Combating Cybercrime in Southeast Europe in the Framework of the Southeast European Law Enforcement Center (SELEC)

Snejana MALEEVA
Southeast European Law Enforcement Center (SELEC)
secretariat@selec.org

Abstract: Cybercrime became a crime area with the uppermost boost, in the number of cases, as well as in sophistication. Enabled by the technology development, cybercrime is continuously growing having a serious impact on most areas of transborder crime, including white-collar crime.

Keywords: Law enforcement, Cybercrime, Southeast Europe, Organized crime, Joint investigations.

INTRODUCTION

The Internet and technology have revolutionized everything around us, including the way in which the criminal networks organise and conduct their activities. There is not a single organized crime group in the region that does not take advantage of the technology development, either by committing cybercrimes or cyber enabled crimes. Thus, the law enforcement community has no other option but to keep up with these increasing criminal activities, and find the perfect synergy between traditional investigation approach and the use of the latest tools at their disposal in order to prevent and counter cybercrime.

SELEC'S ROLE IN THE FIELD

Established in 1999 as SECI Center, transformed in SELEC in 2011, with a stronger legal base and mandate, SELEC has evolved from an operational platform to combat all forms of transborder serious and organized crime, including cybercrime, to an indispensable segment of the security of the region, and one of the most successful examples of regional cooperation.

SELEC is focused on operational matters, offering the platform for the real-time exchange of information and requests of assistance, supporting and coordinating joint investigations and regional operations, developing analytical reports, contributing to the capacity building of our Member States and Partners through trainings, expert missions, secure connection through the new Operational Center Unit, organizing regional conferences, Task Force meetings, workshops, study visits, facilitating networking, a/o.

The swift exchange of information and data is done through the Liaison Officers from Police and Customs authorities of the Member States posted at SELEC Headquarters in Bucharest/ Romania, supported by the National Focal Points established in each of the Member States.

The work of Police and Customs is complemented by the Southeast European Prosecutors Advisory Group (SEEPAG), a network of experienced prosecutors working in international cooperation in criminal matters. The prosecutorial network has been functioning under SELEC's auspices since 2003 with a view of facilitating and speeding-up the cooperation in serious trans-border crime investigations and cases in Southeast Europe.

During the 20 years since its establishment, SELEC's operational activities have gradually developed, the Center continues to remain the most reliable and cost-effective cooperation platform for its 11 Member States and 24 Partners (countries and organizations) and, in general in the region, as a key player in the fight against transborder serious and organized crime.

With the occasion of its 20 anniversary, celebrated in 2019, SELEC organized a high level conference during which a Joint Declaration was adopted by the Ministers, Heads of Police and Customs of SELEC Member States, that recognized and appreciated the achievements made by SELEC throughout the 20 years of successful law enforcement cooperation, and re-confirmed the full support of the Member States to the work and further development of SELEC (SELEC, 2019).

High level representatives of the Member States at SELEC's 20 anniversary

SELEC is the only law enforcement in Southeast Europe that joins the resources and expertise of Police and Customs authorities of its eleven Member States, namely:

Republic of Albania
Bosnia and Herzegovina
Republic of Bulgaria
Hellenic Republic
Hungary
Republic of Moldova
Montenegro
Republic of North Macedonia
Romania
Republic of Serbia
Republic of Turkey

Besides the 11 Member States, SELEC has 24 partner countries and organizations (Interpol, Italy, United Kingdom and USA as Operational Partners; and Austria, Belgium, Belarus, Czech Republic, EUBAM, France, GCC-CIC, Georgia, Germany, IOM, Japan, Israel, The Netherlands, Slovakia, Spain, Switzerland, Ukraine, UNODC, UNMiK, UNODC, WCO, as Observers), and has also established numerous partnerships with various organizations and bodies, as well as with the private sector.

OPERATIONAL CENTER UNIT

In an effort to constantly increase its support to the Member States in countering transborder crime in Southeast Europe, SELEC has recently added to its operational capacities a new state-of-the-art, highly secured Operational Center Unit (SELEC, 2020c).

The hardware architecture is flexible, scalable and provides high data security. It includes the integration and communication with National Focal Points of the Member States with voice and video communication solutions.

A crisis steering committee room is integrated into the Operational Center Unit, with fully encrypted voice, data and video communication.

The Operational Center Unit (OCU), that includes the customized SELEC Intelligence Reporting Application Tool (S.I.R.A.T), is based on a high-reliability and availability infrastructure capable of delivering 24/7 fast service.

The IT solution comprises an operational platform including Geographic Information System (GIS), real-time situation awareness, incident management, reporting, Data Analytics Law Enforcement Intelligence Application, Collection Information Tool and a Document Management System.

The customized S.I.R.A.T application ensures a fast collection, analysis and exchange of strategic and operational information among Case Officers, National Focal Points, SELEC Liaison Officers and SELEC analysts.

The Operational Center Unit

SELEC's operational activities are addressing mainly issues such as drug trafficking, smuggling of migrants, human beings trafficking, financial and computer crimes, smuggling and customs fraud, terrorism, container security, environmental and nature related crimes, stolen vehicles, a/o.

SPECIALIZED TASK FORCE- FINANCIAL AND COMPUTER CRIME TASK FORCE

There is no doubt that the society becomes increasingly digitized, being practically shaped by cyberspace. Technology and the Internet have changed the way we live, communicate and share knowledge, to the extent that we connect almost all everyday tasks to technology.

The Internet connects virtually billions of people and devices. The concept of "*Internet of Things*" leads our existence, as all devices with network capabilities are interlinked and remain vulnerable to attacks and misuse. The Internet is linked to specific crimes that exist because of the Internet itself (cyber-dependent crime,) and to crimes that are boosted up by the Internet (cyber-enabled crimes).

Cyber-dependent crimes are offences whose existence is governed by computers and networks (including Internet), and can only be committed using a computer, computer networks or other forms of information communications technology.

Cyber-enabled crimes are traditional crimes e.g. theft, smuggling, fraud, harassment, that can be committed without the support of technology, but can be increased in scale or reach by use of computers, computer networks or other forms of information communications technology.

Despite the benefits, technology and the Internet offer plenty of opportunities for criminals to commit crimes or to support them in committing crimes.

This increased use of technology poses one of the main challenges to the law enforcement.

In this aspect, since 2001, within SELEC has been functioning the Financial and Computer Crime Task Force, that offers the platform for sharing good practices and challenges faced by the law enforcement officers in their work, for initiating joint investigations in the field, for evaluating the activities conducted and deciding upon further steps to be taken, as part of a common and more effective endeavour in tackling transborder serious and organized crime in the field of cyber crime.

JOINT INVESTIGATIONS

Many successful cyber-related joint investigations were carried out under SELEC's umbrella, and I would like to briefly mention some of them, as examples of good practices in operational international cooperation:

Joint investigation PRATKA/VIRUS (SELEC, 2017), in the field of cybercrime, committed by compromising the countries' Customs computerized systems in order to avoid and save taxes. The organized criminal group consisted in Bulgarian nationals having connections in Republic of North Macedonia, Hellenic Republic, Romania and Republic of Serbia.

The modus operandi used was recruiting corrupted Customs officers in all involved countries with the purpose to infiltrate a virus in the Customs' computerized systems. Once the virus installed, from distance, the offenders were able to finalize various transports, as in the Customs' system appeared that the cargo was already checked and passed.

The Bulgarian authorities have searched more than 100 addresses, suspects and vehicles. A large quantity of money was seized, as well as equipment, devices for communication, computers, tablets, bank documents, etc.

23 suspects were arrested, 5 of them acting as Bulgarian Customs officers.

As result of this criminal activity the damages recorded by the Bulgarian Customs Agency, only for year 2015, was around 5 million euro.

It was determined that the members of the organized crime group invested the money obtained from these illegal activities in bitcoins, around 200,000 being discovered in the virtual space. The offenders choose the bitcoin way of investing/saving the money, because it is rather difficult to be tracked and followed.

Joint investigation MONEY MULLES (SELEC, 2016) developed between Republic of Moldova and Romania targeted an organized criminal group consisting in Moldovan, Romanian and Ukrainian nationals dealing with cybercrime and money laundering.

The Romanian competent authorities performed investigations with regard to the activities of this criminal group that was acting with the purpose to obtain illegal funds by using cybercrime, namely committing cyber-attacks to the Internet banking applications owned by clients of various banks from Europe, United States and Australia. Using a malware, credentials of the online banking accounts were obtained, that were further used for making unauthorized bank transfers.

As a modus operandi for laundering the money the criminal group used the "money mule" scheme which aims concealing the final beneficiary of the money by using different EU citizens recruited with the purpose to act as intermediary, namely to receive and re- transmit amounts of money obtained illegally.

The estimated damages in this case were in value of approximately 6 million euro.

Joint investigation SIMBOX (SELEC, 2015) involved the competent law enforcement authorities from Republic of North Macedonia and Republic of Serbia, and targeted an organized criminal group dealing with illegal transfer of international phone traffic to national phone traffic. The operation led to the seizure of several SIMBOX devices, over 40,000 SIM cards and computer equipment. The organized criminal group illegally started using telecommunication devices for the use of telephone call termination.

The devices were connected through Internet and using the network of foreign mobile communication operators, with their SIM cards, were establishing international communication at the price of a local voice call. In this way, they by-passed international telephone traffic using « VOIP » technologies on unregistered pre-paid mobile phone terminals.

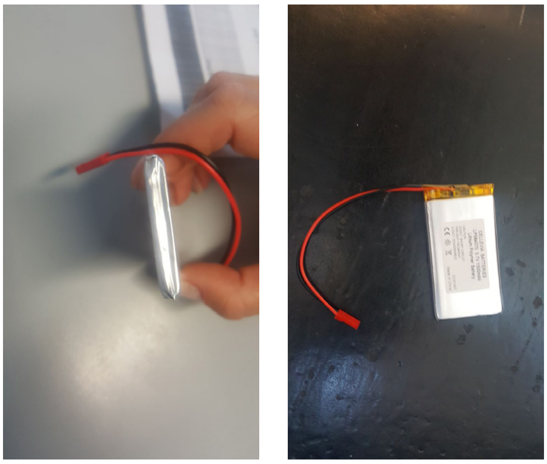
As a result of the criminal activity, the mobile communication operators suffered a financial loss of more than half a million Euro.

Joint investigation SIMBOX

Joint investigation CORVUS was conducted by the Greek, Romanian and Turkish law enforcement authorities, with the purpose of investigating a special case that initially started as a test for deep inserted skimming case.

During the surveillance and wiretapping of almost 85 suspects, intelligence about other crimes (drug trafficking and extortion) was also collected in the course of the investigation.

As a result, 20 suspects were prosecuted for crimes such as setting up an organized criminal group, making fraudulent financial operations, illegal access to an IT system, counterfeiting of bonds or payment instruments, circulation of counterfeited securities and money laundering.



Joint investigation CORVUS

TRAINING ON CYBERCRIME

As part of the SELEC cyber related strategy we organize trainings with the purpose to increase the capacity building of the law enforcement authorities in the field of cybercrime with the overall purpose to improve regional coordination and cooperation in the Southeast European region in fighting cybercrime and related crime (SELEC, 2020a).

Last year, among other trainings, we organised specific trainings on Darknet and cryptocurrency investigations, online investigations, investigations on Surface Web, a/o. More than 250 law enforcement officers being trained in 2019 (SELEC, 2020a).

This year, we expanded our training resources portfolio, introducing a new training module based on Virtual Reality.

Virtual reality equipment

The training is structured as an independent activity, using game specific mechanics in order to offer trainees an opportunity to apply the information they've learned during the training in a scenario which closely matches their actual work environment.

The trainees enter a virtual environment which replicates a border crossing point and have to inspect a vehicle suspected of transporting smuggled cigarettes. This mission tests their attention and perspicacity, completely immersing them in the virtual environment.

This fresh set of training resources include also a collection of multimedia course activities based on interactive branched scenarios. Each of these activities is built around realistic vehicles and ships inspections in search of smuggled goods. Apart from smuggling, they also address other types of cross border crimes which are frequently encountered in the daily activity of the partner institutions from the Member States.

These new training resources and activities make the training programs more appealing, offering the trainer team the opportunity to implement modern training strategies, in step with the ever-changing challenges law enforcement institutions have to face.

ANALYTICAL PRODUCTS

SELEC supports its Member States by providing strategic analytical reports (on drug seizures in Southeast Europe, on smuggling of migrants, on trafficking in human beings, on cigarettes and tobacco smuggling, on vehicle crimes, a/o) (SELEC, 2020b).

One of the most comprehensive report prepared by SELEC is the Organized Crime Threat Assessment for Southeast Europe (OCTA SEE) covering a 5 years period (SELECT, 2018).

SELEC
Southeast European Law Enforcement Center
CRIME STEERS ONLINE
OCTA SEE 2018
ORGANIZED CRIME THREAT ASSESSMENT FOR SOUTHEAST EUROPE
RESTRICTED
LAW ENFORCEMENT AND JUDICIAL USE ONLY

The cover of the 2018 OCTA SEE

OCTA SEE is illustrating the current situation and trends, identifying threats in SELEC Member States, highlighting vulnerabilities and opportunities revealed by various types of crime.

The latest report, OCTA SEE 2018, calls for 5 (five) key priorities, one of these being, of course, Cybercrime.

The organized criminal groups (OCGs) are increasingly incorporating technology and the Internet into their criminal activities, either by committing cybercrimes or by using them to commit other crimes. For all these reasons the report carries the motto “Crime Steers Online” and it applies to all the major crime areas today (SELEC, 2018).

The full report is restricted to law enforcement and judicial use only.

In the area of cybercrime, the public version of this report, available on the SELEC website, compiles the regional current state, emerging trends and cyber-related challenges.

Below are some major key findings from this report (SELEC, 2018):

- Cybercrime embraces many forms in Southeast Europe, classified in: cyber-dependent crimes, cyber-enabled crimes and payment card frauds;
- Cybercrime has increasingly been converted into a business-like concept. Cyber-as-a-service has opened the door to any person looking for committing cybercrimes, regardless of their technical skills;
- As a result of the expansion of the mobile devices, there is an emerging threat to all Internet connected mobile devices;
- Cybercriminals are as diverse as the real criminals, the OCGs having a wide-range of structures, ranging from hierarchical to horizontal, with cell-like structures located in other countries around the globe;
- An important role in an OCG is given to “mules” who are members of the OCGs or temporary collaborators with the role to receive the money (in a bank account or via money transfer companies) and deliver it to the leader(s) of the OCGs for a certain share, or even for a monthly remuneration;
- In the upcoming future it might be expected an overflow of AI-powered malware;
- New tools available to criminals such as open source intelligence, Social Network Analysis, chat bot, misuse of Linked Data, and profiling may be used to initiate complex attacks against many victims simultaneously;
- Blockchain technology has experienced in the last years a notable breakthrough, and, as an outcome of this technology, many cryptocurrencies have emerged in the last years. The cybercriminals will continue to take advantage of the opportunities offered by the privacy coins created to avoid tracking;
- The continuous evolving Darknet continues to represent a major challenge. There are dozens of Darknet markets linked to cybercrime-as-a-service, advertising illegal items, including cybercrime tools, credit card data, services, a/o;
- SIMBOX frauds are used in the region to bypass the international calls;
- In line with traditional crime becoming more connected to cyberspace and criminals becoming more aware of its added value, we can expect to see more and more specialists hired to carry out cyber-attacks to complement other criminal activities;
- Using mainly DDoS, more and more the targets of the cybercriminals are servers and infrastructure of the public and private sectors;

- Ransomware continues to have enormous potential to develop. The ransomware on mobile devices will be most likely one of the major threat;
- Cybercriminals will probably focus on techniques to obtain cryptocurrencies through various means, such as cryptojacking or wallet address stealer;
- Bearing in mind its nature and the fact that it may be used to commit many other crimes, identity theft can be put in the midpoint of all types of frauds;
- Social engineering is a key skill of the criminals involved mainly in frauds, as for example in the increasing number of registered cases of CEO frauds;
- Document forgery is a frequent and necessary technique for Internet fraudsters to deceit victims;
- Even if it remains a practice of the OCGs in the region, the traditional skimming is replaced more and more with massive and complex cyber-attacks;
- The skimmers are becoming smaller and more sophisticated;
- Cyber-criminals in the region may exploit hardware and software vulnerabilities to initiate a contact with the ATM, as Blackbox or ATM malware;
- Alternative payment systems based on contactless technology, wearables, augmented reality are expected to sustain the growth of non-cash payments, bringing along new form of crimes;
- The most prioritized cyber-enabled crimes are those related to child online sexual exploitation. The online environment e.g. files hosting sites, cyber lockers, social media, chat rooms and forums, offers opportunities for sexual offenders to find new victims;
- The Internet is used by criminals also to blackmail or disparage people by taking over their social media accounts and/or by publishing photos/videos with compromising content;
- The challenges for the law enforcement authorities in the field of cybercrime investigations are enormous since the cybercriminals and the evidences may be located anywhere;
- A dangerous type of cybercrime has emerged, the cybercrime initiated to support traditional crime (e.g. drug trafficking), which can only pose new threats.

These are only some of the key findings of OCTA SEE as regards cybercrime.

It is understandable that cybercrime cannot be addressed by each country individually, but through a synergy of actions from all the actors involved, therefore, an enhanced police and judicial cooperation need can be easily observed.

One of the most successful examples of such cooperation is SELEC, that gathers under the same umbrella the law enforcement and the judicial components.

SELEC remains committed in supporting the law enforcement authorities and providing a platform for tackling common regional problems calling for concerted action, with a general objective to identify solutions that can boost the effective cooperation among the Member States and partners, including in the field of fighting cybercrime. More information about SELEC is available at www.selec.org and on Facebook and LinkedIn at #selecbucharest.

REFERENCE LIST

South-East European Law Enforcement Center (2017) More than 200,000 bitcoins in value of 500 million USD found by the Bulgarian authorities. SELEC website, https://www.selec.org/more-than-200000-bitcoins-in-value-of-500-million-usd-found-by-the-bulgarian-authorities/

South-East European Law Enforcement Center (2016) SELEC awards successful operations conducted by the law enforcement authorities of its Member States. SELEC website https://www.selec.org/selec-awards-successful-operations-conducted-by-the-law-enforcement-authorities-of-its-member-states/

South-East European Law Enforcement Center (2015) First prize granted to Former Yugoslav Republic of Macedonia and Republic of Serbia for the Operation SIMBOX. SELEC Website, https://www.selec.org/first-prize-granted-to-former-yugoslav-republic-of-macedonia-and-republic-of-serbia-for-the-operation-simbox/

South-East European Law Enforcement Center (2020a) SELEC Training Activities. Information from SELEC website, https://www.selec.org/trainings/

South-East European Law Enforcement Center (2020b) SELEC Analytical Products. Information from SELEC website, https://www.selec.org/analytical-products/

South-East European Law Enforcement Center (2020c) SELEC Operational Center Unit. Information from SELEC website, https://www.selec.org/operational-center-unit/

South-East European Law Enforcement Center (2019) Joint Declaration of SELEC Member States, https://www.selec.org/wp-content/uploads/2019/11/SELEC-Joint-Declaration_Conference_31.10.2019.pdf

South-East European Law Enforcement Center (2018) Organized Crime Threat Assessment for South-East Europe - OCTA SEE 2018, as SELEC (2018), https://www.selec.org/analytical-products/

Snejana MALEEVA

Is currently the Director General of the Southeast European Law Enforcement Center (SELEC), having a vast experience in international relations, in legal and law enforcement matters. Mrs. Maleeva holds a Master's degree in Law and a BA in Rhetoric, with post-graduation specialization in international cooperation at the Sofia University, and in European Law at the College of Europe (Belgium) and the European Institute of Public Administration (Luxembourg). Prior being elected as Director for Legal and Internal Affairs and then Director General of SELEC, Mrs. Maleeva was Director of the European Integration Directorate within the Ministry of Justice and then Head of the European Affairs Department in the Ministry of Interior of Republic of Bulgaria, being involved and contributing actively in the process of Bulgaria's accession to the European Union. With multiple publications, lectures and speeches in Bulgaria and abroad, Mrs. Maleeva is constantly participating and contributing in numerous international fora on legal, international and law enforcement issues. As recognition of her professional accomplishments she received numerous awards, being also granted the Golden Medal "Justice, Security, Liberty". Mrs. Maleeva speaks English, French and Russian.