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

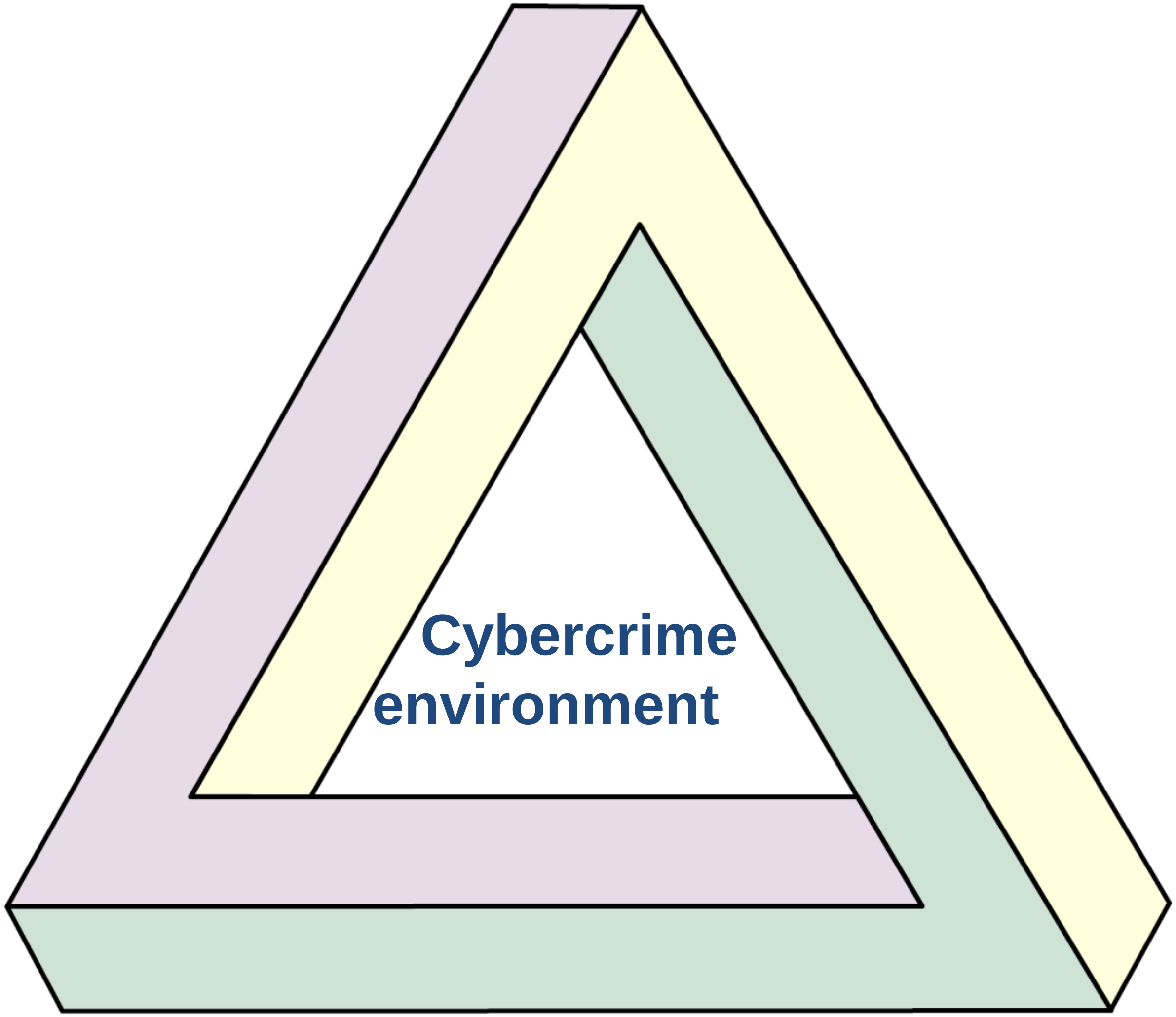
Experience of Romania in setting up a Cybercrime Unit

CyberSouth Launching Conference,
Tunis, March 21-23, 2018

AGENDA

- The historical perspective
- Challenges
- Staff and training
- Reporting platform
- National and international cooperation
- Lessons learned

How it all started?



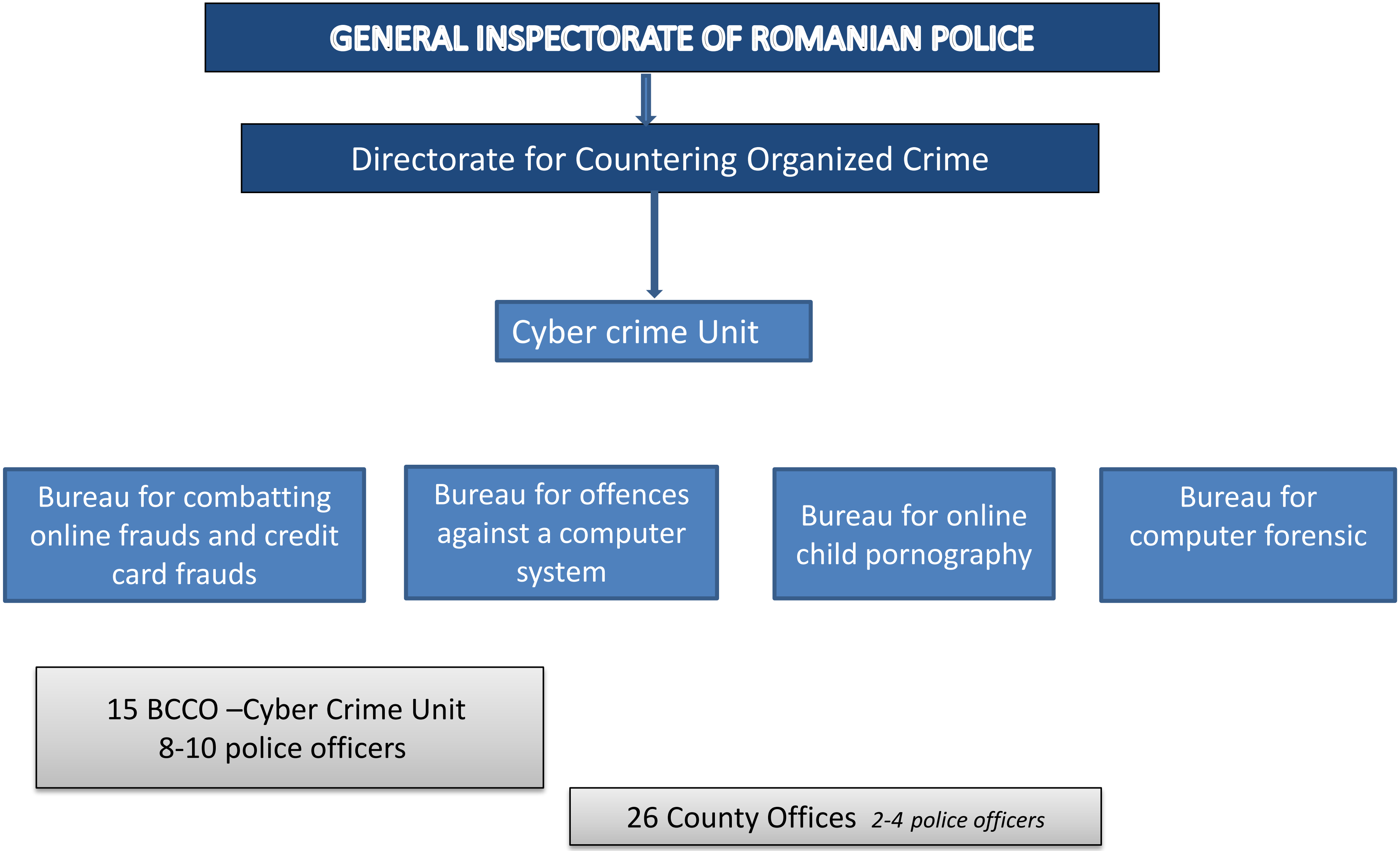
Legislation

Cybercrime environment

Cybercrime Unit

Cyber Cases

Organizational Chart



GENERAL INSPECTORATE OF ROMANIAN POLICE

Directorate for Countering Organized Crime

Cyber crime Unit

Bureau for combatting online frauds and credit card frauds

Bureau for offences against a computer system

Bureau for online child pornography

Bureau for computer forensic

15 BCCO –Cyber Crime Unit
8-10 police officers

26 County Offices *2-4 police officers*

Cybercrime Unit

1. E-Commerce Frauds and Frauds committed with electronic payment instruments:

- Electronic commerce related - *Auction frauds, CEO Frauds*
- Credit card related – e.g. *skimming, phishing, CNP fraud, ATM Malware attacks*

2. Forensic Unit:

- Forensic examination
- Access to a computer sistem
- Data preservation requests and processing internet traffic

3. Child Pornography Unit: - Child Pornography by use of computer

- Producing,
- Offering, making available, promoting
- Distributing or transmitting,
- Procuring for oneself or another,
- Possessing, without right, pornographic materials with minors with in a computer system or data storage device**,**

4. Computer intrusions

- Crimes against a computer systems – e.g. *unauthorized computer access /data transfer/* illegal interception of any transmission of computer data that is not publicly available/ illegal alteration, deletion or deterioration of computer data or the access restriction to such data/ serious hindering, without right, of a computer system operation, by the introducing, transmitting, altering, deleting or deteriorating computer data or by restricting the access to the data

Institutional developments

2003 – was established the Cyber Crime Unit (central level/8 positions)

2004 – was established a technical section (computer searches and internet interception)/ 4 additional position

2005 - was established the section for child pornography on the internet

- was established the section for credit card fraud /6 additional positions

2008 -was established a Directorate for Cyber Crime (Internet fraud and computer crimes/Credit card fraud/Computer forensic -34 police officers

2003- first police officers assigned to the field offices

2004-2006 -increased the number of the police officers assigned to the field offices

2008 –creation of the Cyber Crime Units at the territorial level

2009 -160 police officers

2009- reorganization - Bureau for investigations/Bureau for computer forensic

2012 –increased the number of the officers assigned to the field offices

2012- creation of the Bureau for offences related to online child abuse

2013 –creation of the Bureau for offences against computer systems

2017- increased the numbers of officers for Computer Forensic (10 only at the Central Level)

Cybercrime Legislation

Penal Code

- ART. 367 Creation of an organized crime group
- ART. 360 Illegal acces to a computer system
- ART. 361 Illegal interception of a computer data transmission
- ART. 362 Computer data alteration
- ART. 363 Operation disruption of computer systems
- ART. 364 Unauthorized data transfer
- ART. 365 Illegal operations with digital devices and software
- ART. 249 Computer fraud
- ART. 250 Making fraudulent financial operations
- ART. 251 Accepting transactions made fraudulently
- ART. 311 Counterfeiting of bonds or payment instruments
- ART. 313 Circulation of counterfeited securities
- ART. 314 Possesion of tools used for the counterfeit of securities
- ART. 315 Fraudulent issuance of currency
- ART. 315 Counterfeiting of foreign instruments
- ART. 374 Child pornography through computer systems

Challenges for the creation of Cyber Crime Unit

- Management decisions
- Legal framework and responsibilities
- Competences
- Location
- People and equipment
- Visibility of the Unit
- Investigations

Romanian approach

- Development of the units
- Selection of the personnel
- Training Programs
- Acquisition of necessary equipment
- Investigative procedures
- Enhanced public-private partnership
- International cooperation

Responsibilities for the Central Cyber Crime Unit

- Establish the strategies/policies/evaluations
- Coordination and providing assistance to the field offices
- Develop the internal standard procedures
- Conduct investigations/forensic/undercover/intelligence
- Establish the national training program
- Coordination of the inter-agency cooperation
- Coordination of the public-private partnership
- Coordination of the international cooperation

Cybercrime activities

- perform investigations for combating cybercrime;
- collect and analyze data and information;
- carry out technical activities for researching computer systems;
- assist other police departments in performing online investigations;
- perform activities for international judicial assistance for criminal issues, within national and international mutual assistance;
- conduct public awareness and cybercrime prevention activities

Staff - Police officers or police support staff?

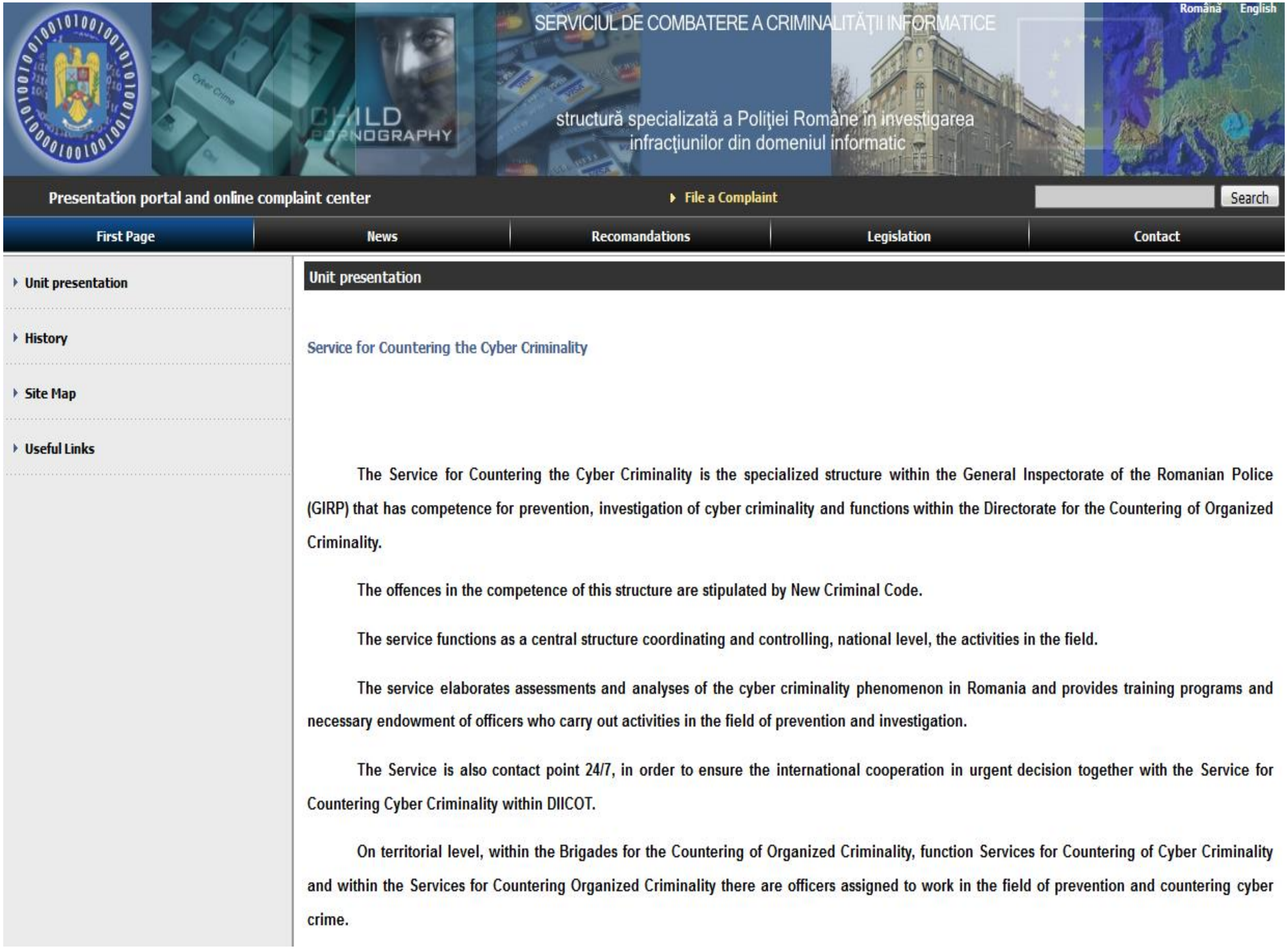
- Recruitment

- Training, staff development
  - Initial training
  - In service training
  - CYBEREX - Centre of excellence in combatting cybercrime

Processes and Procedures

- Image Acquisition
- Digital Forensics Analysis
- Online Child exploitation cases
- Online frauds
- Electronic Payment Frauds
- Cyber attacks

Reporting Platform


Română
English
SERVICIUL DE COMBATERE A CRIMINALITĂȚII INFORMATICE
structură specializată a Poliției Române în investigarea infracțiunilor din domeniul informatic
CHILD PORNOGRAPHY
Presentation portal and online complaint center
File a Complaint
Search
First Page
News
Recomandations
Legislation
Contact
Unit presentation
History
Site Map
Useful Links

Unit presentation

Service for Countering the Cyber Criminality

The Service for Countering the Cyber Criminality is the specialized structure within the General Inspectorate of the Romanian Police (GIRP) that has competence for prevention, investigation of cyber criminality and functions within the Directorate for the Countering of Organized Criminality.

The offences in the competence of this structure are stipulated by New Criminal Code.

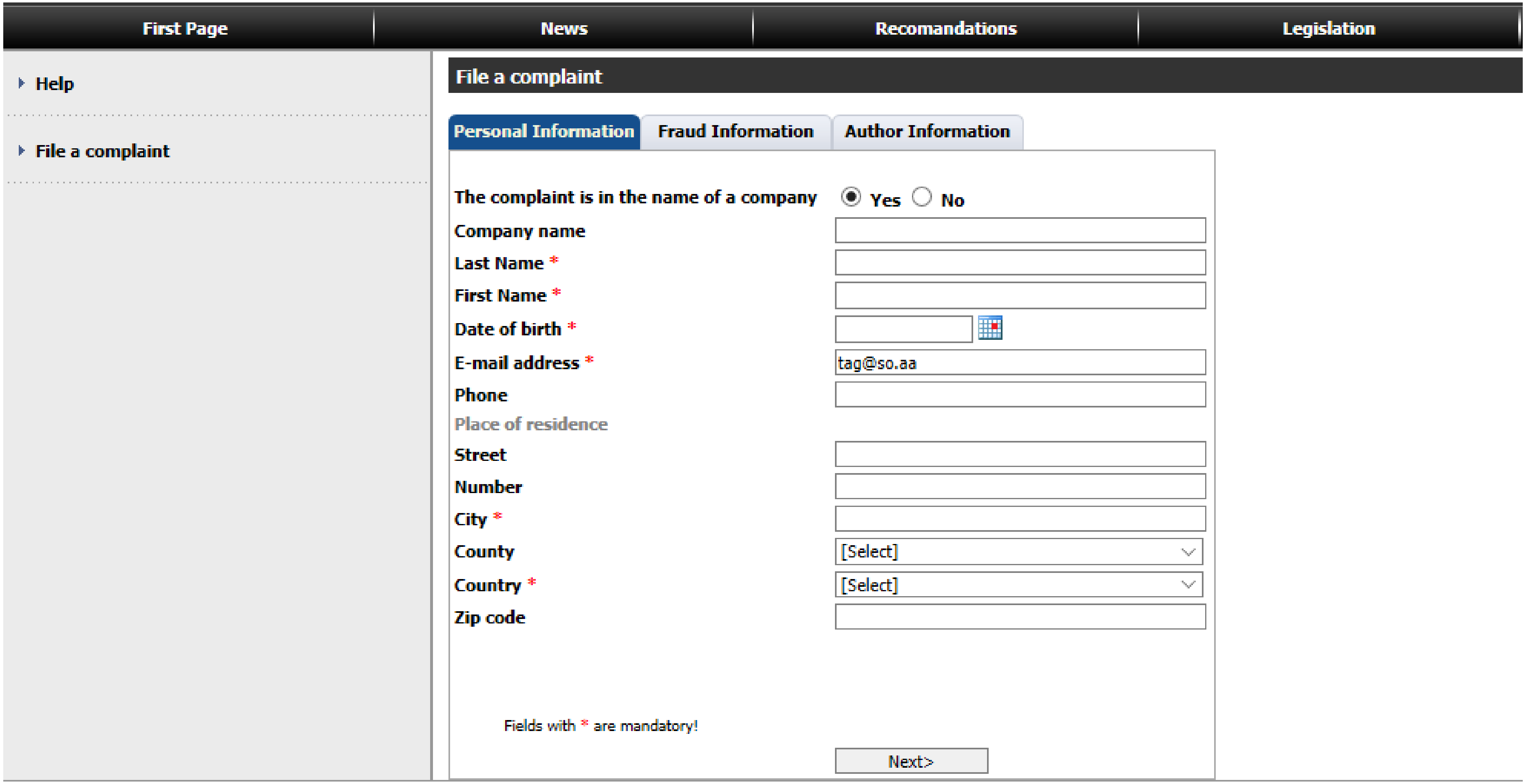
The service functions as a central structure coordinating and controlling, national level, the activities in the field.

The service elaborates assessments and analyses of the cyber criminality phenomenon in Romania and provides training programs and necessary endowment of officers who carry out activities in the field of prevention and investigation.

The Service is also contact point 24/7, in order to ensure the international cooperation in urgent decision together with the Service for Countering Cyber Criminality within DIICOT.

On territorial level, within the Brigades for the Countering of Organized Criminality, function Services for Countering of Cyber Criminality and within the Services for Countering Organized Criminality there are officers assigned to work in the field of prevention and countering cyber crime.

File a complaint



File a complaint

The complaint is in the name of a company	● Yes ○ No
Company name	
Last Name *	
First Name *	
Date of birth *	
E-mail address *	tag@so.aa
Phone	
Place of residence	
Street	
Number	
City *	
County	[Select]
Country *	[Select]
Zip code	

Fields with * are mandatory!

International Cooperation

- Interpol
- Europol
- Liason Officers
- FBI (International Task-force since 2006)
- SELEC Center

Forensic Lab

- Traditional Forensics – image acquisition
- Hardware : Logicube, Tableau, etc

Resources

- **Post Mortem Forensics**

□ EnCase (Windows) http://www.guidancesoftware.com/

□ Internet Evidence Finder (Windows) https://www.magnetforensics.com/magnet-ief/

□ Xways (Windows) http://www.x-ways.net/forensics/

□ FTK (Windows) http://www.accessdata.com/

□ UFed (mobile forensics) http://www.cellebrite.com/home

□ XRY (mobile forensics) http://www.msab.com/xry/what-is-xry

- **Live Data and Network Forensics**

□ Volatility http://www.volatilityfoundation.org

□ Wireshark http://www.wireshark.org/

□ SysInternals http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx

- **Data Interception**

□ Cool Miner Software – processing captured data.

Evidence will be used in Court as part of the case

Public-Private Partnership

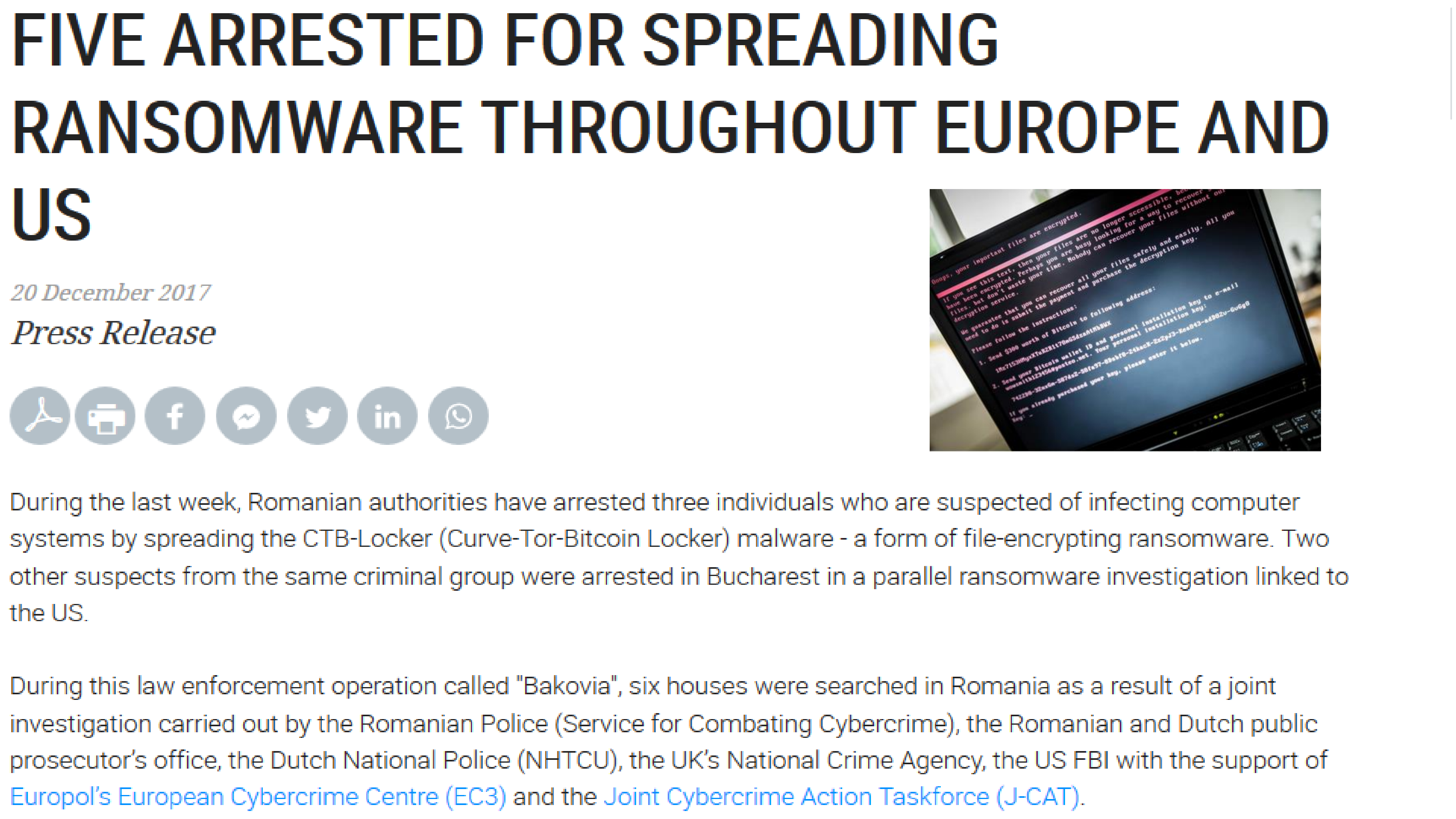
Knowing and building trusted relationships with:

- ITC companies
- Internet Service Providers
- Banking environment (Romanian Banks Association, Wire Transfer Companies, Payment Processors)
- Academia

Lessons Learned

- Partnerships
- Training
- International cooperation
- Legislation
- Strategies/Standards/Procedures

Progress



FIVE ARRESTED FOR SPREADING RANSOMWARE THROUGHOUT EUROPE AND US

20 December 2017

Press Release

During the last week, Romanian authorities have arrested three individuals who are suspected of infecting computer systems by spreading the CTB-Locker (Curve-Tor-Bitcoin Locker) malware - a form of file-encrypting ransomware. Two other suspects from the same criminal group were arrested in Bucharest in a parallel ransomware investigation linked to the US.

During this law enforcement operation called "Bakovia", six houses were searched in Romania as a result of a joint investigation carried out by the Romanian Police (Service for Combating Cybercrime), the Romanian and Dutch public prosecutor's office, the Dutch National Police (NHTCU), the UK's National Crime Agency, the US FBI with the support of Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT).

Thank you for your attention!

Ionut STOICA
Senior Project Officer
Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania
ionut.stoica@coe.int