COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 5 October 2016
cdpc/docs 2016/cdpc-bu (2016) 6

CDPC-BU (2016) 6

EUROPEAN COMMITTEE ON CRIME PROBLEMS

(CDPC)

Bureau
(CDPC-BU)

REPORT ON LINKS/GAPS BETWEEN THE MEDICRIME AND CYBERCRIME CONVENTIONS

Outline document

Contents

1. Introduction

1.1 Online MEDICRIME: a threat identified by the Council of Europe

1.1.1. In the framework of the Committee of Ministers

The Committee of Ministers has raised the impact of ICTs on the selling of medical products on several occasions, although only in broad terms.

- **Resolution ResAP(2001)2 of the Committee of Ministers** to member States concerning the pharmacist's role in the framework of health security

  → *"problems posed by distance sales of medicinal products and the development of this practice through the Internet"*

- **Recommendation Rec(2004)17 of the Committee of Ministers** to member States on the impact of information technologies on health care – the patient and Internet

  → "*the Internet has created a global health information community which transcends national borders and raises issues for states that go beyond their jurisdiction for Internet matters, making them profoundly difficult to regulate*".

- **Resolution ResAP(2007)2 of the Committee of Ministers** to member States on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine

  → *"mail-order trade in medicines is by and large marketed via the Internet, which is uncontrollable and used as a platform for many illegal offers of medicines […]".*

1.1.2. In the 'Internet Governance' strategy (2016-2019)

→ *"The online safety and security of Internet users is a shared responsibility. This requires action to combat […] the sale of counterfeit medicines and drugs". Among other key priorities, the CoE has decided to consider "ways to prevent the illegal sale of drugs and counterfeit medicines as well as illicit trafficking in drugs online, including the promotion of the [MEDICRIME Convention]" (§10.e).*

Activities foreseen under the Strategy include the following:

- Pompidou Group monitoring of sale of illicit drugs on the DarkNet ;
- Promoting implementation of the MEDICRIME Convention as a tool to combat the supply and offering of and the counterfeiting of medical products committed by using the Internet ;
- **Report on the links between the MEDICRIME Convention and Cybercrime Convention.** [emphasis added]

1.2 Objective and scope of the report

- Complementary action of the MEDICRIME and Cybercrime Conventions long recognised, as early as at the drafting stage of the MEDICRIME Convention

- **Objective** of the report: Identifying the possible links and gaps, from a criminal law perspective (substantial and procedural aspects), between Convention CETS No.211 and CETS No.185.

- **Scope**: Cf. Definitions of the aforementioned instruments.
  - Offences covered pursuant to the MEDICRIME Convention:
    Manufacturing of counterfeits; Supplying, offering to supply, and trafficking in counterfeits; Falsification of documents; Similar crimes involving threats to public health.
  - Offences covered pursuant to the Cybercrime Convention:

    Offences against the confidentiality, integrity and availability of computer data and systems; Computer-related offences; Content-related offences; Offences related to infringements of copyright and related rights.
  - Beyond the scope of the report: (among other) Issues relating to the protection of medical data in the digital era

1.3 Structure of the analysis

Potential interactions between the MEDICRIME and Cybercrime Conventions are examined through two focuses:

a) **Internet as a platform for the advertising and the selling of counterfeited medical products**
E.g. 1 : Spam campaigns for counterfeited Viagra pills.
E.g. 2: Illegal e-Pharmacies

b) **Fake e-pharmacies as 'baits' to commit cybercrime offences**
Esp. to steal users data and infect computer systems

Both issues are examined from both a criminological perspective (design and intensity of the criminal threat) and a legal perspective (criminalisation and procedural aspects).

2. Internet as a platform for the advertising and the selling of counterfeited medical products

2.1 The criminal threat

Key elements:

Advertising counterfeited medical products

- The Internet can be used in various ways to advertise counterfeited medical products and devices
  → E-pharmacies (be they 'genuine' or fake); Marketplaces (e.g. Alibaba); DarkNets on the Deep Web; Social networks (Facebook, Twitter, Instagram,…); Forums; E-mailing, spamming and web manipulation

- "Spamming" esp. plays a crucial role. It provides an easy, cheap, and anonymous channel for the trafficking of counterfeit medical products and devices

- DarkNets on the Deep Web are increasingly used as platforms of advertisement, raising important challenges for LEAs
    - E.g. Silk Road 2.0 (shut down in 2014), with prescription medicines as bestsellers

Selling of counterfeited medical products

- Internet has long acted as a market-place for the selling of counterfeited medical products and similar offences, but recent studies show the market continues to grow significantly
    - E.g. IRACM Research Institute reported a trade increase of 90% in 8 years

- Current trends: Increasing presence of *vital* medical products and devices on the market; diversification of medical products available;

- Perspectives: Continued expansion of the trade, thanks to several concordant factors (regulatory; economic; criminological; technological)

2.2 Substantive criminal law under Conventions 185 and 211

Under the MEDICRIME Convention

Several criminal law provisions permit to address quite comprehensively the advertising and selling of counterfeited medical products and related offences.

- Article 6 of the MEDICRIME Convention on supplying, offering to supply, and trafficking in counterfeits seems to apply to many forms of the online advertising and selling of counterfeit medical products and devices
  E.g. Online pharmacies websites; spamming campaigns; trafficking on DarkNets

- Article 7 on the falsification of documents is also clearly relevant, given the broad meaning given to the term 'document' in the Convention
  E.g. illegal e-Pharmacies using falsified documents to abuse patients

- Article 8, which aims at targeting offences involving *non*-counterfeited medical products, but considered to pose an equally serious threat to public health, also has clear relevance.
  A provision of prime important given that criminals operating online pharmacy networks are predominantly not involved in the production of counterfeit or illicit medicines themselves

- Article 13 on aggravating circumstances explicitly addresses activities "having resort to means of large scale distribution, such as information systems, including the Internet"

Under the Convention on Cybercrime

Prima facie, the **advertising** of counterfeited medical products and devices does not seem as such to fall under any of the categories of offences criminalised by the Budapest Convention. Yet, specific issues may be mentioned:

- Spamming: Spamming campaigns undertaken for the purpose of trafficking counterfeits may cause nuisance to its recipient, in particular when such messages are sent in very large quantities or with a high frequency. As such, they may amount to "system interference" under Article 5; yet, the Convention leaves it to the Parties to determine the threshold of nuisance requiring sanctions

  → Remark: Examine whether the scale now reached by spamming for the marketing of counterfeited medical products is such as to fall under this provision, or as to require additional criminalisation measures

- Web manipulation (ie. the involvement of affiliate and sub-affiliate networks in order to infect huge numbers of websites so that they redirect unsuspecting customers to illegal websites, here rogue e-Pharmacies) is often considered as much more efficient than spam e-mails.
  Depending on the technical methods used, web manipulation can amount to various offences against the confidentiality, integrity and availability of computer data and systems, esp. illegal access (art. 2), illegal interception (art. 3), data interference (art. 4) and system interference (art. 5), as well as certain computer-related offences.

Needless to say, the **supplying and trafficking** of counterfeited medical products and devices do not amount as such to offences against the confidentiality, integrity and availability of computer data and systems. However, computer-related offences may be committed *in the course* of such supply or trafficking – esp. computer-related forgery (article 7), given the frequent use of falsified documents for the selling of counterfeit medical products.

2.3 Procedural measures under Conventions 185 and 211

Convention 211

Measures related to procedural law as well as co-operation and information exchange are regulated in Chapters III and IV, international cooperation is regulated in Chapter VII of the Convention 211. In terms of both procedural powers and international cooperation the Convention 211 is very flexible and doesn't provide concrete measures for the implementation. It leaves lots of room for the Parties to decide how to ensure the effective implementation of the Convention. The same applies for the international cooperation. The Convention refers to already existing applicable instruments, but also can be used itself as legal basis for international cooperation.

According to the Article 15 Parties need to take necessary legislative and other measures to ensure that investigations or prosecution of offences established in

accordance with this Convention should not be subordinate to a complaint and that the proceedings may continue even if the complaint is withdrawn. Article 16(1) requires Parties to establish specialised units to combat counterfeiting of medical products and similar crimes involving threats to public health. It also obliges Parties to provide necessary training for the personnel and adequate resources. Article 16(2) requires that Parties take necessary legislative and other measures to ensure effective criminal investigation and prosecution. Measures should also include possibilitities to carry out financial investigations and to use covert operations, controlled delivery and other special investigative techniques.
Article 17 provides for the measures related to co-operation and information exchange between relevant authorities for the purpose of preventing and combating counterfeiting of medical products. Co-operation and information exchange must also include the private sector. Mechanisms should be established not only to receive and collect information from, but also to make it available to the private sector and civil society to prevent and combat crime.

For the purpose of international cooperation to investigate and prosecute crime Article 21 provides for the reference to relevant applicable international and regional instruments and arrangements. International cooperation measures include seizure and confiscation, as well as extradition and mutual legal assistance in criminal matters. According to the Article 21(3) the Convention 211 can also be considered as legal basis for international cooperation if other treaties are not applicable.

Article 22 requires Parties to designate a point of contact responsible for international cooperation and information exchange, in particular for transmitting and receiving requests.

Convention 185

Although the scope of the Convention in terms of substantive law differs from the Convention 211, it can also be used to combat counterfeiting of medical products when it comes to procedural powers and measures. According to Article 14 which provides for the scope of procedural provisions, all the powers and procedures can be used with regard to any criminal offence that has been committed by the means of the computer system and to collect electronic evidence related to any crime. Similar logic is followed by Article 23 on general principles relating to international co-operation. Pursuant to Article 23 international cooperation measures provided by the Convention can be used for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Convention 185 provides for the following domestic and international procedural measures:

Chapter II – Measures to be taken at the national level
Article 14 – Scope of procedural provisions
Article 15 – Conditions and safeguards
Article 16 – Expedited preservation of stored computer data
Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 – Production order
Article 19 – Search and seizure of stored computer data
Article 20 – Real-time collection of traffic data
Article 21 – Interception of content data

Chapter III – International co-operation
Article 23 – General principles relating to international co-operation
Article 24 – Extradition
Article 25 – General principles relating to mutual assistance
Article 26 – Spontaneous information
Article 27 –Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
Article 28 – Confidentiality and limitation on use
Article 29 – Expedited preservation of stored computer data
Article 30 – Expedited disclosure of preserved traffic data
Article 31 – Mutual assistance regarding accessing of stored computer data
Article 32 –Trans-border access to stored computer data with consent or where publicly available
Article 33 – Mutual assistance regarding the real-time collection of traffic data
Article 34 – Mutual assistance regarding the interception of content data
Article 35 – 24/7 Network

Some criminal offences provided by the Convention 211 can be committed by the means of computer system, but electronic evidence could be part of the criminal investigation of any crime. Therefore the procedural powers to investigate and gather electronic evidence as they are regulated in the Convention 185 are also applicable to the criminal offences provided by the Convention 211. In that way two instruments complement each other and by implementing both of them Parties have all the necessary powers to fight crime effectively.

→ Reference to section 3, or developments on procedural measures
→ Best practices of MHRA

3. Fake e-pharmacies as 'baits' to commit cybercrime offences

3.1 The criminal threat

→ Fake e-pharmacies as baits to steal users data and infect computer systems

- The main purpose of fake e-pharmacies websites is to create a false illusion to the customer about the authenticity of the website and by deception convince the customer to enter his/her personal data, including name, postal address, e-mail address, online banking credentials, credit card information etc
- Personal data, including credit card information may be used to commit identity theft or computer-related fraud

- Personal data including e-mail address may be used to spoof e-mails and send targeted spear phishing e-mails
- Fake e-pharmacies websites may contain malware and infect the computers used to access the website
- To advertise fake e-pharmacies websites spam is often used

- Fake e-Pharmacies must be distinguished from rogue e-Pharmacies. Whereas rogue e-Pharmacies are websites that genuinely – but unlawfully – market medical products and devices, fake e-Pharmacies only *pretend* to provide such service in order to attract victims on a website, where they will:
    - voluntarily provide personal data (ID or credit card details);
    - click on links or download files, hence infecting their computer with virus and similar devices (e.g. Trojan files) (again, with the purpose of obtaining ID or credit card details).

- Fake e-Pharmacies websites are sometimes promoted through spam campaigns using various strategies
  (e.g. keywords related to recent health crisis)

- According to recent surveys, the number of legal, licenced e-Pharmacies online amounts to 0,7% of the web offer, in terms of number of sites, the rest of the offer, equally divided between fake and rogue websites

3.2 Substantive criminal law under Conventions 185 and 211

Under the MEDICRIME Convention

- The MEDICRIME Convention does not appear as a leading instrument to be involved in the fight against fake e-Pharmacies. However, this criminal activity, by its intensity, diverts customers from access to genuine medical products, thus undermining the main objectives of the Convention

- Arguably, the setting-up of a fake e-Pharmacy may involve the commission of certain criminal offences set out in **article 6,** inasmuch as the act amounts to offering to supply counterfeits. Other criminal offences might not be relevant.

Under the Cybercrime Convention

- The setting-up and functioning of fake e-Pharmacies appear to involve several offences set out by the Budapest Convention, the qualification of which depends on the scheme used, the type of viral tools, etc.

- Other cybercrime offences may also be committed in the *preparation* of, or as *result* of, the operation of a fake e-Pharmacy.

3.3 Procedural measures under Conventions 185 and 211

(Cf. 2.3, or drafted here)

4. Conclusions/Recommendations

Substantive law

- Both instruments cover, in various aspects, the advertising of counterfeited medical products, while the selling of such products is mainly dealt with by the MEDICRIME Convention;

- Further study should be undertaken to examine to which extent spamming is criminalised as such by the treaties;

Recommendations:

- Examine whether the scale now reached by spamming for the marketing of counterfeited medical products is such as to require additional criminalisation measures

- Consider the need to criminalise specifically in the MEDICRIME Convention the selling or distribution (e.g. on DarkNets) of falsified documents online relating to medical products - to be distinguished from the current criminalisation of the falsification itself under article 7

Procedural measures

- Although the Convention 211 doesn't provide for detailed regulation on procedural powers and measures and international cooperation it refers to national laws and other applicable international instruments.
- The procedural powers and measures and international cooperation measures in Convention 185 can be used with regard to electronic evidence that could relate to any crime.
- Conventions 185 and 211 can be considered to complement each other. If both have been implemented by the Parties that can ensure effective investigation and prosecution.

Capacity building

- Training for LEA on various issues of importance for the fight against the selling of counterfeited medical products (e.g. criminal investigations methods on DarkNets)

Inter-agency cooperation

- [Cooperation CPDC/T-CY] Considering activities on the fight against Web manipulation

- [Cooperation CDPC/EDQM]: Offering a platform to member States' authorities for exchange of information on good practices in approaches to tackle illegal Internet pharmacies supplying or offering to supply counterfeit/falsified medicines

- Organising joint activities CDPC/Pompidou Group on the sale of illicit drugs on the DarkNet