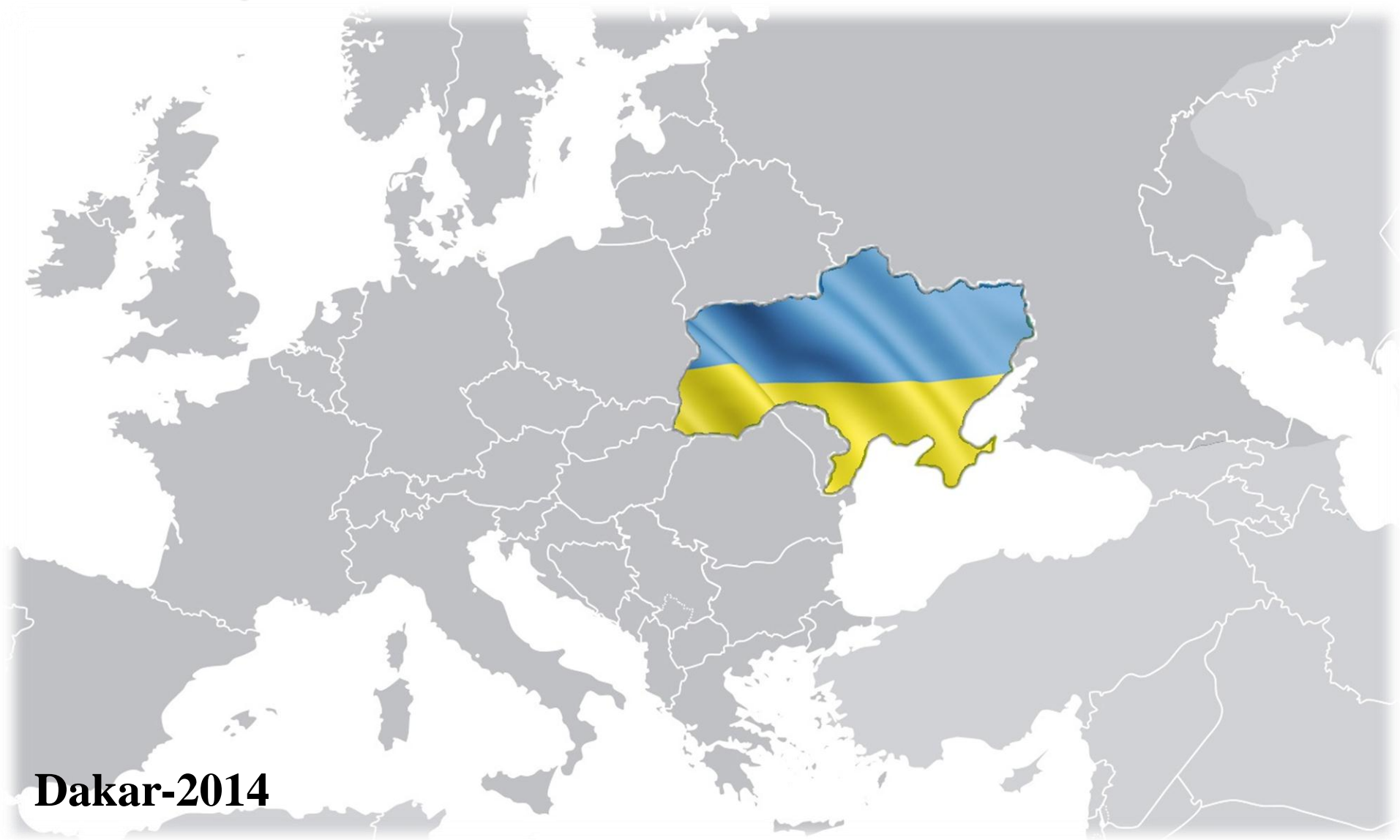




International cooperation

Cybercrime Division MIA of Ukraine



Dakar-2014

Agenda

- History of The Division
- International Cooperation and Capacity Building

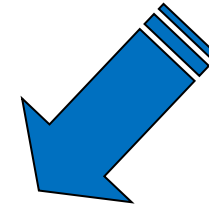


History of the Division

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

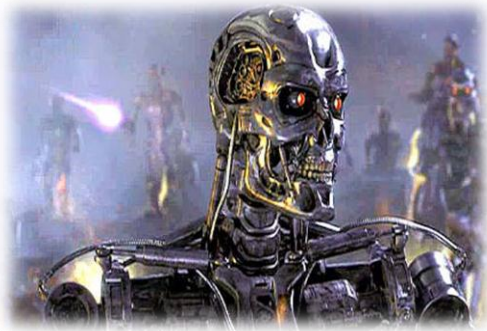


In 2009 functions for fighting on cybercrime been laid on Department for combatting cybercrime and human trafficking



In December 2011 the Division for combating cybercrime been created





Division for combating cybercrime MIA of Ukraine

Headquarter – 30 employees

27 regional units

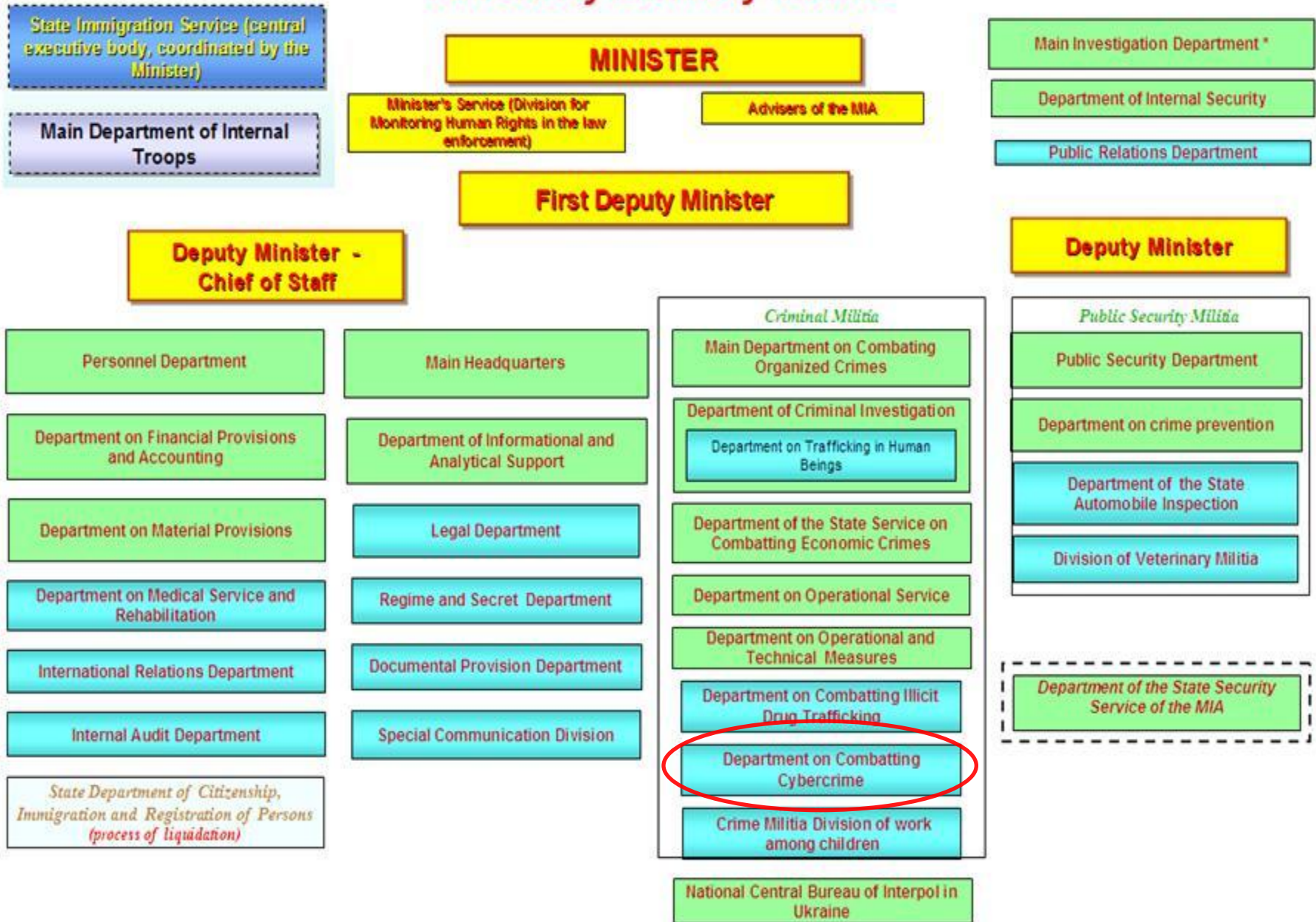
Totally - 270 employees

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



March 2014

Structure of the MIA of Ukraine





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; ...



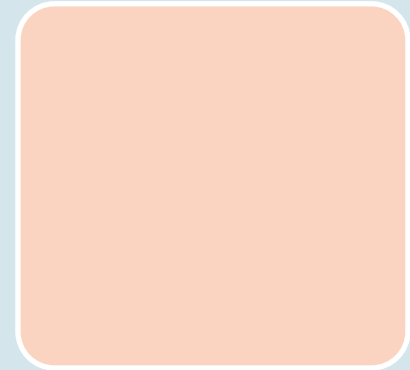


Illegal Content Distribution and Telecommunications Crimes





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





National Bank of
Ukraine



Ukrainian Interbank
Payment Systems
Member Association



FBI



Secret Service



National
Police Agency



BKA

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



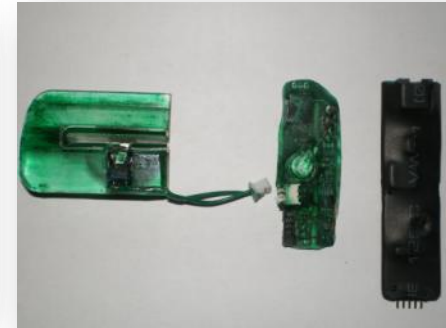
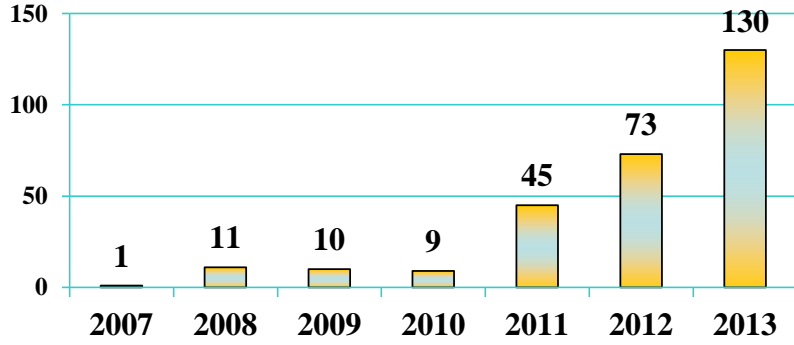
ANONYMOUS

WE ARE LEGION

WE DO NOT FORGIVE WE DO NOT FORGET

Anonymous 'might well be the most powerful organization on Earth'

Skimming





Cambodia

Sri Lanka

Thailand

Recommendations:

- Share best practice;
- Establishment of Contact Points in each country;
- Ongoing training;
- Invite international experts;
- Create and support OUR COMMUNITY...



Thank you for your hospitality!





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