COUNCIL OF
THE EUROPEAN UNION

Brussels, 9 January 2013

17225/1/12
REV 1

LIMITE

ENFOCUSTOM 137
ENFOPOL 406

NOTE

From:	Czech delegation
To:	Customs Cooperation Working Party
Subject:	Draft report of Action 5.2 "To examine the working/investigative techniques applied by customs and other law enforcement authorities to combat customs related crime, including organised crime, through the Internet, and to explore the current situation regarding the existence of Customs Internet Crime specialised units"

Delegations will find enclosed the revised draft of the above-mentioned final report on Action 5.2.

Changes compared to the previous version are underlined.

Table of Contents

1. Introduction

The reinforced strategy for customs cooperation adopted by Council Resolution of 23 October 2009[1] has been implemented by the Customs Cooperation Working Party (CCWP) in the form of Action Plans lasting 18 months.

The Fifth Action Plan for the period of 1 July 2011 and 31 December 2012, approved by the Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS) on 22 June 2011[2], comprises 10 actions, including action 5.2. “To examine the working/investigative techniques applied by customs and other law enforcement authorities to combat customs-related crime, including organised crime, through the Internet, and to explore the current situation regarding the existence of Customs Internet Crime specialised units”.

Internet is a fast growing medium which offers an easy access to a wealthy set of information, entertainment, services or communication tools. As such, it intensely affects and transforms modern life while making it easier. Owing to the Internet expansion, also the public sector and industry have undergone over the last few years a number of changes. The paperless customs initiative or the e-commerce trend could be mentioned in this respect.

However, the increasing number of online users has not brought only positive effects. It has also opened up new methods for the commission of crime. It is a matter of fact that cybercrime[3] is, nowadays, one of the fastest growing areas of crime, involving organised criminal groups too. Thanks to its speed, expediency and anonymity, the Internet based technology has become one of the key facilitators for a vast range of criminal activities, including those of customs competence, such as distribution of counterfeit products, excisable goods or goods subject to prohibitions and restrictions.

[1] OJ C 260, 30.10.2009, p. 1.

[2] 10223/3/11 REV 3 ENFOCUSTOM 45

[3] Cybercrime has a very broad scope ranging from offences related to the interference with information and communication technologies to more conventional ones such as fraud, distribution of child pornography or illegal trade in commodities. It is often used interchangeably with other terms like “computer crime”, “computer-related crime”, “electronic crime” or “Internet crime.” For the purpose of this report, it was agreed to use the term *“Internet Crime”* in the meaning of *“fraudulent and/or criminal acts of customs-related responsibility committed or facilitated by the use of Internet.”*

Customs is the lead authority for control of and the fight against illegal trade in goods crossing the external borders of the EU and has contributed within its competencies to the fight against the illegal trade in goods within the EU customs territory. Nevertheless, along with the growing computerisation of the society also the trade has increasingly moved towards the virtual space. Internet has become a perfect virtual market place where people can buy almost all kinds of products, not excepting the illicit ones like drugs, arms or counterfeits. These goods are then physically delivered/transported in violation of EU- and national customs laws. As a platform for companies and individuals to present their products or services and as a communication tool, it is moreover an important source of information which might be of use while preventing, detecting, investigating and prosecuting a customs related fraud or crime.

Considering the global nature of the Internet, no crime is as borderless as cybercrime. This makes it essential for the law enforcement authorities, including customs, to adopt a coordinated and collaborative approach across borders, together with public and private stakeholders.

Bearing in mind the above-mentioned, Action 5.2 aimed at identifying ways for customs authorities to enhance their capabilities and to make the investigations into customs infringements as much effective as possible while bearing in mind the crime-facilitating role of the Internet.

Statements and conclusions drawn by the report are based mainly on practical considerations leaving aside the legal questions relating to the work and powers of specialised customs Internet crime units in each Member State.

2. Objectives

Under the Reinforced Strategy on customs cooperation, the following strategic objectives were set out with regards to action 5.2:

- to consider new forms of cooperation and new investigative techniques
- to take practical steps towards implementing these new forms of cooperation and to continue to further develop existing forms of cooperation
- to improve and make more flexible the existing cooperation process

The following possible outcomes were identified:

- Setting up of units specialised in combating the use of Internet for criminal purposes and linking them up to existing specialised networks among law enforcement bodies;
- Improved cooperation between existing customs Internet crime specialised units;
- Identification and exchange of best practices;
- New working methods and investigative techniques in fighting illicit trafficking of goods facilitated by the use of Internet.

3. Working methods (of the project group)

In December 2011 the CCWP mandated under the Czech leadership a project group to implement Action 5.2. The participants in the group were Austria, Belgium, Finland, France, Germany, Hungary, Italy, the Netherlands, Poland, Spain, Sweden and the UK. The Commission (OLAF) joined the group at a later stage.

At the time of starting this action, the level of knowledge about existence of specialised teams dealing with Internet based investigations was very limited. Thus, it was first necessary to gain an overview of the current situation in the EU Member States and only then draft a mandate which would properly meet the challenges entailed by growing criminal misuse of the Internet. For that purpose the Czech Republic prepared a short questionnaire which consisted of the following questions:

"Do you have a special unit dealing with customs-related Internet crime and/or fraud within your customs administration?

- *If so, please provide the contact details of the responsible person who would be willing to answer to several questions (by email or phone) regarding the organisation, structure and the tasks this unit is entrusted with.*
- *If not, do you plan to establish such a unit in the near future?"*

By the end of September 2011, a total of 23 answers were received with the following outcome:
8 Member States (AT, CZ, DE, FR, HU, NL, PL, SE) responded to have a team of Internet crime specialists and 7 countries (BE, ES, FI, IT, LT, LU, SK) replied that they were in process of setting up or planning to set up a unit in the near future.

After having summarised the answers, the project group held its first meeting to discuss and agree on the mandate. Besides continuously raising awareness on the customs related Internet crime and following the results of the questionnaire, the action should have addressed two main issues, to provide assistance to the countries in process of establishing a specialised Internet crime structure within Customs and to enable the exchange of experiences between already existing units.

To clearly determine the scope of the project group's activities, it was first necessary to clarify the term "Internet crime." The project group agreed on the following meaning "fraudulent and/or criminal acts of customs-related responsibility committed or facilitated by the use of Internet".

When defining the action's objectives, the project group decided to establish also activities which were to be undertaken in order to achieve the set goals. An overall assessment of the activities done is summarised below:

- *"To raise awareness on the possibilities of fighting Internet-related crime within customs authorities"*

  With a view to achieve this goal, the CZ presented the CCWP's initiative relating to the fight against customs related Internet Crime at various international fora such as 15th Meeting of RILO WE's National Contact Points or 7th WCO Counterfeiting and Piracy Group.
- *"To assist the Member States in process of establishing a Customs Internet Crime Unit/appointing a specialist to deal with customs related crime facilitated by the use of Internet"*

  Considering the number of Member States which were planning to set up a specialised Internet Crime Unit or in the process of setting-up such structure, the project group drafted a short document with guidelines on how to start investigations on the Internet. Previous experience has shown that the already existing customs Internet crime units (hereinafter Customs Internet Crime Units or Specialists are to be referred to as CICU/Ss) were built almost as "greenfield projects" and the Member States were usually lacking a sort of summary of basic requirements for the establishment of a CICU/S. With a view to remove this shortcoming and to provide the decision-makers with an idea about what it is necessary for a CICU/S to be operational, it was decided to produce the document entitled "**Basic requirements for the establishment of a Customs Internet Unit**", which is an annex to this report issued as a separate working document (DS 1831/12).

Furthermore, the participation itself in this action of some of the Member States which plan to establish a dedicated unit has considerably contributed to the achievement of the above goal.

- *"To provide for an exchange of experiences between Customs Internet Crime Units/Customs Internet Crime Specialists"*
  Exchange of experiences was one of the key parts of the whole action. The project group discussed several possibilities of how to enable this exchange in the most efficient way. One of possible options was to organise a dedicated seminar. However, considering the budget and time restrictions, it was decided to use the project group meetings instead.

  In order to take advantage of the questionnaire as a useful tool for gathering information while minimizing the time required for its completion, the CZ drafted a **questionnaire** focusing on different areas of CICU/Ss' functioning (e.g. tasks, activities, web/software equipment, etc.) which was subsequently circulated and completed on-site during one of the project group meetings. Further work of the project group was based for the most part on the outcome of questionnaire.

  Another activity which was identified as a possible way of exchange experiences was to organise a "**joint action/measure**" (similar to joint customs operations) consisting in an Internet search. Such measure would include also a training session dedicated, in particular, to those Member States which are at an early stage of setting up a specialised unit. This topic was largely discussed at each of the project group meetings and resulted in a concrete proposal which needs to be further elaborated.

  To ensure a continuous flow of information (experiences, documents) between the CICU/Ss, it was also proposed to pay attention to the possibility of establishing an **electronic platform**.

  Finally, the present action also allowed the Customs Internet Crime Specialists in the EU to meet for the first time and to know their EU counterparts. Thanks to these contacts, some countries used the opportunity to **organise study visits** in order to learn more about the working methods and technical equipment of other Member States.

- *"To explore the ways of information exchange between Customs Internet Crime Units/Customs Internet Crime Specialists with a possible link to mutual assistance and cooperation channels"*
  Based on the example of the Cooperation Agreement concluded between FR and DE, the project group decided to explore the possibilities of such an enhanced exchange of information.
- *"To map existing anti-cybercrime initiatives within the EU or even a broader context with a possible impact on the work of Customs Internet Crime Units/Customs Internet Crime Specialists"*
  In order to meet this objective, the project group agreed to carry out a mapping exercise of the mentioned initiatives while inviting also guests from the Commission services, Europol and WCO to present their activities in the field of cybercrime.

The project group had in total four project group meetings. Between the meetings, the participants exchanged information also by e-mail and telephone.

4. Customs Internet Crime Units

As a follow-up to the first questionnaire distributed to all CCWP delegations, the CZ prepared and circulated among the project group members the already mentioned second survey which aimed at further exploring the organisation and technical aspects of the work of Customs Internet Crime Units/Specialists. The questionnaire was designed for those Member States which already have specialised team/specialists or are in an advanced stage of establishing such a specialised team. The total of 10 Member States replied (AT, BE, CZ, DE, FI, FR, HU, NL, PL, SE).

The outcome of the questionnaire (see below) then served as a basis of the discussions.

4.1. Location of Customs Internet Crime Units/Specialists

According to the survey, the Customs Internet Crime Units/Specialists make part either of Investigation (BE, DE, HU) and Intelligence/Analysis departments (CZ, PL, SE) or both if combined (AT, FI, FR). NL is in a specific position as the Internet Service Centre, where the Team Data is located, is a multiagency platform performing investigation- and intelligence-related tasks for different public bodies (Customs Administration, Fiscal Information and Investigation Service, etc).

All units/specialists have a nationwide scope.

4.2. Staff

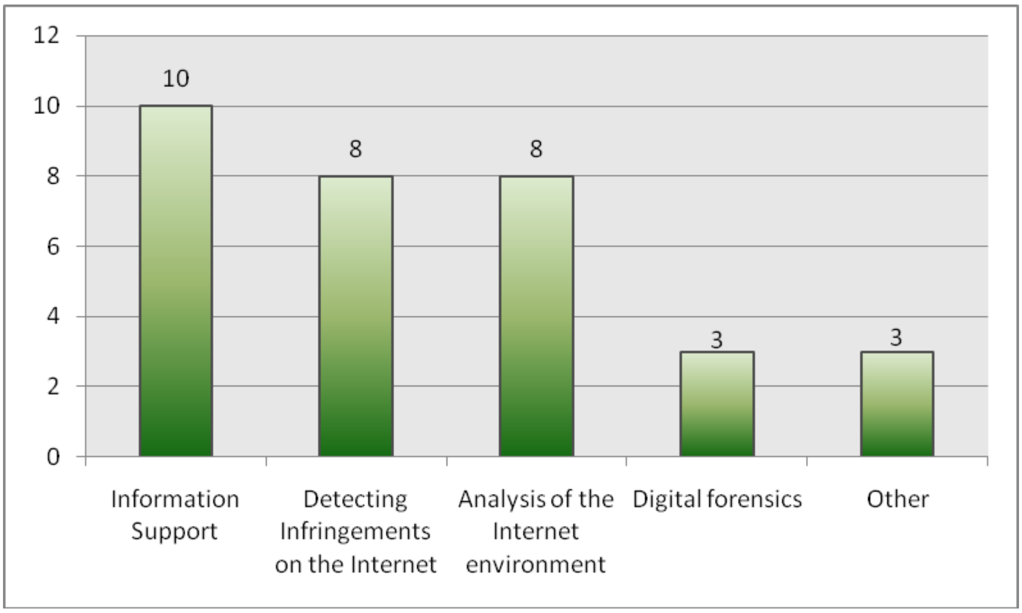
The table below shows the number of CICUs' staff as at 30 November 2012:

Austria	9
Belgium	4 (planned an increase by 2)
Czech Republic	4
Finland	2 (before the end of 2012)
France	10 + 3 customs officers-investigators
Germany	24
Hungary	6
The Netherlands	5
Poland	10
Sweden	2

The development of the staff number since the setting-up of a CICU/S is provided in the **Basic requirements for the establishment of a Customs Internet Unit in annex 1 of this report**.

4.3. Tasks

With a view to better understanding the extent of CICU/Ss' activities, it was first necessary to explore the basic tasks they are in charge of.



TASKS OF CICU/Ss

As shown in the graph above, the specialised teams are in all responding countries entrusted with the task of providing **information support** to other departments of Customs, for example, in the form of gathering evidence for investigation units (e.g. investigator makes a request to collect information about a particular person, find more information relating to a particular case, make a snapshot of certain websites, make covert communication, make a purchase of goods, trace financial flows, etc).

Detecting infringements on the Internet is a sort of proactive search in open sources based on key words. This activity is aimed at identifying concrete cases of customs related infringements which are processed by CICU/Ss and directly investigated by them or handed over to other competent bodies for further investigation/proceedings.

Similar type of activity is the **analysis of Internet environment** in relation to various sensitive areas (falling under the competence of Customs). Compared to the previous activity, the task of carrying out an analysis is much broader as the scope of such exercise may be rather complex. It aims to collect large quantities of data pertaining, for instance, to a sensitive commodity such as drug precursors which are further processed and analysed by means of various software tools. This exercise may then result in a global report on the situation in given area, in a concrete risk profile or case to be further investigated.

Computer forensics, which aims at recovering and analysing the digital evidence from e.g. seised computers, is a less common task among CICU/Ss. However, while at the beginning of this project only 2 Member States reported to perform this task, by its end the number increased by one and other two countries informed the project group about their intention to begin with computing forensics in the future as well. This increase only confirms the current development resulting from ever-growing computerisation of the society and its impact on the modus operandi of committing crime. Be it a communication tool or a crime facilitator, modern technology helps (unintentionally) the perpetrator to successfully interfere with the conventional law enforcement investigation techniques. Hence, it becomes almost an imperative also for Customs to collect digital and electronic data in order to have the chain of evidence complete.

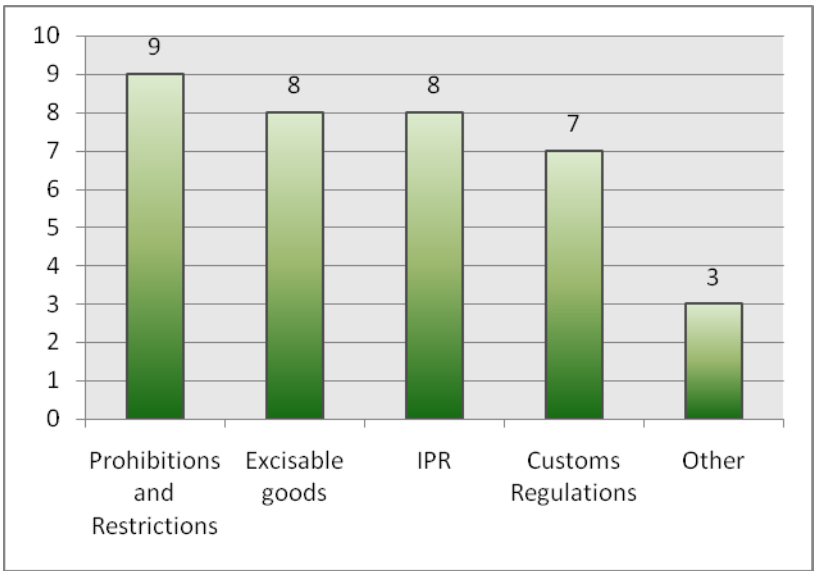
As this area of CICU/Ss work goes beyond the scope of the project group’s mandate, the working methods as well as the appropriate tools were not explored in a greater depth.

Other tasks further mentioned are those pertaining to the area of **trend watching**, **cooperation with other law enforcement authorities (on national and international level)**, **private and academic sector** or **training for other units within Customs**.

4.4. Areas and/or commodities covered

As outlined in the graph below, the areas and/or commodities covered by CICU/S are those of usual customs competence:

- prohibitions and restrictions (drugs, CITES, arms and ammunition, etc.),
- excisable goods,
- intellectual property rights,
- customs regulations (e.g. undervaluation).



AREAS AND COMMODITIES COVERED BY CICU/Ss

Other areas which were mentioned to be dealt with by some countries are illegal gambling and advertising of gambling on the Internet or illegal downloading.

4.5. Working methods and investigative techniques

To fulfil the above-described tasks, the CICU/Ss apply various working methods or investigative techniques while making use of available web/software tools and powers conferred upon to them by national legislation.

Considering the primary aim of the present action and its limited scope to customs related Internet crime, the project group focused discussions only on those working methods or investigative techniques which are linked to the tasks of information support, detection of infringements on the Internet and analysis of the Internet environment. In this context, the following methods were identified as the most frequent:

- collecting information in open sources and available databases;
- making requests for information to other competent authorities or private bodies;
- making contact with the suspect.

One of the basic legal prerequisites in this respect is the power to collect, process and provide information (incl. personal data) relevant for the prevention, detection, investigation and prosecution of violations of customs regulations from/to other competent units/authorities or third parties.

In fact, apart from collecting data in open sources which e.g. enables the identification of a perpetrator (based, for instance, on a telephone number or email address left somewhere on the web), the most frequent method to elaborate on the results of Internet monitoring or to find more information about a suspect person/suspicious goods is the requesting of information from the above-specified bodies, in particular internet service providers, operators of auction portals, ad servers, etc.

Making contact with the suspect with a view to finding out more details e.g. about the goods he/she offers, is also a very common method. However, the scope of such communication is greatly dependent on national regulations which may require also the intervention of national judicial authorities.

Other methods which were mentioned but resulted to be less common are the tracing of suspect financial flows and undercover operations. The former mentioned involves, among others, active cooperation with the financial and payment service providers like bank card providers, PayPal or Western Union. The extent of the second mentioned depends on the powers of customs authorities in criminal proceedings and it includes e.g. undercover purchases of goods sold on the Internet or the use of undercover agents.

Example:

Upon request of a competent authority, the CICU/S is tasked to find in open Internet sources some details about an email address. The investigation results in the detection of a number of life-style drugs' offers (Viagra, Cialis) where the email address in question is provided as the only contact detail. Entering in contact with the user of the above address, it is possible to establish the IP address[4] *and subsequently, by means of requesting the Internet Service Provider, also the identity of its user.*

Unless the customs authorities have sufficient powers in criminal proceedings to carry out an undercover purchase, the CICU may, as another step, ask for assistance the competent state drug control authority which have the possibility of making a control purchase of the offered drugs and analysing its content in order the check the genuineness of given product.

Initially, the project group concentrated on the working methods and, especially, to the work flow of Internet enquiries. Investigation is usually started on the basis of own initiative, information provided by other party (e.g. public) or a request made by other competent unit. The data are sought in both, open sources and available databases, or requested from the mentioned bodies. As soon as the Internet based investigation or analysis is finished, the CICU/S produces a final report which forwards to the applicant unit together with an electronic offline copy of information/websites collected from the Internet which are protected by a unique code. The code is generated as a control number which ensures that the gathered data are identical to those original ones and thus assures that no data has been changed throughout the investigation. This is particularly needed for evidence proceedings before the court.

In relation to the working methods, the project group also discussed how an Internet Crime expert/investigator should behave on the Internet in order to disguise his/her computer's belonging to a law enforcement authority. More information is available in annex of this report.

[4] Every computer connected to the Internet has an address, referred to as an Internet Protocol (IP) address. An IP address may be compared to an apartment/house address.

Single steps of Internet enquiries are often very similar. However, great differences are noted with regard to the use of software tools which in the end influence the whole working process. Discussions were thus moved to the area of web and software tools.

4.6. Software tools

There are several categories of the tools the specialised units/teams are in need of:

- web search engines, meta-search engines, special software search tools,
- web/software tools to trace IP-addresses or domain names,
- data snapshot tools (website copy tool),
- other,
- tools for forensic analysis.

A list of the above software tools has been produced and in the form of presentation circulated among the project group participants.

One of the key factors is to make the Internet enquiries as much automatic as possible and effective at the same time. Appropriate search engines play a crucial role in this respect. Following the results of the study, simple web search engines such as Google Search are very popular. The main advantage of these web tools is their free availability and the extent of websites indexed by them. Nevertheless, there are other search utilities (usually subject to a licence fee) which enable users to enter search criteria once and access several search engines simultaneously (e.g. Copernic Agent). Special search software is another type of tool which is, besides simple search, equipped with other functionalities such as analysis, graphic representation of relations between subjects of interest or monitoring of social networks (EMM OSINT Suite developed by the Joint Research Centre, Website Watcher, Xenon, Paterva Maltego, etc.).

Tools to trace IP addresses or domain names provide information concerning physical location of the computer which is connecting to the Internet or of a website, Internet Service Provider information as well as relevant domain information if applicable. These applications are free to use.

Another important category of tools are those enabling the download of websites from the Internet to a local computer (WinHTTrack, Offline Explorer, Snagit, etc.). The downloaded (or "mirrored") website can be then browsed offline and analysed by means of the mentioned analytical tools. It is necessary to have such tools in place also for the evidence proceedings before the court as the websites with illegal content may be closed down or redirected very quickly.

Tools falling under the “Other” category are usually specific and serve various purposes, for example, antifraud tools designed for the biggest auction portals (eBay, Allegro), computer network monitoring, packet analysis and decoding, instruments for searching in the deep web or picture recognizing tools.

The project group had the possibility to exchange views on and experience with a number of the above-mentioned tools. Their functionalities were mostly demonstrated on concrete cases which contributed also to a general knowledge of the working procedures in different Member States.

In the end, it was pointed out that some of the Member States (either customs or other competent authorities) put a lot of efforts and financial resources to develop new web/software tools which would fully match their needs. The functionalities of such tools could, however, be useful also to other Internet Crime Specialised Units within the EU. Considering the current financial crisis and its impact on public budgets, a certain level of coordination of the mentioned initiatives or even concrete engagement in the developing process of the EU bodies could be helpful to achieve synergies and to avoid unnecessary expenses or duplications. An example of such already existing initiative is the joint project of DG Home and DG Joint Research Centre which developed the EMM OSINT Suite. This tools is designed for law enforcement purposes to find, acquire and analyse data from the Internet based on information extraction technology. The software can be downloaded free of charge.

The same goes as for access to different databases or software applications which are subject to licence fees. The EU bodies could play a crucial role in this relation in order to achieve economies of scale.

5. Cooperation

This chapter is divided into two separate parts. The first part reflects the outcome of the questionnaire and provides an overview of the CICU/S partners within and outside the customs administration.

With regard to cooperation inside the customs administration, major partners are investigation/intelligence departments as well as tax and customs enforcement units (IPR, border control…). These units are either applicants for or addressees of information found on the Internet.

When discussing this topic, the Member States which already have a CICU/S emphasised the need to clearly identify relation between CICU/S and other departments of the customs administration, in particular as to the follow-up of CICU's Internet monitoring outcome. According to these Member States' experience, the CICU/Ss rely at the beginning almost exclusively on their own initiative and thus, it is important to lay down certain rules of procedure on how to further process results of Internet based investigations by other competent units. One of possible solutions which has already proven to be efficient is to appoint a certain number of customs investigators (the number always depends on the actual need) who would handle the cases initiated by CICU/Ss. Another option is that the CICU officers are in charge of the whole investigation (since its very beginning to the moment of handing it over to the competent, police or judicial, authorities). With the time passing, the proportion of own searches and investigations on request changes in favour of the latter mentioned.

Referring to the external dimension of the CICU's cooperation, this might be further subdivided according to the public or private status of the stakeholder. Following the results, all existing units collaborate with the police authorities (exchange of information and experiences) and tax administration. Along with the tasks assigned, the majority of CICU/S closely cooperates also with other control authorities, such as state institutes for drug control (e.g. control purchases of drugs on the Internet, analysis of the product), environmental inspections, etc. Other partners are the counterparts in abroad, especially in other EU countries or Europol. As for the private sector, a key role is played by internet service providers, email operators or right holders, followed by auction houses, ad servers and online payment providers.

5.1. Cooperation between Customs Internet Crime Units/Specialists within the EU

Flexible exchange of information between customs and/or other law enforcement authorities is one of the key elements of an effective fight against fraud and crime. Given the increasing speed of information exchanges on the Internet and the ease to operate a website that sells illegal goods, the project group explored the need and possibilities of an enhanced cooperation between CICU/S in this area. The discussions addressed three issues: direct exchange of information with its link to mutual assistance, the establishment of an electronic platform for sharing information and experiences between CICU/S and exchange of information throughout a joint action/measure.

- As far as **mutual assistance** is concerned, the project group took note of the standardised information exchange related mechanisms which has already been developed throughout the time within the EU and the role of central coordinating units (or similar units dealing with Council Regulation 515/97, if separate). The problems arising from the non-adherence to the standardised procedures and responsibilities stipulated by the respective legislation were outlined. The project group did not study in greater detail all possibilities of the mutual assistance legal tools such as Council Regulation 515/97 or the Naples II Convention, nor was it checked to what extent these instruments can be used by CICU. But it was stressed that any duplication of the above channels shall be avoided unless specific agreements are put in place. An example of such an arrangement is the Cooperation Agreement between FR CICU (called "Cyberdou@ne") and DE CICU (called "ZIRE") which has proven to be an efficient tool of cross-border cooperation in the area of preventing, detecting, investigating and prosecuting customs infringements committed via the Internet. This agreement, primarily based on the Naples II Convention and Council Regulation (EC) 515/97, aims at simplifying cooperation between the parties above, in particular, with regard to establishing identity of criminals or criminal groups who trade in commodities/areas covered by the Agreement on the Internet. To that end, the parties may request each other for information from the Internet service and email providers, administrators of forums, chats, messengers and social networks, banks and credit card companies or for further investigative measures such as identification of the owners of fixed and mobile phone numbers and background research of information on persons and companies in open source databases/registers.

- The idea of setting up an **electronic platform for sharing information and experiences** was raised already at the early stage of this action. However, before even starting the discussions, the project group explored the real need of such platform. One of the major concerns, in this context, related to the sufficient commitment of potential clients to actually use the platform once it is put in place. Throughout the discussions it was pointed out that the experts on customs related Internet crime have only limited possibilities to share experiences and considering the constantly evolving technologies which have impact on the work of CICU/S as well as the dynamic Internet environment which entails new forms of criminal modus operandi, the platform would enable those experts to preserve the network created within the framework of this action and deepen the cooperation between CICU/S.

  Discussions then focused particularly on the type of information which would be exchanged through the platform. With the exception of information falling under the scope of mutual assistance and cooperation which are to be exchanged via usual channels, the tool would be mostly used for sharing experiences regarding new tools, trends, risks or new modi operandi, i.e. it would primarily serve as a documents' repository and a secure communication channel for non-personal data.

  With a view to decide on an appropriate technical solution, the project group discussed the functionalities of available options, i.a. AFIS, CENComm, Europol's Platform for Experts (EPE) and in the end agreed on the latter mentioned. The choice was reasoned mainly by the scope of functionalities of EPE which include among others: library, media gallery, message forum, blog, user's directory, calendar, news, wiki and private communication (e-mail, chat). In this context, one Member State volunteered to explore the conditions for establishing a separate customs-dedicated cybercrime community and will inform the project group once more details are available.

- Another area of reinforced cooperation between CICU/Ss, the project group paid attention to, was the organisation of a "**joint action/measure**" (similar to joint customs operations) consisting in an Internet search exercise focused on a particular area of customs related responsibility (such as CITES, excisable goods). The joint action would pursue several goals, among others:
  - to share information and experiences between CICU/Ss;
  - to provide training to those countries in the process of setting up a specialised unit or planning the establish such team in the future;
  - to assess the added value of such exercise.

Based on the example of PANGEA I-V operations and the RILO WE's Project Mousetrap, the project group explored several concepts of the joint action/measure, in particular proactive and reactive approaches. Proactive approach stands for an independent Internet monitoring exercise targeted at detecting infringements falling under the customs competence and based on key words or risk profiles. Reactive approach means to conduct an Internet based investigations in relation to a concrete case of seizure of illegal goods (e.g. in the post). Both approaches would include an enhanced exchange of information between CICU/S, subsequent investigation into the detected infringements and a thorough evaluation after a certain period of time.

When discussing this topic, the problem of importation of small consignments resulting from Internet sales was pointed out. This type of consignments is less regulated compared to other forms of imports and may be thus exposed to a higher risk of fraud (trade in counterfeit goods, incl. medicines, illicit trafficking of drugs, CITES). In relation to the above-mentioned, BE representative informed about a national operation which aimed at countering trade in illegal goods via post and parcel consignments. Once the competent units made a seizure of illicit goods, the addressee was asked to provide information concerning i.a. value of the goods and websites of purchase. The data were collected in a database and used e.g. for further investigation purposes or throughout other large-scale operations (Pangea V, Skynet).

As a follow-up to the discussion held during the project group meetings, a draft business case of joint action/measure based on Internet investigations was discussed. The project group generally welcomed this proposal. Nevertheless, several problematic issues, such as sufficient legal grounds, were raised. Discussions on this topic should continue within the framework of any future follow-up CCWP actions or separately.

6. Other cybercrime initiatives

Tackling cybercrime and criminal misuse of the Internet is a priority not only for national law enforcement authorities but also for different Union's bodies (e.g. Europol, DG Taxud, Joint Research Centre, etc.) or international fora (e.g. WCO). With a view to gain a better knowledge of the initiatives already undertaken by the above entities, the project group decided to map the existing projects and invited the representatives of these agencies to give presentations on their activities.

6.1. Commission

i. DG Taxud and the *e*-Counterfeit group

When preparing the EU Customs Action Plan to Combat IPR Infringements for the period of 2009 - 2012, the Commission (DG Taxud) and the Member States underlined the need to respond to the growing problem posed by the trade in counterfeit goods via the Internet. The Action plan thus envisaged the creation of an ad hoc working group of experts and the organisation of seminars aimed at identifying and sharing best practices in this area. In October 2010 a Customs 2013 seminar was organised in Paris to exchange information on how customs tackle the phenomenon of counterfeit goods being sold via the Internet, to share experiences and to explore possible ways to improve the efficiency of customs controls on counterfeited goods in small consignments. The seminar produced conclusions that included a recommendation to each administration to provide for a customs structure responsible for the fight against counterfeiting via the Internet. As a follow-up to this seminar, the *e*-Counterfeit Project Group was established in October 2011. The *e*-Counterfeit Group should provide a forum for interested Member State experts to exchange best practices and to review the available instruments to combat e-counterfeiting, with a view to strengthening national customs capacity to curb such illegal activity.

At the early stage of Action 5.2, the CZ and DG Taxud representatives agreed on a coordination mechanism of activities undertaken within the framework of both projects in order to avoid any unnecessary duplication. The representative of DG Taxud also attended one of the project group meetings where the *e*-Counterfeit group initiative was presented.

ii. European Anti-Fraud Office (OLAF)

OLAF has a technical team assistance consisting of 8 forensic experts who provide following investigation related assistance:

- Seizure and forensic acquisition of possible electronic evidence (located e.g. on computers, servers, USB sticks, mobile phones, etc.)
- Scanning (conversion of paper documents/pictures into electronic format) and indexation of documents
- Preserve chain of evidence
- Digital Forensics (e.g. detection and restoration of deleted data, password cracking, data cleaning/narrowing, Indexation, Search function, Internet forensics)

The above services are provided to both, Commission bodies and national law enforcement authorities (including customs). In addition, OLAF organizes training sessions aimed at enhancing computer forensics related capabilities of OLAF’s and law enforcement investigators.

iii. Joint Research Centre

Joint Research Centre (JRC) is one of the Directorates-General of the European Commission. As the Commission’s in-house science service, its mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

JRC has developed the so called „Europe Media Monitor“ software that gathers reports from news portals world-wide, classifies the articles in 60 languages, analyses the news texts by extracting information from them, aggregates the information, issues alerts and produces intuitive visual presentations of the information found.

Based on this application, JRC in cooperation with DG Home developed a desktop tool - Open Source Intelligence Suite (EMM OSINT Suite) - to find, acquire and analyse data from the Internet.

By providing automatic means for downloading and processing it enables the users:

- to gather information from open available sources such as the Internet by removing the need to search manually through a wealthy set of data;
- to visualize the links between the subjects of interest.

The software is, in particular, designed for law enforcement authorities.

A representative of JRC attended one of the project group meetings and presented the current state-of-play regarding further development of the above tool. The participants were invited to take the advantage of this software as being free of charge for EU Member States' public organisations and to engage with the exchange of best practices within the OSINT Community which meets regularly at dedicated seminars in Ispra (Italy).

6.2. Europol

The increasing threat of cybercrime in the EU has led to a situation where cybercrime is now a priority on Europe's agenda and for Europol, too. This confirms not only the current EU Policy Cycle for 2011 - 2013 which, among others, includes a priority aimed at tackling cybercrime and criminal misuse of the Internet, but also the ongoing work on the European Cybercrime Centre's (EC3) institution.

Bearing in mind the above-mentioned, the project group invited Europol representatives to present their activities pertaining, in particular, to the area of gathering of information from open sources and to counter-cybercrime operations.

Open Sources Team is a part of Corporate Communications Unit. The main task of the Open Sources and Documentation team is to regularly inform Europol about important news and developments concerning organised crime, terrorism and law enforcement, including information and reports about Europol and other important EU and JHA issues. The services of Open Sources and Documentation include, *inter alia*, the monitoring, selection and presentation of daily news, publication of a weekly news digest, answering requests for specific information from Europol staff and Europol Liaison Officers, providing access to databases for other Europol's units and maintaining the library, including dealing with requests for books and journals.

Europol Open Sources has access to several commercial databases, which provide a wealth of up-to-date information and the latest news articles from all over the world (e.g. Factiva – provides licensed articles and the world's top media outlets, trade and business publications, Meltwater News - an online global media monitoring and analytical tools service, EMM - a software developed by the Commission (JRC) to enhance public access to information and in support of EU institutions and member state organisations, Dun & Bradstreet, etc.).

Europol's European Cybercrime Centre analyses and coordinates measures against a range of cybercriminal activities, such as intrusion/hacking, identity theft, intellectual property theft, hactivism, cyberterrorism, payment card fraud or child sexual exploitation.

Europol offers in this regard various services, among others, analytical or "on the spot" forensic support for investigations in the Member States, specialist research and development capability, strategic insight into cybercrime (e.g. iOCTA) or creation of joint investigation teams.

In response to the Commission's communication „Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre" of 28 March 2012, the Council endorsed the establishment of a European Cybercrime Centre (EC3) at Europol. The EC3 should be operational as of 1 January 2013 and will focus on:

- Cybercrimes committed by organised crime groups, particularly those generating large criminal profits such as online fraud;
- Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation;
- Cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the Union.

In addition to the analytical and operational support already provided by Europol, it will serve as the European cybercrime information focal point, developing digital forensic capabilities to support investigations in the EU and building capacity to combat cybercrime through training, awareness raising and delivering best practice on cybercrime. The EC3 should also become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

The Europol's representative also briefly introduced the European Cybercrime Training and Educational group (ECTEG). It is an official ad hoc sub group within Europol providing law enforcement cybercrime investigation training which was founded in 2007. The membership of ECTEG is comprised of EU member state law enforcement agencies and Europol, but involves also private industry and academia. Over the past years ECTEG has developed several accredited cybercrime investigation training modules to police officers throughout the EU on the following subjects, e.g. Introductory IT Forensics and Network Investigations, Linux as an Investigative Tool, Mobile Phone Forensics, Internet Investigations, Network Investigations, WiFi and VOIP investigations, Malware Analysis or Data mining and Databases. Customs are allowed to participate in the said training so long as they have the status of a "law enforcement" authority in their own country. More information can be found on: http://www.2centre.eu/.

With regard to the training, also CEPOL offers an online learning module on cybercrime. In the future, it is envisaged to develop, under the collaboration with Europol, a specific training aimed at ensuring that investigators working on illicit trafficking issues will have the opportunity to improve their digital investigation skills.

Further discussion regarding the current EU Policy Cycle and the cybercrime-related priority followed. It was observed that the focus and activities undertaken within the framework of the above project are especially those of police competence. It might be thus worthwhile to draw the EU stakeholders' attention also to the topics falling under the competence of customs cybercrime units.

6.3. WCO

Another important player on the field of customs related cybercrime is the World Customs Organisation. In 2001, the WCO Enforcement Committee gave rise to the Electronic Crime Experts Group entrusting it with the task to provide advice on aspects of electronic crime as it affects the WCO members. Current members of the group are: AU, AT, CA, DE, IL, NL, NZ, SE, UK and the US.

The activities of this expert's group focus on several areas, including:

- Defending the electronic infrastructure of WCO Members by monitoring existing or emerging electronic technologies which may provide specific benefits or advantages to WCO Members;
- Providing early warning of known or potential vulnerabilities to Members from the criminal exploitation of electronic systems;
- Countering threats to the core competencies of WCO Members through the development of best preventative practice, including specific proactive and reactive countermeasures;
- Keeping pace with technological change and inform WCO Members on new challenges;
- Recommendations for training and production of Best Practice documents.

The scope of ECEG's activities is broader compared to those envisaged under the present action as it covers also the aspects of customs computer network protection.

The ECEG has already produced a number of documents which are regularly updated and made available on the WCO Members' websites. To mention just some of those, for example: *Cargo Status Tracking* (2006), *Data mining in the Risk Management process* (2007), *Best practice guidance for online investigations* (2007), *IPR Infringements on the Internet, Basic Model for a centralised unit for fighting Cybercrime* (2009) or *Data Mining* (2010).

The project group had also the opportunity to become familiar with the recent RILO WE initiative "Programme Soteria" which aims to support the WCO Member countries in combating the illegal cross-border trade in goods (also via Internet) potentially harming the health and safety of their citizens, in particular medicines.

The delegates were invited to consider their possible participation in the ECEG. To this end, the project group was given the contact person details in the WCO Secretariat.

6.4. Council of Europe

To complete the picture of cybercrime initiatives, it is necessary to mention also the Council of Europe and the Budapest's Convention on Cybercrime, which entered into force in July 2004. This legal instrument is the only binding international treaty on this subject. It lays down guidelines for all governments wishing to develop legislation against cybercrime. The Council of Europe helps countries to ratify, accede and implement the treaty and its protocol through technical cooperation projects within the framework of which a number of valuable were produced (such as "*Specialised cybercrime units - Good practice study*", "*Cybercrime: current threats and trends*", "*Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines*", etc.). More information can be found on the Council's websites: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp).

7. Current and future challenges

During the discussions, several risks or challenges which can make the detection and investigation into customs infringemens or customs related Internet crime difficult, were brought to the attention of the project group. Some of them are mentioned below:

- **Quantity of information suggesting that a customs infringement may be committed**

As already mentioned, Internet is a wealthy source of information. And it is not difficult to find an indication about a possible fraudulent or criminal activity to be happening on the Internet. The real challenge is to decide how to handle, evaluate and further process such information considering the large quantity of them.

- **TOR**

TOR, which stands for „The Onion Router", is a software application which enables the online anonymity of Internet users to protect them and their activities from being monitored. TOR directs internet traffic through a worldwide network of servers to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis.

This type of secured communication has been in combination with several other counter-measures increasingly misused by criminals for e.g. drug trafficking. One of the best-known websites used to that end is called “Silk Road”, where you can buy or sell drugs like books or clothes. This webpage cannot be found by simply typing its name in a search engine. To access it, each user has a special software and a password. The communication is encrypted. The users pay for drugs with Bitcoins - virtual currency - commonly used for online payments, which can be converted into real money. The drugs are sent to the recipients by ordinary mail in various packages, e.g. for a hair dye, so that it is more difficult to detect the drug.

Similar method is also used to trade in weapons on the “Amory" website.

From the law enforcement point of view, it is one of the most difficult type of fraud/crime to detect.

- **Encryption**

Encryption works by using long algorithms to encode e.g. e-mails. Criminals can use encryption to make their real-time communication about their activities inaccessible to law enforcement. It can make it impossible for law enforcement agencies to obtain the evidence needed for a conviction or the intelligence vital to criminal investigations.

- **Cloud Computing**

With the progress of information and communication technology (ICT), it is already possible to store the data on the leased remote servers. This method is increasingly used by small and medium-sised companies. With this service, companies significantly reduce the cost of ICT and ICT personnel for maintenance. Another advantage of this service is that the data are always available (if the Internet connection is provided). However, this method of storage of data has also its dark side, especially while criminally misused. Cloud computing may represent a significant obstacle in the process of acquiring evidence by law enforcement authorities as it is very difficult to find and acquire the data (especially, if they are located in the countries with which there are no agreements on mutual legal assistance concluded) or to even know about their existence.

- **Setting-up of e-mail accounts or registering web sites with Internet Service/Domain Providers based in countries with which there are no agreements on mutual legal assistance**

If an e-mail account of interest or a web site is set up in a country with which there are no relevant agreements on mutual legal assistance, it is very difficult or even impossible to carry out appropriate investigation. As a result, an ordinary request relating to the account's owner may become an unsolvable problem.

- **Deep web**

Deep Web is that part of the World Wide Web (WWW) which is not reported by normal search engines. In fact, it means that traditional search engines such as Google or Yahoo cannot see or retrieve information from it. There are several reasons for why the Deep Web content cannot be found (e.g. the content is private and is protected by a login or a password; the content is not linked to any other web page; the content is dynamic, i.e. it is generated based on a specific request for data stored in a database). It is estimated that up to 96% of the WWW content belongs to the category of "deep web." Thus, it represents a vast anonymous network hidden from normal users allowing people to communicate without detection. Deep web is hardly traceable and even less analyzable.

In addition to the above mentioned and referring to the software equipment, search in the deep web and picture or video recognizing tools are one of the challenging areas for the future. People sometimes use social networks to offer goods (including illicit ones) within a closed/private community or use only pictures to sell the goods which make it impossible for the law enforcement authorities to apply tools originally designed for the text searching. Thus, it would be necessary to develop new or further improve the already existing search tools to find and analyse information from the deep web or to find information on the surface Internet with no written words (i.e. for picture or video recognition purposes).

8. Conclusions and Recommendations

The project group reached and agreed on the following conclusions and recommendations:

i. **Creation of units specialised in the Internet based investigations:** The increasing reliance of the society on the information and communication technology, the technological progress and related evolution of the criminal modus operandi underline the need to bear in mind the role of Internet also upon prevention, detection and investigation of customs infringements. *Recommendation*: In order to keep pace with the ICT developments, it is recommended that the Member States consider the possibility of setting-up **a structure** (unit, small team of specialists) within the Customs which would deal with the Internet monitoring or investigations and support the work of the customs authorities in general.

ii. **Exchange of information:** Exchange of information between the law enforcement authorities has become an indispensable part of an effective fight against fraud and/or crime. The experience of FR and DE has proven that the agreement on a reinforced exchange of information between CICU/Ss could be an efficient tool of cross-border cooperation in the area of preventing, detecting, investigating and prosecuting customs infringements committed via the Internet. *Recommendation:* The Member States with a team of Customs Internet Crime Experts are invited to assess the need and consider the possibility of concluding cooperation agreements with their EU partners, while taking into account the relation of such an arrangement to conventional mutual assistance channels.

iii. **Electronic platform for sharing experiences:** Internet is a very dynamic environment which, alongside a large number of advantages, may entail new forms of committing fraud or crime. In order to remain up-to-date concerning the latest developments in modern technology and criminal behaviour, it would be beneficial to the work of customs Internet crime experts to have a possibility to share knowledge, best practices and experiences on a permanent basis. *Recommendation:* With a view to preserving and deepening the network of customs Internet crime specialists currently created within the framework of this action, it is recommended to explore, in cooperation with Europol, the possibility of creating a dedicated customs area within cybercrime community of the Europol Platform for Experts.

iv. **Risk analysis and threat assessments:** Internet is an important source of information which can enrich the risk analysis or threat assessments produced for the purpose of customs control activities or investigations. Web-mining or text mining is a true challenge in this respect and should be explored in a greater depth.
Recommendation: The Member States are invited to examine the possibility of creating risk profiles based on information retrieved from the Internet by, inter alia, the use of new data-mining techniques applicable to the Web content as well as to explore possibilities for finding synergies in this area with risk analysis completed under the Commission competences for risk management purposes.

v. **Computer forensics:** Modus operandi of fraud and/or crime changes along with the growing computerisation of the society. As a result, the classical physical form of evidence is being more and more replaced by proofs saved on various electronic devices or computers. Collection of digital and electronic data is thus becoming an imperative also for Customs to complete the chain of evidence.
Recommendation: Bearing in mind the increasing importance of this type of evidence as well as the ongoing work on paperless environment for customs and trade, the Member States, in particular those vested with sufficient powers in criminal proceedings, are invited to consider possible expanding of their activities to the said sphere of expertise. The CCWP is also invited to pay attention to this topic.

vi. **Development and sharing of software tools/licences:** Development of new web/software tools often represents a considerable financial burden to the Member States. Joining efforts on the EU level may not only save time and money but it can also bring synergies, especially in the field of knowledge and expertise. The same goes as for access to different databases or software applications which are subject to licence fees. The crucial role could be played in this respect by the competent EU bodies, in particular the Commission and Europol.
Recommendation: The Commission and Europol are invited to examine the needs of the Member States in the area of software/application equipment designed for Internet search and its analysis and to introduce a mechanism which would enable to join efforts on the EU level when developing or accessing a web/software tool, if appropriate.

vii. **Training:** Taking into account the different levels of development of CICU/Ss across the EU and with a view to deepening the knowledge of already advanced CICU/Ss, it is essential to ensure an appropriate training for the respective customs Internet crime officers. Currently, there are only limited possibilities of how to acquire a basic knowledge. One of those is to organise study visits at the already existing CICU/Ss.
Recommendation: Depending on the outcome of the ongoing revision of the CEPOL's mandate and the implementation of the European Training Scheme, the Member States are invited to monitor and take active participation in the (e-)learning programmes addressing the cybercrime topics and digital investigation-related skills. It is further recommended to consider developing a special training for customs Internet crime experts within the framework of any future follow-up to this Action.

viii. **Joint action/measure:** Taking into account the growing problem posed by sales of illegal goods via the Internet and their imports on the territory of the EU, it is important that Customs adopt appropriate measures to counter this threat. Joint action/measure based on/supported by Internet investigations is a new approach which may provide the customs authorities with an insight into this global phenomenon.
Recommendation: The CCWP/the Member States and the Commission are invited to continue discussions on the possibility of organising a joint action/measure based on/supported by Internet investigations as well as to consider the involvement of CICU/Ss in the preparation and execution of every joint customs operation, where appropriate.

ix. **Mapping other initiatives:** Given its transnational character, the tackling of cybercrime and criminal or fraudulent misuse of the Internet has become a priority to a wide range of EU agencies and international organisations. The initiatives undertaken under the auspices of the bodies described in this report might be useful also to the Customs.
Recommendation: The Member States as well as the CCWP should follow and remain up-to-date concerning the activities pursued by the said bodies.

x. **Follow-up to the present Action:** As already mentioned, the Internet and ICT are one of the most dynamic areas of development which, on one hand, make our daily lives easier, and on the other, facilitate the commission of fraud and crime. In order to keep pace with the technology and to effectively respond to the described threats, it is important to further develop the cooperation between CICU/Ss and explore in a greater depth other customs Internet crime related issues which were not yet addressed by the project group for Action 5.2, in particular:

- cooperation between customs administrations and private sector in the area of Internet sales and online services,
- cooperation between customs administrations and other law enforcement authorities in the area of cybercrime,
- developing a special training for customs Internet crime experts,
- continuing discussions on the joint customs operation based on/supported by Internet investigations,
- examining legal aspects relating to the work of customs Internet Crime units,
- other.

Recommendation: It is recommended to ensure a follow-up to Action 5.2 within the framework of one of the next CCWP action plans focusing on i.a. the listed issues.