"Bulgarian Law Enforcement Counter Cybercrime Authorities: Structure and Legal Framework"

cybercrime section

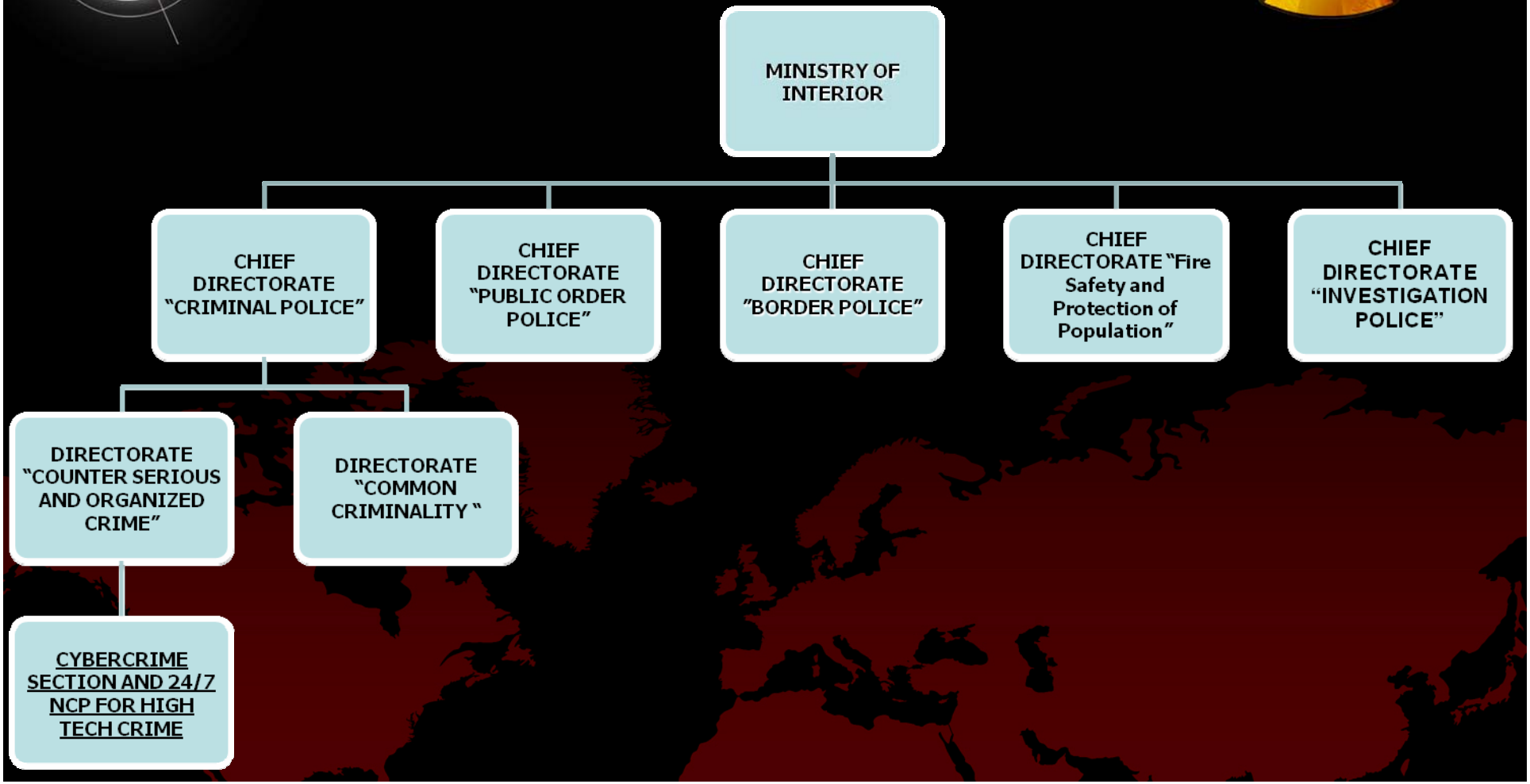
ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS)

7-9 October 2008

Sofia, Bulgaria

STRUCTURE OF THE MINISTRY OF INTERIOR

cybercrime section



FUNCTIONAL STRUCTURE OF CYBERCRIME SECTION AND 24/7 NCP FOR HIGH-TECH CRIMES

cybercrime section

HEAD OF SECTION

UNIT I

"CYBER FRAUDS AND IDENTITY THEFT"

UNIT II

"INTERCEPTION OF ELECTRONIC DATA, ILLEGAL ACCESS, ALTERING AND DESTROYING COMPUTER RELATED DATA, INTRODUCING COMPUTER VIRUSES, DISSEMINATING SYSTEM PASSWORDS

UNIT III

ILLEGAL CONTENT

UNIT IV

"IPR VIOLATIONS"

UNIT V

"INFORMATION AND AND ANALYSIS AND NCP 24/7 FOR HIGH-TEGH CRIME"

Cybercrimes Section
Regional Structures

cybercrime section

THE G8 24/7 NETWORK (MORE 50 COUNTRIES)

cybercrime section

- Provides critical solution for the need of cybercrime investigators to move at unprecedented speeds to preserve electronic data and locate suspects

- Does not replace traditional forms of formal mutual assistance—rather, it facilitates their use for electronic data, such as email traffic that is not permanently stored

- US ISPs: AOL, YAHOO, HOTMAIL

HOW TO USE THE 24/7 NETWORK

cybercrime section

- Law enforcement seeking assistance from a foreign participant may contact the 24-hour point of contact in *their own* state
- That point of contact will, if appropriate, contact his or her counterpart in the foreign participant state where electronic information is located
- If appropriate foreign counterpart will undertake to preserve electronic information under the laws of the foreign state

24/7 MEMBERSHIP COMMITMENT

cybercrime section

- Contact who can be reached 24 hours a day, 7 days a week, to receive information and/or requests for assistance from other countries within the Network.

International Co-operation

cybercrime section

- INTERPOL
- EUROPOL
- 24/7 Contacts for International High-Tech Crime – over a 50 member states
- EU Liaison officers
- FBI and USSS agents in Sofia
- Private sector (BSA, MPA, IFPI, Microsoft, E-bay, Pay-Pal, Citygroup, VISA etc.)

LEGAL FRAMEWORK

cybercrime section

- CONSTITUTION OF REPUBLIC OF BULGARIA
- CONVENTION AGAINST CYBERCRIMES OF COUNCIL OF EUROPE ISSUED ON 23.11.2001

- PENAL CODE
- PENAL PROCEDURE CODE
- MINISTRY OF INTERIOR ACT
- SPECIAL INTELLIGENCE MEANS ACT
- CLASSIFIED INFORMATION PROTECTION ACT
- COPYRIGHT AND ALLIED RIGHTS ACT
- PERSONAL DATA PROTECTION ACT
- ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE ACT
- TELECOMMUNICATIONS ACT
- ELECTRONIC TRADE ACT

Criminal Code

cybercrime section

- Art. 159.
- (1) (Amend., SG 28/82; SG 10/93; SG 62/97) Who produces, exhibits, broadcasts, offers, sells, lends or in any other way circulates works of pornographic contents shall be punished by imprisonment of up to one year and a fine of one thousand to three thousand levs.
- (2) Who exhibits, presents, offers, sells or lends works of pornographic nature to persons under 16 years of age shall be punished by imprisonment of up to three years and a fine of up to five thousand levs.
- (3) For acts under para 1 and 2 the punishment shall be imprisonment of up to five years and a fine of up to eight thousand levs if, for the purposes of creation of the work, was used a minor, underage or a person with such an appearance.

Criminal Code

cybercrime section

- Art. 159.
- (4) When the act under para 1 - 3 has been committed by an errand or in fulfilment of a decision of an organised criminal group the punishment shall be imprisonment of two to eight years and a fine of up to ten thousand levs, as the court may rule confiscation of a part or of the whole property of the offender.
- (5) Who keeps a pornographic work for whose creation a minor, underage or a person with appearance of a minor or underage has been used shall be punished by imprisonment of up to one year or a fine of up to two thousand levs.
- (6) The subject of the crime shall be seized in favour of the state, and if it is missing or has been expropriated its equivalence shall be awarded.

Criminal Code

cybercrime section

Article 171: Who illegally:

1. opens, forges, hides or destroys another's letter, telegram, sealed papers, package or the like;

2. takes another's, although opened, letter or telegram with the purpose of learning their contents or, with the same purpose, submits to somebody else another's letter or telegram;
3. comes to know a message not addressed to him, sent by electronic means or diverts such a message from its addressee.

shall be punished by imprisonment of up to one year or by a fine of one hundred to three hundred levs.

Criminal Code

cybercrime section

- Art. 172a.
- (1) (Amend., SG 62/97) Who records, reproduces, circulates, broadcasts or transmit by a technical device or uses in any other way another's work of science, literature or art, without the consent of the bearer of the copyright required by the law, shall be punished by imprisonment of up to three years and a fine of one thousand to three thousand levs.
- (2) (Amend., SG 62/97) The punishment under para 1 shall also be imposed on those who records, reproduces, circulates, broadcasts or transmit by a technical device or uses in any other way a sound record, video record or radio programme, TV programme, software or computer programme without the necessary consent of the bearer of the copyright required by the law.

Criminal Code

cybercrime section

- Art. 172a.
- (3) (Amend., SG 62/97) If the act under para 1 and 2 has been committed again or substantial harmful consequences have been caused the punishment shall be imprisonment of one to five years and a fine of three thousand levs to five thousand levs.
- (4) For minor cases the perpetrator shall be punished through administrative channels according to the Law for the copyright and its related rights.
- (5) The subject of the crime shall be seized in favour of the state when it belongs to the culprit.

Criminal Code

cybercrime section

Article 212a

- Who, for the purpose of obtaining for himself or for another benefit, excites or maintains deception in somebody by entering, changing, deleting or obliterating computer information data or uses another's electronic signature, thus causing him or someone else damage, shall be punished for computer fraud by imprisonment from one to six years and a fine of up to six thousand levs.
- The same punishment shall be imposed on one who, without having right, enters, changes, deletes or obliterates computer information data in order to obtain something which is not due to him.

Criminal Code

cybercrime section

Article 216

1. Who destroys or damages illegally another's property or real estate shall be punished by imprisonment of up to five years.

2. Who destroys, runs down or damages his mortgaged or pawned property shall be punished by imprisonment of up to five years and a fine of up to two thousand levs.

3. Who, by unwarranted access to a computer of importance for an enterprise, corporate body or individual, destroys or damages another's property, shall be punished by imprisonment of one to six years and a fine of up to ten thousand levs.

Criminal Code

cybercrime section

Article 319a

- Who fulfills unwarranted access to the resources of a computer, copies or uses computer data without permit, when required, shall be punished by a fine of up to three thousand levs.

Article 319b

- Who, without the permit of the person who administers or uses a computer, adds, changes, deletes or destroys a computer programme or data, in significant cases, shall be punished by imprisonment of up to one year or a fine of up to two thousand levs.

Article 319c

- Who commits an act under art. 319b regarding data provided by virtue of a law, by electronic means or on magnetic carrier, shall be punished by imprisonment of up to two years and a fine of up to three thousand levs.

Criminal Code

cybercrime section

Article 319d

- Who introduces a computer virus in a computer or in an information network shall be fined by up to three thousand levs.

Article 319e

- Who circulates computer or system passwords thus causing disclosure of personal data or information representing a state secret shall be punished by imprisonment of up to one year.

Ministry of Interior Act

cybercrime section

Article 55

(1)The police bodies may issue orders to state bodies, organisations, legal entities and citizens whenever necessary for the fulfillment of their assigned functions. The orders shall be given verbally or in writing.

Article 56

(1)The police bodies shall warn verbally or in writing the person about whom there is enough information and it is suspected that he/she will commit a crime or a violation of the public order.

Article 148

(1) The bodies carrying out operative and investigation activity shall issue obligatory orders to state bodies, organisations, legal entities and citizens within the framework of their competence.

Tendencies

cybercrime section

High Technologies Become More Popular In Everyday Life in Bulgaria / 800 000 Internet Access Points in Bulgaria/

The Number Of Cyber Crimes Has Increased

/Mostly Computer Frauds And Crimes Against Intellectual Property/Copyright

THANKS FOR ATTENTION!

cybercrime section

Chief Inspector Yavor Kolev,

Head of Cybercrime Section and 24/7 National Contact Point for High-Tech Crimes

Office phone : +35929828342

Mobile: +359888795021

E-mail : chief@cybercrime.bg

Web site: www.cybercrime.bg

icq 48495113

Skype ID: javor.v.kolev