CyberSouth
Cooperation on cybercrime
in the Southern Neighbourhood

Version November 2020

Situation report on cybercrime and money laundering on the Internet, in Lebanon

Prepared within the framework of the CyberSouth Project

Disclaimer

The views expressed in this report do not necessarily reflect official positions of the Council of Europe, of the European Commission or of the Parties to the treaties referred to.

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

List of abbreviations

AML	Anti-Money Laundering
AMLU	FIU – Jordan
ANABI Romania	Asset Recovery Agency for Romania
ANSI	National Agency for Computer Security – Tunisia
CARIN	Camden Asset Recovery Inter-Agency Network
CERIST	Research Centre for Scientific and Technical Information - Algeria.
CTAF	FIU – Tunisia
CTRF	FIU – Algeria
CCCU	Cybercrimes Combatting Unit – Jordan
DDOS	Distributed Denial of Service Attack.
DGSN	General Director for Territorial Surveillance – Morocco
EGMONT	Egmont group of FIU information sharing network
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FI	Financial Investigator
ICO	Initial Coin Offering (relates to cryptocurrencies)
ICT	Information and communications technology
GDP	Gross Domestic Production
IBAN	International Bank Account Number
MENA	Middle East and North Africa Countries
MENAFATF	Middle East and North Africa Financial Action Task Force
MOU	Memorandum of Understanding.
PSD	Public Security Directorate – Jordan
SIC	FIU – Lebanon
SAR	Suspicious Activity Report
SOP	Standard Operating Procedures
STR	Suspicious Transaction Report
UTRF	FIU- Morocco

Table of Contents

1 Introduction

1.1 Description of CyberSouth project

Countries of the Southern Neighbourhood region, like any other country in the world, are confronted to the challenges of increasing dependency of our societies on information and communication technologies such as cybercrime. It is therefore essential for these countries to reinforce their institutional capacities to address cybercrime at country level, regional level and international level. Through the CyberSouth project, the European Union and the Council of Europe, in cooperation with other partners, will support this effort on the basis of existing tools and instruments including the Budapest Convention on Cybercrime.

PROJECT OBJECTIVE AND EXPECTED RESULTS
Objective: To strengthen legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood in line with human rights and rule of law requirements
Result 1 - Criminal law frameworks strengthened in line with the Budapest Convention on Cybercrime, including rule of law safeguards (Article 15)
Result 2 – Specialised police services and interagency as well public/private cooperation strengthened
Result 3 – Judicial training on cybercrime and electronic evidence mainstreamed
Result 4 – 24/7 points of contact are operational (at prosecution and/or police level) for more effective international cooperation on cybercrime and e-evidence
Result 5 – Strategic priorities on cybercrime and electronic evidence identified

1.2 Description of this activity

The growth of business on the on-line environment comes together with the development of various forms of payment instruments to facilitate the interconnectivity at the international level and rapid and smooth wired transfers.

The criminals looking to take advantage of the development of the new technologies are also benefiting of the on-line payment instruments for transferring the illegal income not only coming from cybercrime but also from other crime areas.

Cybercrime is a lucrative business and one of its key driving forces and motivation is generation of profits. Targeting cybercrime proceeds through conducting financial and money laundering investigations will increase efficiency and success of criminal investigations and criminal proceedings from the perspective of both prosecuting a criminal and seizing proceeds generated by such criminal activities.

Moreover, cybercrime reported and investigated by criminal justice authorities is related to different types of fraud aimed at obtaining illegal economic benefits. Vast amounts of crime proceeds are thus generated – and often laundered – on the Internet and through the use of information and communication technologies.

More efficient investigations and prosecutions of cybercrime and online crime proceeds depend on a range of factors including, availability of an effective legal framework criminalising conduct and putting in place necessary investigative tools, inter-agency cooperation and dialogue between various agencies, exchange of information between different professional communities, international cooperation, as well as public-private partnerships in cybercrime and financial investigations, and when following the money flows of the cybercriminals.

Hence, the CyberSouth project is trying to support the project countries to develop their capacities to target on-line crime proceeds and the interagency cooperation for benefiting of the tools and resources available in having a multidisciplinary approach.

These capacities will help the authorities not only to deal with cybercrime investigations but to look for on-line crime proceeds of other crimes as a comprehensive response and close cooperation between partners from various sectors.

In furtherance of these statements, the CyberSouth project held a half day regional online workshop on 1st July 2020, which had a number of international presenters from Romania, USA and UK who aimed to share knowledge on fighting against cybercrime and targeting online crime proceeds. At the conclusion of the workshop delegates gave some descriptions of current capacities of national authorities in conducting financial investigation in relation to cybercrime cases. This was supported by a short questionnaire that was completed by each beneficiary in order to provide further details of current tools and procedures used in the investigation of cybercrime and targeting online crime proceeds.

1.3 Aim of the report

The aim of this report is to summarise the details shared during the activity in order to assist authorities of the project countries to increase their knowledge on fighting against cybercrime and targeting online crime proceeds through the following:

- Identify the current capacities, tools and procedures for each of the national authorities to conduct financial investigation in relation to cybercrime cases.
- Examine challenges related to online crime proceeds and identify methods to enable project countries to identify and make use of national legislation and tools.
- Review interagency cooperation relating to search, seizure and confiscation of online crime proceeds.
- Present recommendations to the project countries for strengthening of current capacities, tools and interagency cooperation to conduct improved financial investigations and better target online crime proceeds in investigations and prosecutions relating to cybercrime and online crime.

1.4 Participants

The Council of Europe Workshop delegation was composed of:

– Mr. Virgil SPIRIDON, Head of Operations, Cybercrime Programme Office, Council of Europe;
– Ioana LAZAR, Senior Project Officer for CyberSouth, Council of Europe;
– Mr. Mick Jameison, Consultant on cybercrime and financial investigations, UK.
– Dean Kinsman (FBI, Assistant Legal Attaché - Bucharest)
– Elena Savu (Head of Online Child Sexual Exploitation Unit - Romanian National Police)
– Daniel Staicu (FIU Romania),
– Cornel Calinescu (ANABI Romania).

1.5 Description of organisational units and tools involved in the search, seizure and confiscation of proceeds of cybercrime and online crime.

Relevant to each country report are a number of organisational units and tools that are utilised in many countries for the search, seizure and confiscation of the proceeds of cybercrime and online crime.

The roles and powers of each unit often rely upon legal instruments being in place in that respective country, which designates roles and responsibilities.

Generic descriptions of these roles are provided below in order to understand the current status and recommendations in respective countries.

1.5.1 Cybercrime Unit

A dedicated police investigation or government unit that comprises of many different capabilities involving the prevention, detection and investigation of cybercrime and technology enabled crime.

1.5.2 Financial Intelligence Unit

A financial intelligence unit[1] (FIU) serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis.

The FIU should be able to obtain additional information from reporting entities and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

FIU's are usually able to share and receive information with national entities and financial institutions and with International Partners through informal intelligence sharing agreements such as the Egmont Group.

There are known at international level, four types of FIU:

- The **Judicial Model** is established within the judicial branch of government wherein "disclosures" of suspicious financial activity are received by the investigative agencies of a country from its financial sector such that the judiciary powers can be brought into play e.g. seizing funds, freezing accounts, conducting interrogations, detaining people, conducting searches, etc.

- The **Law Enforcement Model** implements anti-money laundering measures alongside already existing law enforcement systems, supporting the efforts of multiple law enforcement or judicial authorities with concurrent or sometimes competing jurisdictional authority to investigate money laundering.

- The **Administrative Model** is a centralised, independent, administrative authority, which receives and processes information from the financial sector and transmits disclosures to judicial or law enforcement authorities for prosecution. It functions as a "buffer" between the financial and the law enforcement communities.

- The **Hybrid Model** serves as a disclosure intermediary and a link to both judicial and law enforcement authorities. It combines elements of at least two of the FIU models.

[1] https://egmontgroup.org/en/content/financial-intelligence-units-fius

1.5.3 Financial Investigation

Financial investigation[2] is an investigative discipline concerned with exploring the finances that relate to criminal activity. It provides an important tool for the disruption of serious and organised crime and can be used to:

- develop evidence, which can be used in criminal proceedings,
- identify and trace the proceeds of crime,
- identify the extent of criminal networks and/or the scale of the criminality.

Although it is not always necessary to be a financial investigator (FI) to make use of financial investigative tools, FIs are the main practitioners of financial investigation.

Financial Investigators are not normally entitled to receive confidential information from financial institutions unless it is provided for through legislation allowing for the issue of production orders, search warrants or equivalent.

1.5.4 Parallel investigation

A 'parallel financial investigation'[3] refers to conducting a financial investigation alongside, or in the context of a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation or be able to refer the case to another agency to follow up with such investigations.

During the workshop adequate examples were provided on how parallel financial investigations can identify evidence that can be used in the predicate criminal investigation, how the locations and identities of suspects can be revealed and how the search, seizure and confiscation of criminal assets can be expedited.

1.5.5 Asset Recovery Unit

An Asset Recovery Unit[4] or Agency is created through legal instruments to conduct both national and international asset recoveries.

Asset recovery makes sure that crime does not pay by investigating, seizing and confiscating assets acquired by individuals, as a result of crime such as cash, property, vehicles and high-value goods.

Some Asset Recovery Units, such as Romania's 'Agentia Nationala de Administrare A Bunurilor Indesponbilzate' (ANABI) also convert assets into tangible fiat currency through the sale of confiscated assets to prevent the amount seized from devaluing.

1.5.6 Predicate offence of money laundering

A predicate offence is a crime that is a component of a more serious crime. For example, producing unlawful funds is the primary offence and money laundering is the predicate offence. The term "predicate offence" is usually used to describe money laundering or terrorist financing activities.[5]

---

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/753212/exploring-the-role-of-the- financial-investigator-report-horr104.pdf

[3] https://cfatf-gafic.org/index.php/documents/fatf-40r/396-fatf-recommendation-30-responsibilities-of-law-enforcement-and-investigative-authorities

[4] https://www.app.college.police.uk/app-content/investigations/investigative-strategies/financial-investigation-2/asset-recovery/

[5] https://aml-cft.net/library/predicate-offence/

Many countries indicate which primary offences must be committed before money laundering can be lawfully considered a predicate offence.

1.5.7 Relevant currencies used online

This report will refer to different descriptions of currencies, which are often relevant in financial investigation. They include fiat currency, representative money, virtual payment systems, digital currencies and cryptocurrencies. Often these terminologies are referred to in reporting that relates to financial investigation and the definitions often overlap or duplicate one another.

Fiat money is a government-issued currency that is not backed by a commodity such as gold. Fiat money gives national central banks greater control over their respective economies by controlling how much money is printed.[6]

Representative money is something that represents the intent to pay physical money (fiat money) and can be backed by a number of things such as money in a bank. Examples of representative money include credit cards and cheques. These forms of payment are used in place of traditional money.[7]

Virtual payment systems are the provision of electronic payment solutions for entities to make and receive payments typically by credit card and debit card.[8] An example of a virtual payment system is PayPal.

Digital currencies are a type of currency that have no physical form and only exist in digital form. Digital currencies include virtual money and cryptocurrencies. Digital currencies can be used as traditional money to buy and sell goods, but with the allowance of instant transactions and borderless transfer of ownership. Digital currencies can be both regulated by central authorities or decentralised.[9]

Virtual assets or virtual currencies are a type of digital currency, typically controlled by their creators and used and accepted among the members of a specific virtual community. Virtual money only exists in an online environment. Virtual currencies are not issued by banks and are unregulated. Examples of virtual money include Webmoney and cryptocurrencies such as Bitcoin and Ethereum.

Cryptocurrencies are virtual money or currency systems that rely upon encryption algorithms and cryptographic techniques to deliver security. The encryption algorithms make it difficult to counterfeit the currency or transactions. Most cryptocurrencies use blockchains to record and manage transfers. Cryptocurrencies have no central repository, meaning a computer failure or can wipe out the account if there is no back up or if the user does not have a private key.

Bitcoin is the most popular cryptocurrency and there is a growing skill set in the investigation of transactions. But other types of cryptocurrency such as Dash, ZCash and Monero are far more difficult to trace that Bitcoin.

---

[6] https://www.investopedia.com/terms/f/fiatmoney.asp
[7] https://www.investopedia.com/ask/answers/041615/what-difference-between-fiat-money-and-representative-money.asp
[8] https://dpath.com/virtual-payment-faqs/
[9] https://cointelegraph.com/tags/digital-currency

2 Lebanon

2.1 Financial Intelligence Unit

The Special Investigation Commission (SIC) is the Lebanese Financial Intelligence Unit. It is a multi-function financial intelligence unit with judicial status. It was established by the Anti-Money Laundering Law No 318 in 2001 (amended by Law 44/2015).[10] It acts as a Hybrid (administrative/judicial) FIU with key roles in countering money laundering and terrorist financing.

The initial assessment situation reports done in the project reported, "Well known, as being at the center of financial services in the region, the Lebanese banking sector is also a target for cybercriminals. The phenomena keeps increasing with cases of illegal money transfer. For 2015, the SIC reported that losses from cybercrime had exceeded $12 million. Very much aware of the risk, the SIC and the Cybercrime and Intellectual Property Bureau at the Internal Security Forces joined their efforts to fight cybercriminals attacks and mainly to spread awareness to the banking sector and individuals/companies that are more vulnerable to cyberattacks.

On its website www.sic.gov.lb the SIC provides two publications regarding cybercrime[11] which can be found easily through the home page. One is a quick reference for individuals and non-financial institutions which is an advisory note on how persons should protect themselves from a cybercriminal and what to do if they are subject to an online attack or loss. The second is a more detailed document providing advice and cybersecurity techniques on how businesses and banks could protect themselves from cybercriminals. Most of the comments in both documents relate to emails, phishing attacks and business email compromise type attacks.

In the questionnaire the SIC identified these documents stating that they, jointly with the Cybercrime Bureau at the Directorate of Internal Security Forces and the Association of Banks in Lebanon, issued the Guidance Manual on cybercrime protection in 2016. The manual identifies the various types of cybercrime conducted on the financial sector, companies and individuals. It comprises a guidance for each of the before-mentioned parties on how to protect themselves from cybercrime and provide them with indicators and red flags. The guidance also suggests policies and protective measures in order to mitigate such risks and proposes corrective measures for each of the types discussed within.

Since 2015, the SIC has conducted the Anti-Cybercrime Forum jointly with the Internal Security Forces which convenes yearly with respective international and local stakeholders as well as local banks and financial Institutions in order to share knowledge and exchange expertise in this domain.

Through the questionnaire the SIC identified that virtual currencies are not regulated in Lebanon and it does not have specific red flags for virtual assets. However, SIC is aware of existing trends and typologies abroad. The SIC has received several STRs regarding cryptocurrencies where the banks have automatically stopped the transactions from being conducted.

Further answers to the questionnaire indicated that a number of STR's relating to cybercrime have been received including fraud, email hacking and phishing. All such cases were passed on to the General Prosecutor in order to take appropriate measures, such as referring them to the Cybercrime Bureau at the Directorate of Internal Security Forces for the purpose of sharing intelligence and contacting the INTERPOL, when needed. In 2019, 48% of cases submitted to the General Prosecutor by SIC related to Cybercrime.

[10] https://sic.gov.lb/sites/default/files/publications/SIC%202014%20annual%20report_english.pdf

[11] https://sic.gov.lb/publications/11

2.2 Financial Investigations

Police officers undertake the investigation of financial crimes and money counterfeiting, but no details were provided of parallel financial investigations in relation to cybercrime.

Financial investigators do receive some training in detecting counterfeiting, money laundering, financing terrorism. Their task to obtain financial information from banks or similar institutions in parallel with financial investigations and money laundering cases is limited due to Bank Secrecy requirements.

The responses to the questionnaire tend to indicate that Financial Investigators in Lebanon tend to focus upon financial crime rather than parallel financial investigations involving the recovery of the proceeds of crime. No examples were provided of parallel investigations involving cybercrime.

2.3 Cybercrime Unit

The cybercrime unit leads investigations involving Intellectual Property Crimes and Cybercrimes, whilst providing support to investigations involving terrorism, financial crimes, organized crimes, drugs crimes and illegal gambling.

The cybercrime unit conducts many investigations involving financial losses and gains and often conducts investigations with the office countering financial crimes.

The cybercrime unit reported that there is a coordination and information sharing with the SIC through the Public Prosecutor.

2.4 National legislation

Lebanon has legislation in place which is known as Law no 44 of November 24. 2015 Fighting Money Laundering and Terrorist Financing (Law no 44/2015). Article 1 of Law no 44/2015 adequately describes illicit funds to include tangible and intangible, movable and immovable, including any legal documents or instruments evidencing title to, or interest in, such assets, resulting from the commission of, or the punishable attempted commission of, or the participation in any of the 21 offences listed, whether in Lebanon or abroad.

Law no 44/2015 also describes offences of extortion (which would include ransomware and distributed denial of service attacks with a demand for a ransom), sexual exploitation of children, credit card counterfeiting and fraud as predicate offences.[12]

Law no 44/2015 appears to offer coverage of most cybercrimes that are likely to result in financial loss or gain and article 14 provides the Courts with legal frameworks to confiscate these illicit funds. However, fraud or another predicate offence would need to be preferred in criminal cases as Law no 44/2015 does not specifically detail criminal offences of Illegal Access to an Information System, Compromises System

[12] https://sic.gov.lb/sites/default/files/laws-regulations/Law%2044%20En.pdf

Integrity, Compromising Digital Data Integrity, Hinderance, Disturbance or Disruption and Misuse of Hardware and IT Platforms (Articles 110 – 114 of Law No 81 Relating to Electronic Transactions and Personal Data). These offences meet the criteria of Articles 2, 3, 4, 5, 6 of the Budapest Convention on Cybercrime but provide no legal framework to undertake financial investigations. It is known that cybercriminals acquire data through a number of illegal methods and then sell it to other criminals through online forums on the Internet and Dark Net.

No law was identified during the workshop, the questionnaire or research that identified national legislation that provided a legal instrument for Police Financial Investigators to apply to banks or other financial institutions either through the courts or prosecutors for information and evidence in financial investigations. In many similar countries these types of activities are limited to the public prosecutor.

Albeit that cryptocurrencies are not currently included in the Lebanese legislation, there appears to be no legal barrier in the search, seizure and confiscation of these types of funds during criminal and parallel investigations.

2.5 Interagency cooperation

There appeared to be strong collaboration between the SIC, the Police and the Private Sector aimed at the prevention of cybercrime and laundering online crime proceeds.

The Interagency cooperation relating to search, seizure and confiscation of online crime proceeds appeared to be limited to those permitted under the auspices of the Public Prosecutor. Examples are provided by the SIC where cases are shared with the General Prosecutor and the Directorate of Internal Security Forces for the purpose of intelligence sharing and contacting Interpol when needed, which is a positive position.

The collective use of international networks, such as Interpol, CARIN, FIU.Net, Egmont, Budapest convention 24/7 networks could further enhance parallel financial investigation. Interagency cooperation is often underpinned through memorandum of understanding (or similar) to ensure fast time exchange of information and intelligence and according to pre-determined agreements. There was no evidence of any such agreements, but cooperation is reported to be productive.

2.6 Challenges

Financial Investigation and specifically parallel financial investigation methodologies are underused tools in the search, seizure and confiscation of online crime.

There are no legal obstacles to the search, seizure and confiscation of cryptocurrencies and virtual currencies. But there are no current decrees required to arrange for the transferring of any illicit funds into Fiat Money.

There are no current Standard Operating Procedures (SOP) for the investigation of blockchain evidence and the search, seizure and confiscation of cryptocurrencies.

There is no legislative framework that allows for parallel financial investigation as explained in section 1.5.3 and regarded as best practice in many countries.

There are no legislative orders regarding the use of blockchain evidence in criminal investigations such as cybercrime and money laundering investigations. But Chapter II of Law No 81 Relating to Electronic Transactions and Personal Data does allow for electronic documents to be accepted as evidence.[13]

[13] https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf

Interagency cooperation takes place through the General Prosecutor's Office and that may sometimes delay intelligence sharing opportunities.

2.7 Recommendations

The following recommendations could be of consideration for the Lebanese authorities in order to reinforce their capabilities to conduct parallel financial investigations in relation to cybercrime cases:

1. Make parallel financial investigation a strategic part of all investigations where online proceeds of cybercrime are involved.

2. Create Standard Operating Procedures in the investigation, search, seizure and confiscation of all virtual currencies.

3. Create a system that enables cryptocurrencies that may be confiscated or seized to be legally held in wallets or similar under the control of the authorities, which could be the Police, Prosecutor, Court or Asset Recovery Agency.

4. Improve levels of training in cybercrime and cryptocurrencies at the Cybercrime Unit, SIC and Financial Investigators.

5. Use Memorandum of Understanding to support Interagency Cooperation and intelligence sharing.

3 Agenda of the workshop

WEDNESDAY, 1st of July 2020	
14.30 – 14:40	Introductory remarks • Council of Europe representative *COE representative:* Mr Virgil Spiridon
14:40 – 15:00	Session 1: Cybercrime economy and emerging challenges related to on-line crime proceeds • Cybercrime global impact • Payment card fraud • Money mules • Cryptocurrencies • Darknet *Presentation*: Mr Mick Jameison (International expert)
15:00 – 15.30	Session 2 – Countering money laundering in the on-line environment • On-line money laundering typologies • Case studies *Presentations*: Dean Kinsman (FBI Legal Attaché - Bucharest) Elena Savu (Online Child Sexual Exploitation Unit - Romanian National Police)
15.30 -16.00	Session 3 – Interagency cooperation in the search, seizure and confiscation of on-line crime proceeds • Procedures and best practices • Legal and technical instruments for cooperation *Presentations*: Daniel Staicu (FIU Romania), Cornel Calinescu (ANABI Romania)
16.00 – 16.40	Session 4 – National legislation and tools for the search, seizure and confiscation of on-line crime proceeds. Each delegation will prepare a short presentation (5-7 minutes) focusing on the current national situation on cybercrime and money laundering on the internet.
16.40 – 17.00	Session 5 – Overview and final recommendations *Presentation and discussions on the recommendations for strengthening the capacities of the priority countries on targeting on-line crime proceeds.* • International expert • Delegations • COE representative