Council of the
European Union

Brussels, 13 December 2017
(OR. en)

15738/17

LIMITE

COSI 332
CYBER 214
TELECOM 361
JAI 1205

NOTE

From:	Europol
To:	Standing Committee on Operational Cooperation on Internal Security (COSI)
No. prev. doc.:	13461/17
Subject:	Improving the EU's fight against cybercrime: EU law enforcement response - Progress report

Delegations will find in annex a progress report on "Improving the EU's fight against cybercrime: EU law enforcement response", prepared by Europol.

ANNEX

The Hague, 13 December 2017

EDOC# 935872v4

Improving the EU's fight against cybercrime: EU law enforcement response

Progress report

At its meeting of 21 November 2017, COSI discussed four elements of improving the EU‘s fight against cybercrime[1], namely

i) Improved fight against criminality on the Dark Web

ii) Joint EU law enforcement response to major cyber-attacks

iii) Reform of the domain name and IP address WHOIS database and improve the accuracy of the RIPE Database

iv) Carrier-Grade NAT and online crime attribution.

and tasked Europol to take forward work at the expert level.

In line with the Estonian Presidency report[2] and following Council endorsement[3] this progress report outlines in more detail concrete steps to be taken in order to implement the measures agreed by COSI as well as provides an update on the progress already made in the short-term.

[1] 13461/17
[2] 14762/17
[3] 14840/17

I. Update on the Roadmap for a Coordinated EU Law Enforcement Response to Criminality on the Dark Web[4]

Planned activities

To improve the fight against criminality on the Dark Web, COSI agreed to develop a roadmap to coordinate and align the Member States´ efforts and practices. The Roadmap will be implemented within the new EU Policy Cycle. During the drafting of the Multi-Annual Strategic Action Plans (MASPs), On-line trade in illicit goods and services was considered as a common horizontal minimum strategic goal.

After the official endorsement of all MASPs and Operational Action Plans in December 2017, Europol will conduct a mapping exercise to identify the priorities and activities of relevance for the Roadmap by addressing specifically the Dark Web aspects of the horizontal strategic goal.

In January 2018, a meeting will be organised at Europol with the relevant Action leaders and Co-leaders in order to discuss the results of the mapping exercise, de-conflict the planned activities and identify synergies and potential Joint Action Days (JADs). A possible outcome of the meeting will be agreeing on executing the second iteration of the Cyber Patrol Action, similar to the one held in June 2017, as well as identifying opportunities for other joint operational actions (takedowns, targeting high-value targets on the basis of the intelligence harnessed from the 1st Cyber Patrol Action and other illicit marketplace takedowns, etc.).

Furthermore, Europol's European Cybercrime Centre (EC3) intends to organise a Dark Web Conference at Europol in 2018, leveraging the power of its network of trusted public and private partners involved in fighting criminality on the Dark Web, or certain aspects of it.

Additionally, depending on the resources allocated to the Agency in 2018 for the new Europol Dark Web team, embedded within EC3, the team will focus on enhancing the support provided to the Member State (MS) experts vested with the responsibility to conduct investigations in the Dark Web. The priority focus will be on improving and/or developing specialised technical tools to facilitate the work of the investigators and to mitigate the resource limitations at national level by providing state-of-the-art support and tailor-made solutions. A team leader for the new team has already been recruited and will take up their function in 2018.

[4] 11809/17

Way Forward

COSI is invited to take note of the above-described planned actions which would be executed in accordance with the resources made available for 2018.

II. Draft Index for the EU Law Enforcement Emergency Response Protocol[5]

Background

The EU Law Enforcement Emergency Response Protocol (LEERP) is intended to be a tool to support the EU LE authorities in addressing transnational cyber-attacks through the fast and effective sharing of relevant information and the coordination of the international implications of their investigations. As such, the LEERP strives to determine clear roles and responsibilities, the procedures and channels for the exchange of critical information, as well as the overall coordination and de-confliction actions during and in the immediate aftermath of such an attack.

Cognisant of and in accordance with the applicable crisis management mechanisms existing or under development at national level, the LEERP will also complement the procedures in other relevant frameworks such as the Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises.[6]

Draft Index for the LEERP

The herewith proposed index for the LEERP was elaborated in line with the discussions held during the dedicated expert workshop organised in September 2017[7] and the contributions from COSI and COSI Support Group. Additionally, the European Union Cybercrime Task Force (EUCTF), composed of the Heads of the EU MS National Cybercrime Units, was also consulted in November 2017, thus their feedback and country-specific preferences have also been taken into consideration.

The proposed detailed framework for the LEERP is described below in the form a flow chart (see Figure 1 below) as well as additional explanatory remarks, building upon the main steps outlined in the initial concept note.

[5] 11809/17
[6] C(2017)6100
[7] 13461/17

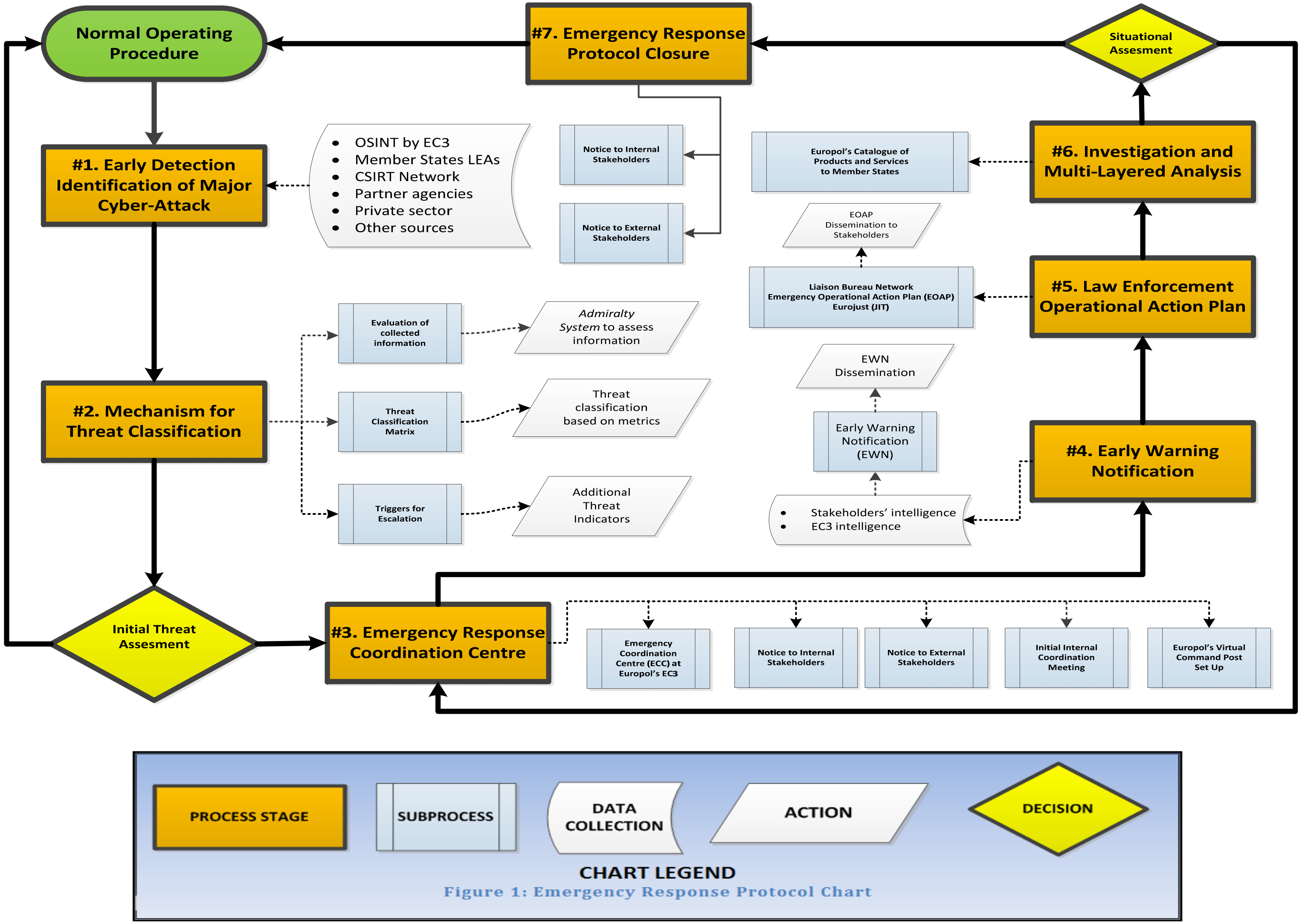
Normal Operating Procedure
#7. Emergency Response Protocol Closure
Situational Assesment
#1. Early Detection Identification of Major Cyber-Attack
OSINT by EC3
Member States LEAs
CSIRT Network
Partner agencies
Private sector
Other sources
Notice to Internal Stakeholders
Notice to External Stakeholders
Europol's Catalogue of Products and Services to Member States
#6. Investigation and Multi-Layered Analysis
EOAP Dissemination to Stakeholders
Liaison Bureau Network Emergency Operational Action Plan (EOAP) Eurojust (JIT)
#5. Law Enforcement Operational Action Plan
Evaluation of collected information
Admiralty System to assess information
Threat Classification Matrix
Threat classification based on metrics
Triggers for Escalation
Additional Threat Indicators
#2. Mechanism for Threat Classification
EWN Dissemination
Early Warning Notification (EWN)
#4. Early Warning Notification
Stakeholders' intelligence
EC3 intelligence
Initial Threat Assesment
#3. Emergency Response Coordination Centre
Emergency Coordination Centre (ECC) at Europol's EC3
Notice to Internal Stakeholders
Notice to External Stakeholders
Initial Internal Coordination Meeting
Europol's Virtual Command Post Set Up
PROCESS STAGE
SUBPROCESS
DATA COLLECTION
ACTION
DECISION
CHART LEGEND

Figure 1: Emergency Response Protocol Chart

I. Early Detection and Identification of a Major Cyber-Attack

This chapter will elaborate on the specific mechanisms for early detection and identification of a major cyber-attack which poses an imminent and high impact threat to multiple victims and/or severe compromise affecting critical infrastructure(s) and disrupting the functioning of key services in the MS.

It entails multiple avenues for receiving the initial information and stemming from one or more of the below indicated key stakeholder groups:

1) Open Source Intelligence Monitoring function performed by Europol’s European Cybercrime Centre (EC3) Cyber Intelligence Team.

2) Law Enforcement/Competent Authorities.

3) Network of the national Computer Security Incident Response Teams (CSIRT), also known as CSIRT Network.

4) Partner agencies and institutions (ENISA, CERT-EU, EDA, Eurojust, EU INTCEN, EEAS, INTERPOL, UNODC, OSCE, etc.)

5) Private sector partners.

6) Other sources (academia, research institutes, etc.).

It is notable that if there is no clear indication that a particular major cyber incident resulted from a technical failure or a natural disaster, it is presumed that it is a cyber-attack with criminal intent behind it, which should be handled as a crime by the responsible LE and the judicial competent authorities, unless and/or until proven otherwise.

Under 1), EC3 detects and identifies the major cyber-attack or a cyber incident of a suspect criminal nature on the basis of primary sources (intelligence collection) and secondary sources (cyber intelligence solutions).

Under 2) to 6), the respective actor from the different stakeholder group notifies EC3, on the basis of their information.

II. Mechanism for Threat Classification

This chapter will focus on the initial triage of the available information and the threat classification procedures from a LE perspective in order to provide a shared situational awareness and decide whether the specific cyber-attack warrants the triggering of the LEERP or it should be handled within the applicable normal operating procedures.

The mechanism includes:

1) **Evaluation of the information collected under I.:** the reliability of the source and the credibility and the veracity of the information shall be done according to the Europol Evaluation System (4x4) or to another system agreed by the MS experts, such us the *Admiralty System*.

2) **Threat Classification Matrix:** is a method for accurately and consistently classify cyber threats. It will be based on the existing metrics and developed together with the MS expert input.

3) **Triggers for Escalation:** identification of additional criteria to escalate a threat classified at a lower level to a level that demands emergency response (high likelihood of broader propagation, high probability of impact on critical infrastructure(s), political reasons, etc.)

4) **Initial Threat Assessment:** on the basis of the initial triage and the 3 above-mentioned steps, a decision to launch the LEERP or not is taken.

If the threat does not demand an emergency response, the process will finish at this stage. If it calls for an emergency response, the process will continue by following the next steps described below.

III. Emergency Response Coordination Centre

The chapter will outline the concrete actions to be taken in the framework of the LEERP towards enabling the effective operational and technical cooperation at LE level and enabling the efficient collaboration with the other key players in the cyber security ecosystem.

1) **Establishment of an Emergency Coordination Centre (ECC) at Europol's EC3:** EC3 identifies the Emergency Response Team and personnel distribution per shift if necessary and in accordance with the specific threat and the skillset required to support the MS efforts (ex. malware analyst, digital forensic expert, decryption expert, cryptocurrency analyst, operational analyst, etc.).

2) **Notice to Internal Stakeholders:** EC3 communicate the internal Europol stakeholders the triggering of the LEERP and the Points of Contact (PoC) for the ECC; these stakeholders are other relevant Europol units and the Europol Liaison Bureau Network, including the Joint Cybercrime Action Taskforce (J-CAT).

3) **Notice to External Stakeholders:** EC3 communicate the external stakeholders the triggering of the LEERP and the Points of Contact for the ECC. These stakeholders include the 24/7 LE PoCs (list to be agreed and provided as an Annex to the LEERP), the CSIRT Network, other partner agencies and institutions (ENISA, CERT-EU, Eurojust, INTERPOL, European Commission, Council Secretariat, etc.), trusted private sector partners that could add value to the subsequent investigation, and the crisis communication PoCs of the European Commission.

4) **Initial Internal Coordination Meeting:** depending on the situation and available resources, an internal coordination meeting may be organised between the EC3 Emergency Response Team and/or representative with the Europol Liaison Bureau representatives of the MS, including the J-CAT and other internal stakeholders of relevance.

5) **Set Up of the Europol's Virtual Command Post:** set up of the secure communication channel to facilitate real-time critical communications and on need-to-know basis with the different stakeholder groups.

IV. Early Warning Notification

This chapter will elaborate on the preparation and immediate dissemination of information from the LE angle to the different key stakeholders.

Its process includes:

1) EC3 collates the input from the key stakeholders and makes the initial tactical assessment of the situation, including potential mitigation measures (if such have been identified).

2) EC3 produces the Early Warning Notification (EWN) at the respective classification level and in compliance with the data handling procedures and the Europol Handling Codes.

3) EC3 disseminates the EWN to the different stakeholders.

4) The EWN will serve as input to the shared situational awareness referred in the Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises.

V. Law Enforcement Operational Action Plan

The chapter will focus on the development of a joint LE Operational Action Plan, which would be prepared during an emergency operational coordination meeting and/or a secure communications, should there be insufficient time to organise a physical meeting with the LE representatives.

The following steps are included:

1) EC3 notifies the Europol Liaison Bureau network, the LE PoCs, and where relevant Eurojust, of the date and location for the emergency meeting/conference call.

2) Emergency Operational Action Plan (EOAP) is drafted, including the proposed course of action and agreed upon roles and responsibilities; this enables the de-confliction of the ongoing and the planned country-level activities and ensures that the vital intelligence will be captured in a lawful manner thus making it possible to use it evidentiary later on.

3) A potential Joint Investigation Team (JIT) could be considered by the judicial authorities involved in the investigations, supported by Eurojust.

4) EC3 disseminate the outcome of meeting and the EOAP to the stakeholders involved.

VI. Investigation and Multi-Layered Analysis

This chapter will elaborate on the intelligence-led policing activities at MS and EC3 level. The intelligence collected by the MS as a result of the multi-layered analysis of the information is contributed to EC3 towards being pooled together in a secure and centralised repository in Europol's criminal intelligence databases. This enables the identification of any links and facilitates the data examination, querying, categorisation and intelligence packages creation per relevant jurisdiction, in relation to both the technical and the financial investigative angles.

On this basis, EC3 will deliver the relevant items from Europol's official Catalogue of Products and Services in support of MS investigations, in accordance with the specific needs and the type of threat (operational analysis products, forensic analysis reports, cross-match reports, etc.).

Depending on the findings and the continuous open source intelligence gathering and monitoring of the threat evolution over time, additional operational coordination meeting(s) and/or secure conference call(s) may be organised. Where necessary, the Emergency Operational Action Plan is also updated.

VII. Emergency Response Protocol Closure

This chapter will outline the final steps related to the closure of the LEERP.

Once the immediate threat has been contained, the LEERP can be officially closed. Containment in this case signifies either that the investigation has led to an operational success, or that the competent authorities will proceed investigating but following the normal operating procedure as the emergency aspects of the cyber-attack have been mitigated.

A closure notice is sent to the same internal and external stakeholders who received the initial notice when the LEERP was triggered.

Way Forward

The above-described detailed framework for the EU Law Enforcement Emergency Response Protocol and the associated processes will be further developed in 2018 during follow-up expert workshops, planned within the framework of the 2018 OAP Cybercrime-Attacks to Information Systems.

The input gathered will serve as basis to formulate the final draft of the LEERP, which will be submitted to COSI for endorsement in 2018.

III. Update on the reform of the domain name WHOIS database

1. Background

For many years, law enforcement agencies (LEAs) have relied on WHOIS services, which provide publicly available domain name registrations information. The WHOIS is a key tool to investigate and attribute crime.

Data Protection Agencies have taken issue with the public availability of personal data contained in the WHOIS[8]; nonetheless ICANN policy related to WHOIS in generic top-level domains (gTLDs) has not evolved significantly as the community did not manage to come to agreement on any replacement policy, and LEA access to such data has been largely unaffected.

This is now set to change fundamentally with the entry into effect of the EU General Data Protection Regulation (GDPR) on 25 May 2018. A growing body of legal opinions[9] recognizes that collection and publication of personal data contained in the WHOIS database is unlawful and that compliance with GDPR will likely involve reducing the number of data elements collected and implementing purpose-based access to differentiated subsets of the remaining registration data, also known as **layered access.**

[8] https://www.icann.org/en/system/files/correspondence/falque-pierrotin-to-chalaby-marby-06Dec17-en.pdf

[9] https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf; https://gnso.icann.org/en/drafts/wsgr-icann-memorandum-25sep17-en.pdf

As a consequence, while the legitimacy of law enforcement access to registration data, including personal data, for investigations purposes is generally not challenged, LEA access to such data will be affected, both from a practical and from a legal perspective. Practically speaking, there will be fewer data elements and therefore fewer leads available. Cross-referencing data elements across different registrations, e.g. to identify which other domains a bad actor may have registered using the same information, would likely no longer be possible.

Currently under consideration are the following models:

- a model where every WHOIS lookup would require an individualized request justifying the purpose for access, specific data elements sought, etc., possibly validated by a judge;
- a model where some form of authentication would be provided, allowing access for law enforcement by means of logins and passwords. Such access might be provided through a centralized clearinghouse logging access requests and verifying proportionality.

While such models are advantageous from a data protection perspective, they might create a number of challenges and risks for law enforcement. In particular, individualized access requests would be difficult to fathom in view of the fact that one cyber unit might make as many as 50,000 lookups a week. Tracking and tracing law enforcement activity might reveal sensitive data, potentially compromising investigations if revealed or illegally accessed.

In addition, while law enforcement access is not contested, it is unclear whether and how other relevant actors would maintain current levels of access. This concerns in particular cybersecurity authorities, private sector companies and academic researchers; consumer protection authorities, or IP right holders.

2. Suggestion for an EU joint message

In order to guarantee EU LEA access to essential WHOIS data, it is suggested to define a **set of minimum requirements for LEA access** and to ask ICANN to implement these requirements in order to guarantee timely LEA access to the appropriate elements of a **GDPR-compliant Registration Directory Services (RDS).**

These minimum requirements should also be used as a joint input from the EU LEA community to the RDAP pilot program currently underway, testing a replacement protocol to WHOIS which does not allow for gated access[10].

Because a layered access model implies **credentialing**, **authenticating** and **authorizing users** to access data that is not made public and may be hosted in foreign jurisdictions, below is a first series of draft minimum requirements for a future layered access model for discussions.

3. Proposal for minimum requirements for LEA access to a future layered access model to domain registration data:

Any layered access model for domain registration data would need to fulfil the following requirements in order to support legitimate LEA access to restricted data:

a. <u>Necessary data elements</u>

- Delegates are invited to seek feedback from national law enforcement to identify those data elements currently available that are essential to law enforcement investigations and need to remain available.
- According to current considerations, it is likely that information such as the Technical Contact, Billing Contact and Administrative Contact would disappear. Furthermore, reverse lookups would not be supported.
- Delegations are invited to refer to the eco data flows model[11] as an example of a possible future model.

[10] https://community.icann.org/display/RP/RDAP+Pilot

b. Accreditation system

Global versus national accreditation systems?

Delegates are invited to reflect upon the 2 different options:

- Accreditation of LEA and CSIRT requestors for global access to RDS data should be carried out at national level by a designated national central authority (RDS user accreditors), according to national policies.

  OR

- Accreditation of LEA and CSIRT requestors for global access to RDS data should be carried out at global level by designated global central authorities such as ICANN (RDS user accreditor).

The following factors are proposed for consideration as essential elements of an accreditation system:

- The accreditation decision is made according to the need for the requestors to access data elements on the basis of permissible purposes defined by ICANN RDS policies.

- Accreditation must allow access to any gTLD[12]'s restricted RDS data that may be sought under national law.

- Access should be granted to the system, rather than requiring an individually justified request each time.

- RDS user access credentials must be tied to an auditable accreditation system.

[12] Generic Top Level Domains (.com, .org etc.)

c. **<u>Authentication of Access</u>**

- Accredited requestors (at the national level or at global level) must be provided with the necessary level of access to requested gTLD domain registration data through a <u>unique set of credentials</u>.

- Registration data lookups by authorized users must be anonymized ensuring confidentiality of the request possibly through a system of hashes.

- Queries by accredited and authenticated actors must not be logged in order to guarantee the confidentiality of investigations.

- There shall be a balance between accountability (log query) and safety of the searches, by accredited and authenticated actors for the purposes of verifying the lawfulness of data processing, monitoring and auditing and ensuring proper data integrity and security

- Authentication mechanisms should be compatible with the rate of look-ups expected from authorized users

d. **<u>Access policy and data location</u>**

- Accredited and authenticated requestors must have access to all available information provided by registrants in compliance with the 2013 Registrar Accreditation Agreement (RAA).

- Access to gTLD WHOIS data needs to be maintained regardless of location of storage. This could be performed in practice through a centralized federated access system, e.g. hosted by ICANN.

- Delegates are invited to verify that access to data can be maintained regardless of storage location, as is currently the case. Individualized legal process should be avoided, as it would significantly slow down the investigation process, which is a serious concern as some law enforcement agencies do as many as ten thousand WHOIS lookups per day and is not justified in view of the low level of impact on fundamental rights.

e. Accuracy and validity of data

- As stipulated by the GDPR and in line with the obligations of contracted parties under their contracts with ICANN, personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. To comply with the data quality principle, reasonable steps should be taken to ensure the accuracy of any personal data obtained.

f. Data Retention and Record of Historical RDS Data

- In order to ensure the availability of historical RDS information, the RDS system model should allow access to historical domain data retrospectively. Historical domain and IP ownership information[13] is necessary for the success of investigation by LEA and other parties, thus an adequate retention policy of historical data should be allowed for.

- The data retention period for the different categories of personal data should be based on individual business needs and proper data protection assessment. A judgement must be made about: the current and future value of the information; the costs, risks and liabilities associated with retaining the information; and the ease or difficulty of making sure it remains accurate and up to date. How long personal data shall be kept depends on the purpose for which it was obtained and its nature.

- Such records should also be searchable in such a way as to allow for cross-referencing of information, e.g. where the same data set was used to register several sites.

- In line with the storage limitation principle, data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes.

[13] For example as offered by Domaintools.

Way Forward

- Delegates are invited to reflect upon the proposed minimum requirements and consult their experts to complement those.
- On that basis a joint EU position would be prepared for endorsement by COSI.

IV. Carrier-Grade NAT

1. Background

Given the limited number of IP addresses available under IPv4, CGN technologies are used by Internet Access Providers to share one single IP address among multiple subscribers at the same time (possibly several thousands), making it technically impossible for the companies to comply with legal orders to identify individual subscribers on the basis of an IP address. This in turn leaves many crimes unpunished.

To improve the capability of law enforcement authorities to investigate and attribute online crime, COSI agreed that **voluntary codes of conduct** should be proposed with Internet Access Providers operating in the EU to commit to limiting the number of subscribers behind each Internet Protocol Version 4 (IPv4).

Additionally, COSI agreed that **alternative technologies to Carrier Grade Network Address Translation (CGN)** should be deployed.

COSI also recommended **engaging with Internet Content Providers, within the EU Internet Forum, to log source port numbers** as an additional measure to facilitate cybercrime investigations.

EU Member States also included relevant actions to address the negative impact of CGN in the *Action plan for implementation of the Council conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*[14].

In particular by calling the Member States to provide incentivizes for the private sector deployment of IPv6, e.g. through possible introduction of requirements in public procurements.

[14] 14965/17

2. Update

Europol will organise a number of dedicated CGN-related meetings in 2018 to further engage with key Internet Access Providers, explore alternative technologies to CGN and convince IAPs to limit the number of subscribers behind each global IPv4.

More specifically, in Q3 2018, Europol could host a meeting, co-organised with the European Commission and the incoming EU presidency, to gather European LEAs and major EU-based IAPs which are willing to conclude a voluntary code of conduct and limit the ratio subscribers/global IPv4 address, to jointly address the problem of CGN.

Europol will continue to support the EU LEA network of CGN specialists, document cases of non-attribution linked to CGN.