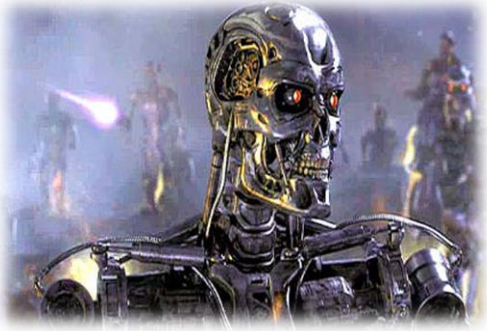
Capacity Building in Ukraine
Cybercrime Division MIA of Ukraine

History of the Division

In 2001 in MIA of Ukraine was created a unit for fighting on high-tech crimes

In 2009 functions for fighting on cybercrime been laid on Department for cybercrime and human trafficking

In December 2011 the Division for combating cybercrime been created



Division for combating cybercrime MIA of Ukraine

Headquarter – 30 employees

27 regional units

Totally - 270 employees

In the headquarter there is a National Contact Point for combatting cybercrime (more then 60 members connected)

December 2013

Structure of the MIA of Ukraine

State Immigration Service (central executive body, coordinated by the Minister)

Main Department of Internal Troops

MINISTER

Minister's Service (Division for Monitoring Human Rights in the law enforcement)

Advisers of the MIA

Main Investigation Department *

Department of Internal Security

Public Relations Department

First Deputy Minister

Deputy Minister - Chief of Staff

Deputy Minister

Personnel Department

Department on Financial Provisions and Accounting

Department on Material Provisions

Department on Medical Service and Rehabilitation

International Relations Department

Internal Audit Department

State Department of Citizenship, Immigration and Registration of Persons (process of liquidation)

Main Headquarters

Department of Informational and Analytical Support

Legal Department

Regime and Secret Department

Documental Provision Department

Special Communication Division

Criminal Militia

Main Department on Combating Organized Crimes

Department of Criminal Investigation

Department on Trafficking in Human Beings

Department of the State Service on Combatting Economic Crimes

Department on Operational Service

Department on Operational and Technical Measures

Department on Combatting Illicit Drug Trafficking

Department on Combatting Cybercrime

Crime Militia Division of work among children

National Central Bureau of Interpol in Ukraine

Public Security Militia

Public Security Department

Department on crime prevention

Department of the State Automobile Inspection

Division of Veterinary Militia

Department of the State Security Service of the MIA

There are 4 units in the Division

E-Commerce and Online-Fraud

Functions of the unit

Fraud, deceit; Illegal commercial activity, gambling; Commercial activity regulations violation; Disrupting legal commercial activity; Theft; …

Illegal Content Distribution and Telecommunications Crimes

Functions of the unit

Fraud, deceit; Illegal commercial activity, gambling; Commercial activity regulations violation; Disrupting legal commercial activity; Theft; …

Intellectual property rights violation; Trademark misusing; Child sexual abuse; correspondence and conversation privacy; Illegal arms trade; Drug trafficking; Violence video; Child and adult pornography; …

Payment Systems Crimes

Functions of the unit

Fraud, deceit; Illegal commercial activity, gambling; Commercial activity regulations violation; Disrupting legal commercial activity; Theft; …

Intellectual property rights violation; Trademark misusing; Child sexual abuse; correspondence and conversation privacy; Illegal arms trade; Drug trafficking; Violence video; Child and adult pornography; …

Carding, other illegal access to bank accounts, illegal financial transactions; Forgery, counterfeiting; Money laundering; …

24-Hour Cybercrime Response

Functions of the unit

Fraud, deceit; Illegal commercial activity, gambling; Commercial activity regulations violation; Disrupting legal commercial activity; Theft; …

Intellectual property rights violation; Trademark misusing; Child sexual abuse; correspondence and conversation privacy; Illegal arms trade; Drug trafficking; Violence video; Child and adult pornography; …

Carding, other illegal access to bank accounts, illegal financial transactions; Forgery, counterfeiting; Money laundering; …

24/7 Point of Contact;

DDOS; Hacking, phishing, id theft; Malware; Botnets; Spam; Illegal traffic routing; Illegal dissemination of classified information; PC, network or system intrusion; …

International cooperation


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION


UNITED STATES
SECRET SERVICE


EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL


МУС


osce


РЕПУБЛИКА БЪЛГАРИЯ НАЦИОНАЛНА


NCA
National Crime Agency


OIPC ICPO
INTERPOL


D.C.P.J.
OFFICE CENTRAL DE LUTTE CONTRE LA CRIMINALITE LIEE AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
OCLCTIC


POLITIE


Bundeskriminalamt

Cooperation with OSCE

Cooperation with OSCE

With the support of OSCE in November 2012 we established the Training Center in the Division for combatting cybercrime of Ministry of Internal Affairs of Ukraine.

Computer Forensics LAB

1. Remote access

2. Copying data

3. Make data inaccessible

Factors of urgency assistance

- cybercrimes take place instantly
- cybercrime traces are quite unstable and easy to destroy
- in the majority of cases, cybercrimes are transnational
- have a high degree of ‘depersonalization’
- cybercrime-related information is limited or completely nonexistent
- determining the time and place of a cybercrime is problematic

Thank You for Your Attention!

Leonid Tymchenko

Deputy Chief
Cybercrime Division
Ministry of Internal Affairs of Ukraine
PhD

+38-097-925-82-88
skype – leonid_tymchenko
tymchenko@cybercrime.gov.ua