not keep the pace of criminal development (newer and newer technologies being used by criminals),
- lack of awareness of the law enforcement of the new payment tools developed by industry that are being abused by criminals,
- high-volume and high-return crime with low impact on individuals as being reimbursed.

B. With regards to "**online child sexual exploitation"** sub-priority

- lack of awareness on the threat of parents, teachers, children, media, judiciary,
- vulnerability of children if not being properly monitored while using Internet,
- not harmonized legal framework (no "cloud" EU legislation, "child" data protection),
- instant and secure distribution of child abuse materials among offenders,
- wide range of opportunities for offenders to contact children,
- law enforcement capability not up to the needs (lack of technical equipment, specialized training taking into account the expansion of Internet and development of new features, insufficient intelligence exchange),
- insufficient cooperation between NGO/law enforcement and ISP (e.g. blocking websites),
- too many communication channels in the law enforcement at national/international level,
- no international data base (including on travelling sex offenders),
- cooperation with 3rd countries and/or countries where ICT not well penetrated,
- difficulty to follow the money; assets/money recovery; confiscation and reuse of the money for the victims,
- need to improve international/European cooperation and create database in this field,
- lack of means to transmit and exchange intelligence among countries (intelligence gap)
- problems with information flow from the private sector, need to facilitate its contribution,
- criminal and victim often belong to different countries,
- need of undercover European coordination,
- few people are dealing with identification tasks and analysis.

C. With regards to "**cyber attacks**" sub-priority

- lack of sufficient intelligence on criminal networks (including how they work and recruit) in order to properly identify common threats, prioritise key targets and rapidly change priority,
- lack of awareness on risks/threats both of companies and individual users,
- legal obstacles to:
- receive vital information from private sector as there is no legal obligation to report,
- share information (too complex mechanisms in place, different data retention periods),
- tackle botnets (no EU uniform procedures),
- conduct coordinated investigations/prosecutions,
- incapacity to respond effectively (inability to analyse big amount of data, lengthy judicial proceedings, different data retention periods),
- lack of common taxonomy and common rules for preserving evidence,
- no common format for reporting incidents,
- weak/limited knowledge/skills/capacity of law enforcement and judiciary,
- youngsters attracted to cybercrime as highly profitable,
- many criminals from outside EU, especially in hard to reach countries or countries where MLA agreements are missing,
- too limited use of JITs,
- no incident reporting mechanism for hated messages,
- lack of cooperation and trust among the parties,
- insufficient reporting (private companies reluctant to report) and weak detection of cyber attacks, small number of arrests,
- limited input from the private sector,
- transfer of criminal proceeding is rarely used, cases scattered across MS, damages seem rather small, big cases are missing,
- lack of criteria to act together.

4. Strategic goals: their definition and measurement of achievement:

A. With regards to "**online card fraud**" sub-priority

Goal 1:

Increasing security of non-cash payments[1] by:

– promoting strong authorization of online transactions and authentication of customers,

– promoting a common secure global standard for face-to-face transactions, and

– promoting geo-blocking as an intermediate means of fraud prevention.

- Example of an OAP action: clear definition of strong authorisation of online transactions and authentication of customers based on ECB recommendations; promote EMV by adding it to the EU-US working group on cyber security and cybercrime agenda.

- Measurement of achievement: higher commitment from US to implement EMV, reduction in cards skimming and level of losses caused by this type of fraud, number of countries implementing securing standards.

Goal 2:

Ensuring that law enforcement and judicial authorities have access to the right tools, platforms, training and technical information to combat non-cash payment fraud including new developments in industry such as payment tools or emerging threats and countermeasures.

[1] While there is currently no legal definition of non-cash payment fraud at EU level, it is used here to refer to fraud relating to all non-cash means of payment, including payment cards, such as credit or debit cards (both in the form of card-present and card-not-present fraud), online banking, credit transfers, direct debits and cheques, e-payments and mobile payments.

- Example of an OAP action: provide platform for exchange of experience and best practice; provide repository for tools, e.g. at Europol (Space), develop tools; forensic expert group uniting law enforcement and private sector to find best practices to prevent and investigate non-cash payment fraud; cross-border forensic support; provide training and exchange of good/best practices on threats, prosecution and international cases amongst the law enforcement community, judicial authorities and other relevant actors including private sector.

- Measurement of achievement: number of users registered on the Europol Platform, courses and meetings organised related to this issue; number of early warning messages based on notifications to Europol from Member States and the figure of developed tools.

Goal 3:

Raising awareness of non-cash payment fraud as a crime with a serious economic impact and as a facilitator of other serious forms of crime among law enforcement and judicial authorities, the public and private sector and citizens.

- Example of an OAP action: awareness raising campaigns by the private sector, alone or in cooperation, promote enforcement of cards schemes own rules and regulations and PCI standards; present case studies on specific problems to the judiciary.

- Measurement of achievement: information on the websites of company about non-cash payment fraud and number of press releases; budget and resources dedicated to non-cash payment fraud.

Goal 4:

Improving communication of information between law enforcement and the private sector to obtain an overall picture and information about specific incidents at national and international level including by encouraging the private sector to report non-cash payment fraud.

- Example of an OAP action: quick procedure for receiving data from the private sector on a specific cardholder and other data relevant for the investigation; regular update from private sector regarding to non-cash payment fraud**;** direct contact with the private sector across borders; create a template for reporting of non-cash payment fraud; map obstacles to non-cash payment fraud investigations, encourage private sector to share information on the number of compromised credit cards.

- Measurement of achievement: number of reports received from the private sector in individual cases and availability of updated statistics on payment fraud.

Goal 5:

Improving the exchange of intelligence, information and evidence among law enforcement and judicial authorities across EU and non-EU countries to target OCGs involved in non-cash payment fraud, including by fostering closer cooperation.

- Example of an OAP action: use secure Europol platform for exchange of information; access to SIENA for units that need it; improve quality of information flows to and from TERMINAL database; perform analysis on international criminal networks to target the whole structure, including the leaders/organisers and the technicians; improve cooperation with law enforcement in non-EMV-compliant countries; identify the most affected third countries and create task forces to dismantle OCGs; create a template for collecting all the information regarding to non-cash payment fraud for the law enforcement in the Member States; establish a common information collection point and ensure submission to TERMINAL.

- Measurement of achievement: data available in TERMINAL, use of the template by Member States and number of MLA requests, number of SIENA users who have access to TERMINAL.

Goal 6:

Increasing cross-border investigations and prosecutions against OCGs involved in non-cash payment fraud in the EU and beyond, including financial investigations and asset recovery to make non-cash payment fraud less attractive to criminals.

- Example of an OAP action: increase number of coordinated actions and JITs, including through removing obstacles; coordinate simultaneous arrests and assets recovery across EU Member States; increase the number of parallel financial investigations; coordinated international actions such as the airline fraud action day; improve judicial coordination at EU level.

- Measurement of achievement: increase of JITs number, number of convictions, number and volume of confiscations, number of Eurojust coordination meetings, number of coordinated international actions such as airline fraud action day, number of parallel financial investigations.

Goal 7:

Disrupting OCGs involved in non-cash payment fraud by limiting their access to financial data and credentials, software, technical devices and technical know-how.

- Example of an OAP action: common definition of financial data and credentials; shut down carding websites, monitor and shut down forums.

- Measurement of achievement: number of investigations link to carding websites and forums, number of websites and forums shut down.

Goal 8

Promote harmonisation of legislation in the EU to address legal loopholes in non-cash payment fraud cases, including jurisdictional issues, criminalisation of specific stages of criminal activities and levels of sanctions.

- Example of an OAP action: review of existing regulation on this issue and debate the possibility of a global mandate; review the level of sanctions; identification of the legal loopholes/obstacles.

- Measurement of achievement: amended legislation.

B. With regards to "**online child sexual exploitation**" sub-priority

Goal 1:

To reduce the vulnerability of children to become victims of online sexual exploitation.

- Example of an OAP action: prevention campaign at EU level; develop and provide training material for children, parents, teachers, etc.; develop a grooming detector within the browser; integrate a social media policing (child helpline).

- Measurement of achievement: achievement of the operational action plans.

Goal 2:

To increase and improve the capacity and capability to combat online child sexual exploitation within the EU, with a focus on victim identification, expertise in investigation and forensic techniques.

- Example of an OAP action: establish a specialised capacity for victim identification; establish a European image library; establish a specialised forensic capacity; provide specialised training.

- Measurement of achievement: achievement of the operational action plans.

Goal 3:

To improve cooperation and increase the sharing of intelligence, information and evidence regarding child sexual exploitation and abuse amongst law enforcement and judicial authorities within the EU, inter alia by using EC3 as a focal point.

- <u>Example of an OAP action</u>: working process and routines at EU law enforcement including the systematic sharing of information with EC3 about online child sexual exploitation cases under investigation; implementation of a general data collection information plan both at national and international level; a 6-month update listing strategic and operational activities; increase the use of the Europol Information System to report significant online child sexual exploitation activity.

- <u>Measurement of achievement:</u> achievement of the operational action plans.

Goal 4:

To facilitate and encourage cooperation and the exchange of online child sexual exploitation information by industry, civil society and EU law enforcement, with a view to using EC3 as a focal point.

- <u>Example of an OAP action</u>: national law enforcement authorities to ensure channelling to EC3 information relating to online child sexual exploitation provided by industry located in their territory and operating in different countries, regardless of an actual investigation being conducted by those authorities; agree with NCMEC that reports on EU offenders or victims will channelled via US ICE and EC3, as agreed by Member States.

- <u>Measurement of achievement:</u> achievement of the operational action plans.

Goal 5:

To increase and improve international operational cooperation amongst judicial authorities and law enforcement against online and related offline child sexual exploitation.

- Example of an OAP action: coordinate undercover operations, coordinate joint operation on TOR network; coordinate cooperation on Peer-to-peer networks; coordinate an action day across the EU on Travelling Sex Offenders; analyse online communications in fore by Travelling Sex Offenders about online child sexual exploitation offences they plan to commit and to record.

- Measurement of achievement: achievement of the operational action plans.

Goal 6:

To raise awareness and share best practise on combating online child sexual exploitation by pooling tools, research and techniques amongst industry, academia, law enforcement, prosecutors and judges.

- Example of an OAP action: exchange best practise on undercover operations, forensics. provide repository for tools e.g. at EU level; expert group uniting law enforcement and private sector to find best practises to prevent and investigate online child sexual exploitation; develop a research and development project on TOR (involving academia); define a common standard for sharing and exchanging data.

- Measurement of achievement: achievement of the operational action plans.

Goal 7:

To facilitate and to promote efforts of industry to reduce the availability of child sexual exploitation material on the internet.

- Example of an OAP action: promote blocking technologies; facilitate action by the industry to detect and remove online child sexual exploitation material; develop an upload detector on online child sexual exploitation material.

- Measurement of achievement: achievement of the operational action plans.

C. With regards to "**cyber attacks**" sub-priority

Goal 1:

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

- Example of an OAP action: develop standards on information reporting, information collection and sharing.

- Measurement of achievement: lists of threats and key targets prioritised; number of contributions sent to EC3 focal points; relevant reports.

Goal 2:

To tackle the prioritised threats and targets through joint operational activities, including disruptive actions, joint investigations and coordinated prosecutions.

- Example of an OAP action: take down botnets/criminal forums, disruption of bullet-proof hosting, take down of Automated Vending Carts, develop a method to measure the impact of a joint activity; establish joint investigation team and coordinated prosecutions, conduct asset recovery.

- Measurement of achievement: number of joint activities such as joint investigations and coordinated prosecutions, assets recovered.

Goal 3:

To improve operational and judicial cooperation and coordination with third countries on the prioritised threats and targets.

- Example of an OAP action: coordination of outreach, joint investigations and coordinated prosecutions with the support of EUROPOL, EUROJUST and INTERPOL, liaison officers and liaison magistrates in key third countries.

- Measurement of achievement: number of joint actions (i.e. investigations and arrests), identified relevant third countries, number of relevant countries with dedicated cybercrime liaison officers and liaison magistrates.

Goal 4:

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.

- Example of an OAP action: develop common taxonomy and common format of messages, identify relevant private sector partners, conduct targeted operations with non-law enforcement partners.

- Measurement of achievement: number of contributions exchanged with the non-law enforcement partners, variety of areas of cooperation, number of operational and prevention activities initiated with the non-law enforcement partners, public-private partnerships.

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.

- Example of an OAP action: develop criteria for a serious cyber-attack; define roles for law enforcement, judiciary and EC3 specifically; responsibilities and procedures, cooperate with the relevant actors involved; participate in exercise/ test of the mechanism.

- Measurement of achievement: level of mechanism establishment; relevant actors involved, time for reaction in case of a cyber-attack, cyber exercises and lessons learned therefrom.

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.

- Example of an OAP action: develop a coordinated training strategy involving key partners, including CEPOL, EUROJUST and EC3; engage with all relevant parties; train trainers; train and educate law enforcement, judiciary and key partners; create a central depository of existing tools; exchange programmes.

- Measurement of achievement: training strategy, training events, number of people trained, tools available to law enforcement, judiciary and key partners, harmonised methods, training standards and curricula.

Goal 7:

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.

- Example of an OAP action: common media campaigns (e.g. videos directed at youth), EU-wide specialised alerts, teleconferences (at schools), national cybercrime prevention and planning.

- Measurement of achievement: accurate statistics, number of quality campaigns.

Goal 8:

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.

- Example of an OAP action: identify obstacles in judicial cooperation and legal loopholes (e.g. the legal framework of e-evidence, paradigm of territorial jurisdiction), reporting of data breaches, centralised procedures.

- Measurement of achievement: reports, recommendations from law enforcement, judiciary and relevant parties, specification of legal requirements.