027044/EU XXVI. GP
Eingelangt am 18/06/18

Council of the
European Union

Brussels, 18 June 2018
(OR. en)

8928/1/18
REV 1

CORDROGUE 47
SAN 147
ENFOPOL 230
CYBER 114
COPEN 162

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	7628/18
Subject:	"Challenges and possible solutions of tackling Internet and especially Darknet related drug crime": Presidency summary of the thematic discussion held at the HDG meeting

Delegations will find below the above-mentioned Presidency summary paper, as revised taking into account delegations' comments provided at and after the HDG meeting on 30 May 2018.

_____

www.parlament.gv.at

ANNEX

"Challenges and possible solutions of tackling Internet and especially Darknet related drug crime": Presidency summary of the thematic discussion held at the HDG meeting

On 17 April 2018 the Bulgarian Presidency organized a thematic discussion on the challenges and possible solutions of tackling Internet and especially Darknet related drug crime at the Horizontal Working Party on Drugs (HDG). The aim was to launch a first reflection on the practice, challenges and needs of the relevant stakeholders in the EU Member States in tackling more successfully this new phenomenon.

The subject was examined in the context of the significant drug problem and the rapid emergence of the internet as an online marketplace for drugs. Delegations actively participated in the discussion at the meeting and a number of them send the written comments after the meeting (CY, CZ, DE, EE, FI, FR, HR, HU, IT, LT, LV, PL, PT, SK, UK, IE, Europol and EMCDDA). It was acknowledged that the proliferation of the virtual crime markets poses additional challenges for law enforcement authorities in terms of understanding, monitoring and tackling this phenomenon. Due to the specificities in the functioning of the Darknet markets, the investigations and proving of the criminal activity of the vendors is a great challenge for law enforcement.

During the discussion Member States agreed that drug trafficking on the internet and Darknet is a type of crime which has to be taken seriously in the frame of the holistic approach that most of the member States are applying when tackling the criminal threats on the dark web. Although there is a broad range of potential measures and measures already in place for tackling this phenomenon from the law enforcement prospective, that need to become more enrooted in the daily routine. There was also a general agreement that it is a unique opportunity for policy makers and law enforcement to tackle a new crime field at its beginning.

As a result of the discussion and the subsequently provided written contributions, the following general considerations emerged.

www.parlament.gv.at

With regard to the actual situation:

- In the field of prevention and countering the problem of drugs and Darknet there is still no specific - legislation at national level, as the general rules of carrying out criminal investigations are applied. However, some countries are taking initiatives to adapt and utilize the existing legislation in order to respond to the issues arising from the criminal use of Darknet. As to the measures in place in the field of prevention and countering this phenomenon, many of the Member States consider taking future actions such as creating dedicated working groups, starting training programmes and developing new strategies. Only few countries do not plan taking actions or developing such measures in the near future.

- In most Member States there is more than one structure/competent authority which share the responsibility for combating drug related crime including Darknet (most often these are the police authorities, the customs authorities and the judicial authorities). In some Member States specialized drug units have been set up and trained to support investigations such as in the field of cybercrime that require specialized technical knowledge.

- As to the experience on international level regarding dismantling of Darknet markets, some good results have been achieved thanks to joint actions and international cooperation. Europol (especially through Cyber patrol week and EMPACT activities), Eurojust, and partner countries' law enforcement authorities (eg. the US) played an important role in facilitating international cooperation in this respect. The wide and open exchange of information has been pointed out as vital for the law enforcement and the judiciary.

- As a general rule, international cooperation and coordinated actions are **critical** measures against illicit activity on the Darknet. Moreover the development of public-private partnerships is essential for the successful tackling of this phenomenon.

www.parlament.gv.at

- The challenges and the weaknesses in tackling this phenomenon are common for most of the Member States. Law enforcement authorities have to take account of the current development of data protection and retention policies on EU level due to some recent ECJ judgements, which does not facilitate the collection of data for the purposes of the investigations. At the same time, the high level of anonymity offered by the Darknet drug marketplaces, the use of bitcoins or other cryptocurrencies and the hidden location of the vendors make it difficult to trace the operators of the marketplace. The content on the Darknet platforms cannot be indexed by the major search engines of the Internet, such as Google, Firefox or Internet explorer and in order to access this content, a computer application different from the usual browsers is required. It is therefore substantial to develop alternative survey techniques that will make it possible to obtain data from the source. Solving different technical issues, the need of well-trained IT experts and the implementation of new tools and methods are essential for better understanding and addressing the problem in its complexity.

With regard to the way forward:

The general conclusion resulting from the discussion is that the relevant stakeholders in the Member States are aware of the need to upgrade their knowledge, capabilities, practice and tools in order to tackle more efficiently the Internet and Darknet related drug crime.

As a result the following non-exhaustive list of recommendations could serve as a basis for consideration as regards the concrete future actions to be taken.

Strategic and legislative

Effective use of the existing international and national legislation to tackle Internet and Darknet related drug crime could be sufficient for the moment, however a close eye on possible future developments is needed and the necessity for specific legislation addressing the use of Darknet could be considered across the relevant working parties in the future.

www.parlament.gv.at

- Currently the adoption of a common strategy as regards tackling Internet and Darknet related drug crime on EU level remains difficult. However, in case this initiative is considered in the future, it should take into account the holistic approach to Internet related crime.

Operational

- Better centralization of the information by considering the possibility of establishing national contact points within one central body;

- Pooling of expertise in the field of research, modus operandi of the perpetrators and best practices;

- Improving and simplifying the exchange of information and finding workable solutions for the availability and use of e-evidence;

- Enhancing the international cooperation at a horizontal and vertical level between law enforcement, judiciary and customs authorities;

- Considering the organisation of joint investigations;

- Using the experience of Member States' and Europol's "cyberpatrols" while developing concrete actions in the Darknet;

- Developing public-private partnerships with the internet providers and postal operators;

- Developing methodology and tactics for combating illegal on-line drug trafficking, by finding solutions for dealing with practical issues regarding financial institutions, Internet regulatory bodies as well as judicial bodies (state attorneys, courts, etc.);

www.parlament.gv.at

Operational actions as regards prevention

- Use the unique potential of Internet-based prevention approaches to selectively target the most appropriate groups, offer tailor-made prevention services and address and correct misperceived social norms;
- Develop and promote guidelines, tools and methods for parents and care-givers to effectively prevent, notice and react to the use of internet by children and young people to acquire illegal drugs;

Role of EU bodies

Delegations agreed on the important role of the EU bodies in supporting Member States by providing expertise (Europol), training (CEPOL) and research (EMCDDA and Europol) on the Drugs and Darknet phenomenon.

At the same time, the EU institutions could take action on or support the Member States in pursuing the following actions:

- Promote agreements and protocols with Internet service providers in order to prevent unlawful use of their platforms;

- Develop a toolset for practitioners to ensure effective prevention and effective counteraction, i.e. de-anonymization and other relevant IT solutions, development of human resource capabilities, involvement of private sector into the process, as well as sufficient legal premises for electronic communication data retention;

- Raise awareness of postal services, including the express postal services;

- Organise training in order to ensure a broad outreach to all relevant stakeholders from the public and private sector;

- Support the Member States in regard to an access to the new cyber solution IT programs.

www.parlament.gv.at

Role of Europol

- Europol should be the central body at EU level for technical support and the exchange of information by using the Secure Information Exchange Network Application (SIENA);

- Europol has established a Dark Web Team and a roadmap for a Coordinated EU Law Enforcement Approach to Addressing Criminality on the Dark Web. This was endorsed by COSI and the Member States in December 2017. As such it is now established in the EU Policy Cycle and is comprised of eight focal points:

    1. Information position
    2. Operational support and expertise in different crime areas
    3. Tools, tactics and techniques to conduct Dark Web investigations
    4. Prioritisation of top threats and/or targets
    5. De-confliction among the different entities involved
    6. Joint technical and investigative actions
    7. Training and capacity building
    8. Prevention and Awareness Raising

www.parlament.gv.at