UNODC
United Nations Office on Drugs and Crime

SHERLOC
SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME

NEWSLETTER

ISSUE NO. 25 | JUNE 2023

The UNODC SHERLOC team is pleased to share with you Issue No. 25 of our newsletter regarding our recent efforts to prevent and counter cybercrime.

EDITORIAL

CYBERCRIME

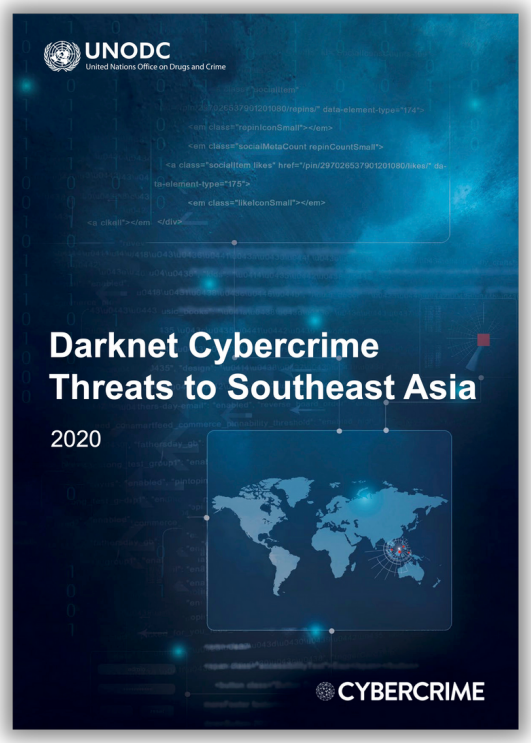
The present issue focuses on the topic of cybercrime and the work of UNODC to counter this global phenomenon. This issue provides an overview of the key publications and related tools developed by UNODC, and presents a series of teaching modules focusing on different aspects of cybercrime available on SHERLOC's Education for Universities (Edu4U) Database.

Furthermore, the current issue provides information about the Summer School on Transnational Organised Crime organized in Vienna by the ECPR SGOC in cooperation with the Global Programme on Implementing the Organized Crime Convention of UNODC, during which cybercrime was discussed with the students. A case study relating to cyber organized crime is also included.

In this issue

CYBERCRIME PUBLICATIONS AND TOOLS

DARKNET THREATS TO SOUTHEAST ASIA



In 2020, the Global Programme on Cybercrime researched on Clearnet and Darknet threats and published the UNODC Report on Darknet Threats to Southeast Asia. The report assessed the Dark web from the viewpoint of users, criminals and law enforcement with a particular focus on cybercrime targeting countries in Southeast Asia.

This report, which can now be found in SHERLOC's Bibliography Database, explored the main *modus operandi* of organized criminal groups and highlighted features like escrow payment systems and reputation metrics, which had increased. The extended use of cryptocurrencies in the region was also confirmed, particularly with the objective to move illicit money to jurisdictions away from victims and to hide the identity of criminals by means of crypto-mixers, tumblers, or laundry services break. All of these make the tracking of illicit flows of money and attribution of criminal activity to individuals more difficult than usual.

The report is still relevant today, where Bitcoin remains the main cryptocurrency used on the Darknet. Bitcoin and other public coins are generally mixed with other private coins such as Monero, Litecoin and Bitcoin Cash, which are perceived as offering greater anonymity to cybercriminals.

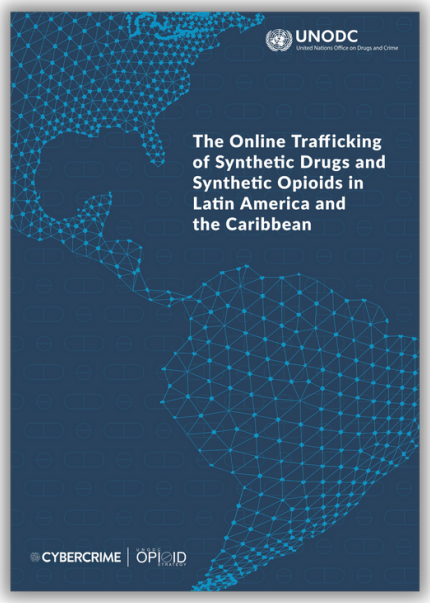
All over the world, national specialized capabilities on Darknet investigations and cryptocurrency-related crimes are limited and need to be strengthened to respond to current threats. UNODC supports States in developing operational knowledge and standards related to Darknet investigations, cryptocurrency tracing and anonymizing technologies, among others. In Southeast Asia, the Global Programme on Cybercrime has established a Cryptocurrencies Working Group among the public and private sectors to exchange ideas and solutions for an effective regulation and legislation of cryptocurrencies and digital financial platforms. The tools available on SHERLOC have been key to starting a conversation on innovative solutions and the implementation of comparative best practices.

Bibliography database
SHERLOC.UNODC.ORG

THE DARKNET REPORT IS AVAILABLE ON SHERLOC'S BIBLIOGRAPHY DATABASE IN FOUR LANGUAGES: ENGLISH, BAHASA INDONESIA, THAI AND VIETNAMESE.

CYBERCRIME PUBLICATIONS AND TOOLS

ONLINE TRAFFICKING OF SYNTHETIC DRUGS AND SYNTHETIC OPIOIDS



The borderless nature of cyberspace enables criminals and organized criminal groups to operate online in a more flexible and covert manner. The pseudo-anonymity offered by online platforms that conceal the identity of vendors and customers together with the simplicity of online communications and transactions, and the low costs associated with establishing and carrying out operations, are attractive to drug traffickers.

The field of cyber-enabled crimes is growing day by day. What it used to be a field operating mainly on the Darknet has now moved to the Clearnet and is changing the dynamics of international drug trafficking.

The UNODC Report on Online Trafficking of Synthetic Drugs and Synthetic Opioids in Latin America and the Caribbean, analyses the new *modus operandi* of trafficking of synthetic drugs and precursors carried out by organized criminal groups. The results of the investigation carried out by the Global Programme on Cybercrime in collaboration with the OPIOIDS Strategy suggests that synthetic drug markets in Latin America and the Caribbean are controlled by approximately 30 criminal groups misusing both the Darknet and Clearnet to negotiate the acquisition of precursors.

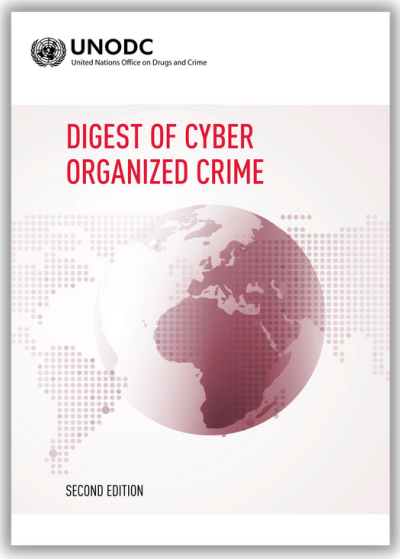
This report shares indications that cross-continental cooperation in the production and trafficking of synthetic drugs and synthetic opioids has gained momentum and changed previous patterns of offline drug trafficking. Now, some organized criminal groups in Latin America and the Caribbean receive shipments of precursors from Asia which are then used to produce synthetic drugs in clandestine labs in their respective areas. These groups are believed to be using both the Darknet and Clearnet to negotiate the acquisition and shipment of precursors through legitimate air and/or ocean transport services. These shipments are now made between Latin America and Southeast Asia directly, without any stops during the journey. Afterwards, drug traffickers seem to be misusing geolocalization and filtering capabilities of Clearnet apps, through which they can advertise and sell synthetic drugs and opioids at the destination points.

Bibliography database
SHERLOC.UNODC.ORG

THE REPORT IS AVAILABLE BOTH IN ENGLISH AND SPANISH ON SHERLOC'S BIBLIOGRAPHY DATABASE.

CYBERCRIME PUBLICATIONS AND TOOLS

DIGEST ON CYBER ORGANIZED CRIME

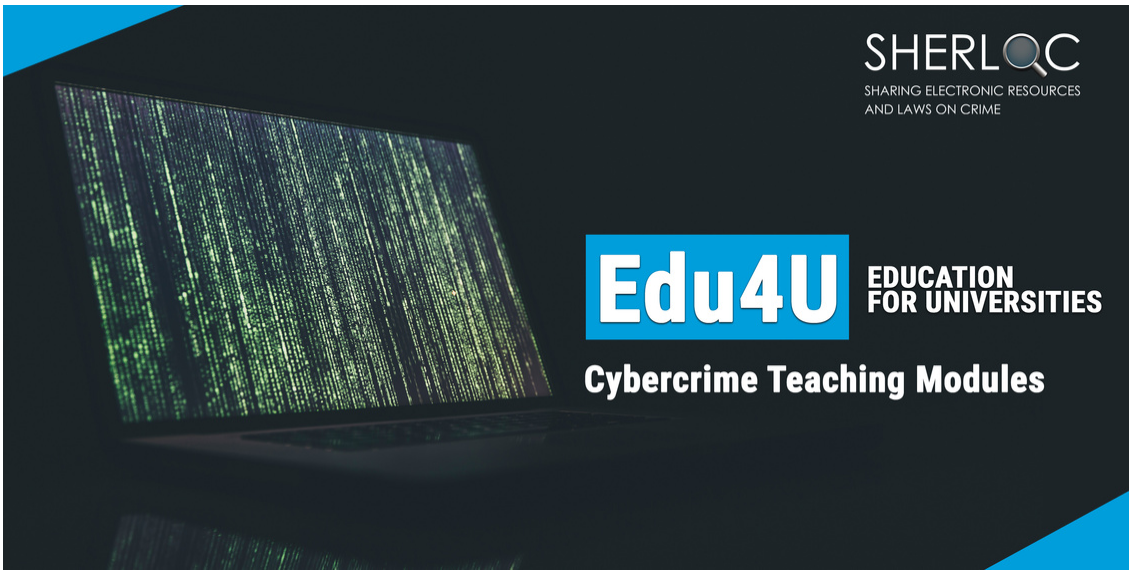


The combination of organized crime and cybercrime challenges is a complex one to handle at investigation, prosecution and adjudication levels.

In the UNODC Digest on Cyber Organized Crime, criminal justice practitioners can find a collection of 130 cases from 30 jurisdictions across the world that examine the structure and organization of cyber organized criminal groups, tools used by perpetrators, types of crimes and procedural challenges relating to the investigation, prosecution and adjudication of cyber organized crime cases. The case digest is a living document and is constantly updated with new cases, particularly from regions that are starting to develop their cybercrime case law.

THE 2ND EDITION OF THE DIGEST OF CYBER ORGANIZED CRIME IS AVAILABLE ON SHERLOC IN ENGLISH AND SPANISH.

CYBERCRIME TEACHING MODULES



High levels of digitalization and digital inter-connectivity have created opportunities for many forms of cybercriminal activities. To address this challenge, the Global Programme on Cybercrime has developed 14 Teaching Modules on different aspects of cybercrime that cover key issues and give an overall picture of the existing challenges around prevention and countering of cybercrime. While the teaching modules provide lecturers with the guidelines and resources to develop a comprehensive course on cybercrime, the corresponding Teaching Guide offers pedagogical guidance.

THE TEACHING MODULES ARE AVAILABLE IN ENGLISH AND RUSSIAN ON SHERLOC'S EDUCATION FOR UNIVERSITIES (EDU4U) DATABASE. SELECTED MODULES ARE ALSO AVAILABLE IN ARABIC, FRENCH, PORTUGUESE AND SPANISH.

LEARNING ABOUT CYBERCRIME AT THE SUMMER SCHOOL ON TRANSNATIONAL ORGANISED CRIME

On 21 June 2023, the Cybercrime and Anti-Money Laundering Section discussed on cyberspace, law and cooperation with 32 students participating in the Summer School on Transnational Organised Crime organized by the ECPR SGOC in cooperation with the Global Programme on Implementing the Organized Crime Convention of UNODC.

Students learned about the challenges of identifying applicable jurisdictions in cases of cybercrime, as well as the challenges posed by the asymmetric cooperation between the private and the public sector for the purpose of requesting digital evidence. They also learned about the four UN entities with cybercrime mandates: the General Assembly, the Security Council, the Department of Political and Peacebuilding Affairs and UNODC.

The crucial role of UNODC in developing international standards on cybercrime via the Ad Hoc Committee process to develop a comprehensive international convention to counter the use of Information and Communication Technologies with criminal purposes was discussed, including UNODC's role in providing technical assistance through the Global Programme on Cybercrime.

Case law database

SHERLOC.UNODC.ORG

Students will further contribute to expanding the resources on cybercrime available on SHERLOC by researching real-life examples of organized crime, including cyber organized crime, and developing case briefs, which will be reviewed and uploaded to SHERLOC's Case Law Database.

FEATURED CASE RELATING TO CYBER ORGANIZED CRIME

CYBERCRIME CASE LAW

R v. Vachon-Desjardins, 2022 ONCJ 43

Netwalkers was an organized criminal group dedicated to creating data-theft ransom software (Ransom-as-a-service, RaaS). Their affiliates were individuals who carried out these data-thefts, extorted their victims and shared up to 20% of the ransoms paid with Netwalkers' developers.

In 2021, Sebastien Vachon-Desjardins was arrested and detained in Canada pursuant to an extradition request by the United States of America.

In 2021, Sebastien Vachon-Desjardins was accused of ransomware attacks in several countries and suspected to have received more than USD 15 million in ransom payments. He was arrested and detained in Canada.

He was accused of ransomware attacks in several countries and suspected to have received over USD 15,000,000.00 in ransom payments from many extorted institutions, including health care and emergency services, law enforcement, educational and commercial institutions.

Based on IP addresses, and pursuant to thorough investigations into various accounts, aliases, email addresses, and personal information revealed on social media platforms, 20 tera-bytes of data were seized and recovered.

A complex set of offences involving mischief and theft of computer data, unauthorized use of a computer, extortion, and participation in a criminal organization were confirmed. The sentence included imprisonment and payment of more than 2 million CAD in restitution and the forfeiture of cryptocurrencies.

The case shows the difficulties and challenges in the investigation and prosecution of cyber-attacks including the identification and tracking of cryptocurrencies related to the attack.

This feature has been adapted from the original SHERLOC case entry. To find out more about this case, click here to access it on SHERLOC.

MEET A CONTRIBUTOR

RENATA DELGADO SCHENK

Renata is a lawyer specialized in international law and a criminal analyst. She is a national of Germany and has a 15-year career in the United Nations delivering technical assistance and training to strengthen skills and processes to investigate and prosecute complex crimes.

She has spent the majority of her career working in the field in countries such as Colombia, El Salvador and Guatemala. Prior to UNODC, Renata worked at OHCHR, UNDP, UNFPA, ILO and in a DPA special political mission that had the most ambitious UN mandate to carry out independent investigation and prosecution in national courts.

She joined UNODC twice. The first time supporting the Attorney General of Guatemala in developing the first prosecution operational standards on trafficking in women and children, and on femicide and violence against women, including within organized crime structures. The second time, in 2018, when she joined UNODC in El Salvador to advise a special prosecution unit dedicated to high-profile corruption cases. From there, she moved to the Vienna Headquarters. In 2021, she joined the Global Programme on Cybercrime as a Coordinator for projects implemented in Latin America. Recently, she has expanded her responsibility and leads the cyber diplomacy portfolio.