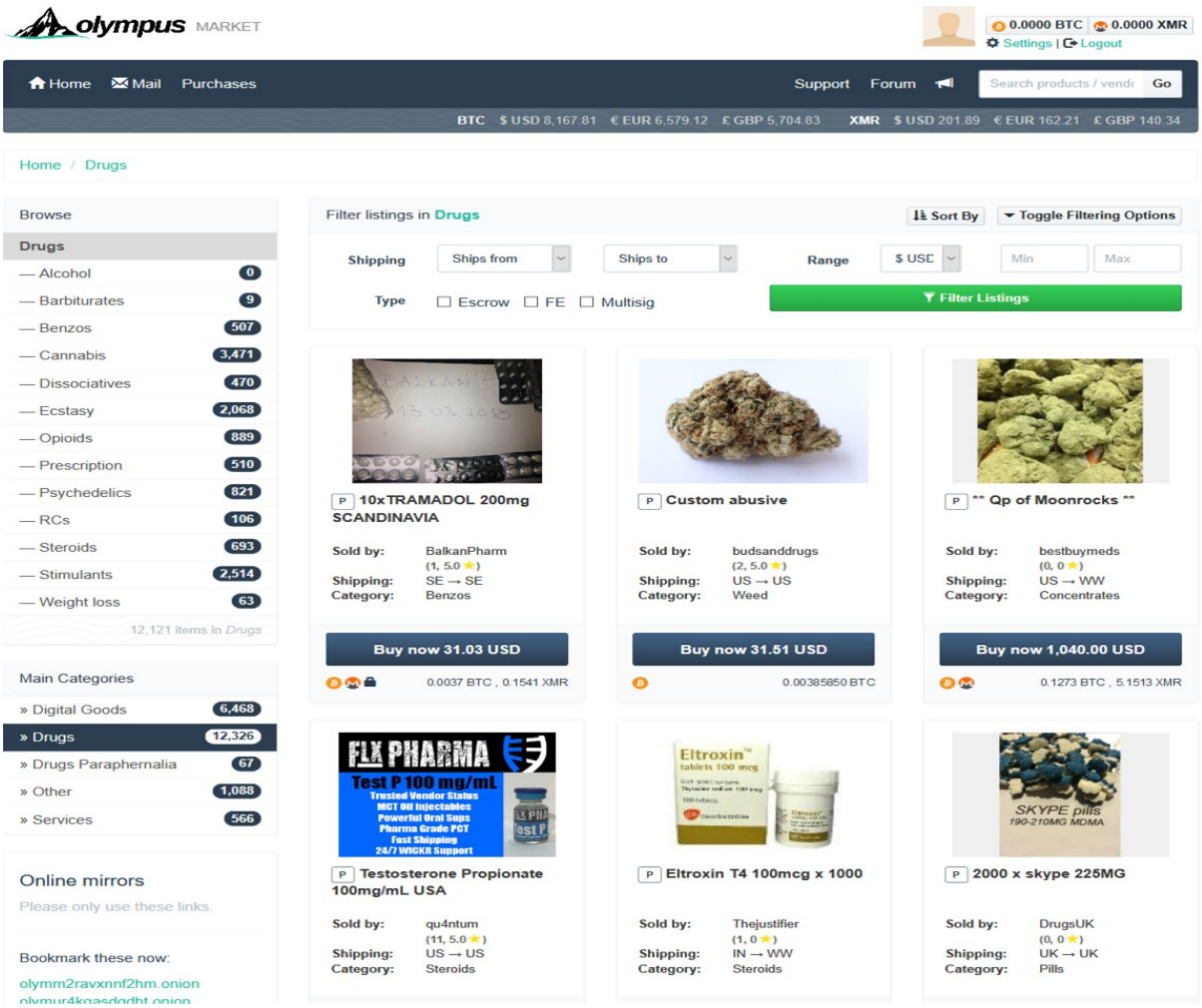
Online Trade in Illicit Goods and Services

Executive Summary

> 'In just a few clicks, buyers can purchase almost any type of drug on the darknet whether synthetic drugs, cannabis, cocaine, heroin or a range of new psychoactive substances, including highly potent fentanils.'
>
> Alexis Goosdeel, Director of EMCDDA (28 Nov 2017)



This e-learning module is concerned with the different kinds of illicit trade on the internet, and especially the part of the internet known as the darknet. Criminals operate online marketplaces that sell a wide range of illicit products and services, such as drugs, firearms, counterfeit goods, child pornography, counterfeit currencies, financial data, fake documents, ransomware and hacking services.

Illicit markets have existed for countless years but due to the technology revolution over the past two decades, online marketplaces have become increasingly significant.

The development of free tools and cryptocurrencies has created a user-friendly environment and opened the doors of the online marketplaces to people that are not necessarily technology

specialists. Moreover, many of these tools, such as Tor Browser and PGP encryption, are 'anonymising' – concealing the users' identities and information about the transactions.

This module aims to raise awareness on online trade in illicit goods and services. It is targeted at those police and law enforcement officers, border guards, customs officers and judiciary staff who are not used to dealing with internet crimes.

This module is one of three closely related and partly overlapping CEPOL e-learning modules, the other two being:

- **Cybercrime**: which covers 'cyber-dependent' crimes – crimes that require electronic systems to be involved, such as attacks against information systems, denial of service attacks and hacking;
- **Darknet**: which covers all criminality taking place on the darknet.

The module consists of an introduction, nine topic chapters and a glossary of terms and abbreviations related to illicit online trade. In the My Progress section, users can check their levels of understanding of each of the topics by considering a selection of true/false statements.

The topic chapters are:

1. **Introduction**

2. **Online Products and Services:** The first of the two chapters describing the online environment, this one providing an overview of all the types of products and services available online.

3. **Online Criminal Actors:** The second of the two chapters on the online environment, this one providing a typology of traffickers and organised groups involved in illicit activities.

4. **Anti-Money Laundering:** This chapter focuses on the processes used to launder money derived from illicit online activities.

5. **Open Source Intelligence (OSINT):** This chapter describes good practices to target and identify criminals and their networks using open source research.

6. **Challenges to Investigation:** This chapter covers obstacles and difficulties for investigators working in the virtual world. In particular, it focuses on darknet platforms which offer different means to protect anonymity.

7. **Technologies Enabling Crime:** This chapter describes technologies and techniques that enable online criminality, whether this is by design or not. It also shows how these technologies can be used to anonymously access or offer illegal services online.

8. **Cooperation:** This chapter covers cooperation between the different EU Member States and also with EU agencies. One section is dedicated to cooperation with the private sector.

9. **Online Prevention and Training:** This chapter covers the most common threats to online security. It also deals with spreading good practices to a public audience in order to avoid personal data leakages. In addition, this chapter introduces the basics for the training of law enforcement officers who are to be proactive online.

10. **Online Investigations:** This chapter discusses the investigation of an online crime. It includes the composition of the investigative team, the investigative resources required and how cases are referred for investigation.