Ministry of Internal Affairs of the Republic of Moldova
General Inspectorate of Police
National Inspectorate of Investigations
Centre for combating cyber crime

Cyber-threats seen from Moldova

Sibiu, 2015
Market Evolution: Fixed Internet and data transmissions sector

Evolution of Broadband xDSL Subscribers Number, thousand

Evolution of Broadband FTTx Subscribers Number, thousand

Source: http://en.anrceti.md/transpdate
**Market Evolution: mobile Internet access**

Evolution of the number of mobile voice users, who used mobile broadband Internet based on 3G/4G, thousand

The number of Users Accessing Mobile Internet via 4G Networks Increased 34.7% in First Qtr of 2015

Total Internet traffic, generated by dedicated subscribers (TB)

Viruses detected within 7 days

Source: http://cert.gov.md/incidente/statistica-incidentelor.html
Government CERT incidents statistics

![Emails stopped as spam to .gov.md](http://cert.gov.md/incidente/statistica-incidentelor.html)

- **Blocked: Spam**
  - Current: 4699
  - Average: 8644
  - Maximum: 30809
  - Minimum: 1856

![Emails stopped as virus to .gov.md](http://cert.gov.md/incidente/statistica-incidentelor.html)

- **Blocked: Virus**
  - Current: 1
  - Average: 125
  - Maximum: 130
  - Minimum: 0
The Criminal Code of the Republic of Moldova was adopted on 18.04.2002. It included:
- Article 237. Production or putting into circulation of false cards or other pay checks
- Chapter XI. Cyber crimes and crimes in the communications area

On 08.11.2007 article 208/1 „Child pornography” was introduced

On 12.04.2012 the article 175/1 „Berthing children for sexual purposes” (grooming) was introduced

In 2011 there were registered:
- 341 cases of informational frauds in the bank field, causing a loss of 1,088,857 MDL (equal to more than 68,000 EUR)
- 3 cases of child pornography (in one of these cases with sexual abuse of the children, the criminal was convicted with 20 years of imprisonment, with atonement of the sentence in a penitentiary of closed type)

In 2012 there were registered:
- 7,239 cases of informational frauds in the bank field, causing a loss of 13,172,248 MDL (equal to more than 823,000 EUR)
- 6 cases of child pornography

P.S. Average monthly salary in 2011 – 3,000 MDL;
Average monthly salary in 2012 – 3,300 MDL.
Direction for economic frauds investigation of the MIA

Centre for Combating Economic Crimes and Corruption (National Anticorruption Centre)

Centre for combating trafficking in person of the MIA

Crimes related to frauds in banking field

Crimes related to copyrights violation

Crimes related to child pornography and online CSE

No law enforcement unit was specialized in investigating cyber crime
The Reform of the Ministry of Internal Affairs

CCCC was founded on March 5, 2013, after the reform of the MIA, according to the Government Decision nr. 986 of December 24, 2012.
The structure of the Centre for combating cyber crime

Head

Deputy Head,
Head of Strategic Planning Section

Strategic Planning Section
(analysis, strategic planning, capacity building)

Cyber Security Section
(hacking, malware, intellectual property etc.)

Child Protection Section
(child pornography, online abuse and CSE etc.)

Electronic Payment Means Section
(carding, e-payment frauds etc.)

Criminal Prosecution Section
(conducting criminal cases)

Operational Support Service
(first response, examination of computer systems)
Legal base
international treaties

The Council of Europe Convention on Cybercrime,
adopted in Budapest on November 23, 2001,
approved on the February 02, 2009;

The Optional Protocol to the UN Convention on the rights of the Child, on the Sale of Children, Child Prostitution and Child Pornography,
adopted by the UN General Assembly on May 25, 2000,
approved on February 22, 2007;

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote),
adopted on the October 25, 2007,
approved on the December 19, 2011.
Legal base
national legislation

The Constitution of the Republic of Moldova

Criminal procedure code

Law on international legal assistance in criminal matters

Law on electronic communications

The code of offences

Law on preventing and combating cyber crime

Law on the protection of children against the negative impact of information

Government Decision approving the regulation on the import, export, design, production and marketing of special technical means intended to obtain secret information and Classification of special technical means intended to obtain secret information
The Criminal Code:

- art. 175 (Perverted Actions, in the aspect of obscene discussions with the child)
- art. 175/1 (Grooming)
- art. 206 part (1) letter a) (Trafficking in children, for the purpose of commercial or non-commercial sexual exploitation in prostitution or a pornographic industry)
- art. 208/1 (Child pornography)
- art. 208/2 (Resorting to prostitution practiced by a child)
- art. 237 (Production or putting into circulation of false cards or other pay checks)
- art. 259 (Illegal access to computerized information)
- art. 260 (Illegal production, importation, marketing, or offering of technical means or software products)
- art. 260/1 (Illegal interception of an information data transfer)
- art. 260/2 (Violation of the integrity of the information data contained in a data system)
- art. 260/3 (Impact on data system operation)
- art. 260/4 (Illegal production, importation, marketing, or offering of passwords, access codes, or similar data)
- art. 260/5 (Information data forgery)
- art. 260/6 (Information fraud)
- art. 261 (Violation of data system security rules)
- art. 261/1 (Unauthorized access to telecommunication networks and services)

Other cyber related crimes
The Law on payment services and electronic money

The Law was adopted according to:


According to article 5 of the Law, legal persons having the right to provide payment services in the Republic of Moldova are:

a) banks operating under the Law on financial institutions;
b) payment companies;
c) companies issuing electronic money;
d) postal service providers operating under the Law on postal services;
e) the National Bank of Moldova - if does not act as monetary authority or other public authority;
f) the State Treasury.
National cooperation

- National Bank of Moldova
- Customs Service
- General Prosecutor’s office
- Information and Security Service
- Special Communications Centre (Gov)
- Border Police Department
- National center for Child Protection and Assistance
- “LaStrada” Moldova
- National domain registrar
- Ministry of ITC
- The Association of Banks of Moldova
- National Agency for Regulation in Electronic Communications and Informational Technology
International cooperation

OSCE

Department for combating cyber crimes and trafficking in person of Ukraine

International Police Cooperation Centre of the GIP

Department K and Department for combating trafficking in person of Belarus

Department K of Russian Federation

Service for combating cyber crimes of Romania

NCA

24/7 Points of Contact

G8 24/7 NETWORK

International Police Cooperation Centre of the GIP

Council of Europe

Conseil de l'Europe
International cooperation

Centre for combating cyber crime

Exchange of information with the “Interpol” member-states.

Facilitation of information exchange.
Regular assessments that provide thorough and prospective analyses concerning criminality.

International police cooperation center of the GIP

Provide support for Member States and enhance coordination in preventing and combating crime.

Cooperation in investigating serious crimes within the Commonwealth of Independent States.
Article 35 – 24/7 Network

<table>
<thead>
<tr>
<th>A point of contact available on a 24/7 basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>each Party is at liberty to determine where to locate the point of contact</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Immediate assistance for the purpose of investigations or proceedings</th>
</tr>
</thead>
<tbody>
<tr>
<td>criminal offences related to computer systems and data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Facilitating, or directly carrying out:</th>
</tr>
</thead>
<tbody>
<tr>
<td>provision of technical advice</td>
</tr>
</tbody>
</table>
International cooperation

Centre for combating cyber crime

24/7 network - G8

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
International cooperation

What kind of data can be transmitted?
International cooperation
Preservation of stored computer data

- Request for preservation
- Prevention of data alter, removal or delete
- Preparation of request for mutual assistance
- Transmission and execution of request for mutual assistance

Computer data is highly volatile!!!
The need for preserving stored computer data

Computer data contains cyber crime traces

Computer data is stored by the ISPs for only short periods of time

Executing a formal mutual assistance request may take weeks or months
Preservation principles

1. The information provided in the request will be summary and include only the minimum information required to enable preservation of the data.

2. The procedure is protective for the privacy of the person whom the data concerns. 
   (NO DISCLOSURE)

3. Dual criminality not required.

4. Only already stored data can be preserved.

5. Refuse only in case of prejudice to sovereignty, security, public order or other essential interests.
   Or in case of political offense.
Case 1
Cyber attacks

A Manhattan federal court has sentenced the Swedish head of a hacker network to almost five years behind bars for selling a malware program that allowed its buyers to break into victims' computers and spy on them through a web camera.

Alex Yucel, 25, was identified as a co-creator of the Blackshades Remote Access Tool, which has infected half-a-million computers worldwide since the hacker group was established in 2010.

Yucel was arrested in 2013 in Moldova and was the first defendant ever to be extradited to the United States where he pled guilty to computer hacking in February 2015.

The malware was used to gain remote control over a victim’s computer, allowing cybercriminals to get access to private documents and photographs, steal passwords to online accounts, and even activate the victim’s web camera to spy on them.

The malicious program was sold for $40 each. The US Department of Justice estimates that Yucel’s organization earned over $350,000 between September 2010 and April 2014.
Case 2
Forged bank cards

The officers of CCCC documented a criminal group specialized in manufacture and circulation of fake bank cards.

Criminals were making frauds on the territory of the Republic of Moldova and Ukraine over several years.

The operation started with several records of unidentified offenders registered by the ATMs’ camera.

The investigation had shown that the members of the criminal group were renting an apartment in Chisinau, even if they all were living in this city.

According to the data provided by the banks of Moldova, only in 2013 the criminal group put into circulation over 900 fake bank cards and extracted more then 1.5 million lei (about 100,000 Euro).
Case 3
Child pornography

Chief-accountant of a Commercial Centre

Businessman

Magazines publisher

Businessman

Priest
Case 4
On-line CSE in web chats
Challenges

➔ Continuous evolution of criminal activity methods, due to the possibilities offered by the informational technologies;

➔ Lack of equipment and modern technical means;

➔ Cybercrimes committed from the territory of Transnistria, uncontrolled by the constitutional authorities;

➔ Legal barriers.
Electronic payment frauds

Cyber attacks

Online sexual exploitation of children

Other IT crimes
Thank you for attention!

Center for Combating Cyber Crimes
Chisinau
Bucuriei, 14 St.
Tel.: +373 22 57-72-56
e-mail: ccci@mai.gov.md