QUESTIONNAIRE

BULGARIA

Yavor KOLEV

Director of IT and Cyber Security at Lev Ins Insurance Company,

Former Director of Cybersecurity at the Directorate General for Combating Organised Crime

1. Introduction

Please read carefully before answering the questionnaire

The RAYUELA project is aimed at protecting children in their online interactions. For this purpose, the project will develop a "game", which will present the children with realistic scenarios relating to the following cybercrimes/cyber-facilitated crimes:

- ***Online grooming*** (further: OG) is the crime where the perpetrator (usually an adult) uses electronic communication services, including social media, to contact a minor and build rapport with the aim of eventually meeting in person for the purposes of sexual activity. The perpetrator may employ various strategies (deception, romantic/emotional attachment, promise of material or other benefits, blackmail, coercion, etc.) to lower a child's inhibitions, heighten their curiosity about sexual experiences, or otherwise convince them to meet up.
- ***Cyber bullying*** (further: CB) is a broad term that includes all types of bullying behaviour online. This includes cyber stalking and cyber harassment, and any other type of behaviour online aimed at hurting the victim. Cyber bullying may also have a sexual component.
- ***Misinformation and deception*** (further: MD) is a behaviour that may or may not be punishable by law depending on the context. It involves all kinds of information sharing that is fake, or deceptive. For a criminal qualification to apply, typically the behaviour will need to be intentional and there will need to be material consequences to this intention.
- ***Human trafficking with a cyber component*** (further: HT) is the online facilitation of human trafficking by grooming and attracting potential victims for human trafficking.

The purpose of the game is to teach children how to remain safe online, while the obtained insights will be used to provide policy recommendations and educational tools.

The game does not focus solely on the threats of potentially falling victim to one of these four crimes. It also aims to raise awareness about the general threats of using IT, such as the Internet and connected devices, and minors' capacity to make responsible choices in this regard.

A particular point of interest is understanding whether minors are aware of when they, or someone else, is crossing the line in becoming offenders themselves, as this an important aspect of protecting children online. Due to the nature of online communication, inhibitions may be lowered, and certain actions may feel more innocent or less "real" than in real life. In addition, a perception may exist that what happens on the Internet has little or no impact beyond the digital world. This creates situations where minors engage in what they perceive to be relatively innocent behaviour ("everyone does this on the internet"), that may however have serious legal consequences.

One of the goals in RAYUELA is to ensure that minors realize when their behaviour may turn into actions that are punishable by law.

The present study and questionnaire are set up in the context of the RAYUELA project in order to provide an overview of the **legislative framework and relevant policies** in a number of countries, both in the EU and beyond, in relation to:

- How the main crimes of OG, CB, MD and HT are dealt with by the legal system i.e., which behaviours are punishable and under which conditions?
- How cybercrime and cyber-facilitated crime perpetrated by minors is dealt with in the legal system (both in general and specifically in relation to the crimes in focus)?
- What international instruments and cooperation mechanisms are available in dealing with cybercrime perpetrated by minors?

Importantly, we want to know both the legal rules and policies which are implemented in practice, and their effect on the **real enforcement situation**. If you have knowledge about the effects of current policies on crime rates by minors and on the crime rates for OG, CB, MD and HT, this would be of interest.

We are specifically interested in **case law** that illustrates the "why and how" of certain legal rules, principles and policies in practice. Case law will help us illustrate the similarities and differences between jurisdictions and is therefore *essential***.** Please ensure to have a good amount of case law processed in your answers.

In addition, we want input on **international legal instruments and international cooperation** relevant for cybercrime, and in particular for cybercrime perpetrated by minors. What happens when cybercrimes is perpetrated in a cross-border context? What are the legal rules in place for cooperation with authorities from other countries, and how does this work out in practice (issues, problems, etc.)?

Lastly, we are interested in some **statistical information on cybercrime** in your country and cybercrime by minors specifically.

The purpose of this questionnaire is to help you provide this information for your jurisdiction.

2. Questions relating to OG, CB, HT and MD with minors as victims

Question 1: Is online grooming punishable by law in your country?

Answer:

Bulgaria Criminal Code, 1968

Article 155a

(New, SG No. 38/2007, amended and supplemented, SG No. 27/2009, amended, SG No. 26/2010, SG No. 74/2015)

(1) Anyone who, by using information or communication technology or otherwise, discloses or collects information about a person under 18 years of age for the purpose of establishing contact with that person so as to perform molestation, copulation, sexual intercourse, or prostitution, or to create pornographic material, or for the purpose of involvement in a pornographic show shall be punished by imprisonment from one to six years and a fine from BGN 5,000 to BGN 10,000.

(2) The punishment under Paragraph 1 shall also be imposed on anyone who, by using information or communication technology or otherwise, establishes contact with a person under 14 years of age so as to perform molestation, copulation, or sexual intercourse, or to create pornographic material, or for the purpose of involvement in a pornographic show.

Question 2: Is cyberbullying punishable by law in your country? Please take into account a broad understanding of cyberbullying (cyber/online stalking, harassment, sexual harassment)?

Answer:

It depends on whether the cyber harassment affects the components of other crimes as a threat to life under Art. 144, art. 144a, coercion under art. 214 or other corpus delicti:

Art. 144. (1) (Amended, SG No. 28/1982, effective 01.07.1982, amended, SG No. 10/1993, amended, SG No. 62/1982). 1997, amended, SG No. 92/2002, amended, SG No. 26/2010) Whoever threatens another with a crime against his person or property or against the person or property of his relatives and this threat could arouse a well-founded fear of its realization, punishable by up to three years in prison.

(2) (Amended, SG No. 28/1982, effective 01.07.1982, amended, SG No. 10/1993, amended, SG No. 62/1997) ., Amended, SG No. 26/2010) For threatening an official or a representative of the public during or on the occasion of the performance of his service or function, or against a person enjoying international protection, the punishment shall be imprisonment. up to five years.

(3) (Amended, SG No. 62/1997, amended, SG No. 92/2002, effective 01.01.2005, amended, with regard to entry into force, SG No. 1/1997) 26 of 2004, in force from 01.01.2004, amended - SG, iss. 26 in 2010, supplemented - SG, iss. 16 in 2019) If the perpetrator has threatened murder or the act has been committed by a person under Art. 142, para. 2, items 6 and 8, or committed in the conditions of domestic violence, the punishment shall be imprisonment of up to six years.

Art. 144a. (New, SG No. 16/2019) (1) Whoever systematically monitors another and this could arouse a well-founded fear for his life or health, or for the life or health of his neighbors, if the act is not more serious crime, punishable by up to one year in prison or probation.

(2) Monitoring under para. 1 is any conduct of a threatening nature against a specific person, which may be expressed in persecution of the other person, showing the other person that he has been observed, entering into unwanted communication with him through all possible means of communication.

(3) If the act was committed in the conditions of domestic violence, the punishment shall be imprisonment of up to five years.

Article 214

(Amended, SG No. 10/1993, amended and supplemented, SG No. 50/1995)

(1) (Amended, SG No. 62/1997) A person who, for the purpose of procuring material benefit for himself or for another, by force or threat; compels somebody to do, to fail to do or to suffer something contrary to his will, and thereby inflicts material damage to that person or to another, shall be punished for blackmail by imprisonment for one to six years and a fine from BGN 1,000 to 3,000, whereas the court may impose confiscation of up to 1/2 of the property of the perpetrator.

(2) (Amended, SG No. 62/1997) For blackmail as per Article 213a, paragraphs (2), (3) and (4) the punishment shall be:

1. under paragraph (2) - imprisonment for two to ten years and a fine from BGN 4,000 to 6,000, whereas the court may rule confiscation of up to 1/2 of the property of the perpetrator;

2. under paragraph (3) - imprisonment for five to fifteen years, a fine from BGN 5,000 to 10,000 and confiscation of up to 1/2 of the property of the perpetrator;

3. (amended, SG No. 153/1998) under paragraph (4) - imprisonment for fifteen to twenty years, life imprisonment or life imprisonment without a chance of commuting and confiscation of no less than 1/2 of the perpetrator's property.

(3) For blackmail the punishment shall be imprisonment for five to fifteen years and a fine from up to BGN 500, whereas the court may rule confiscation of up to one half of the property of the culprit, provided that:

1. it has occurred together with severe or medium bodily injury;

2. the act constitutes a case of dangerous recidivism

Question 3: When would misinformation and deception online constitute a criminal offence in your country? In other words, what potential qualifications could apply to wilful misinformation and deception on the internet?

Answer:

Article 209

(1) (Amended, SG No. 28/1982, SG No. 10/1993, SG No. 26/2010) A person who for the purpose of acquiring material benefit for himself or for another evokes or maintains in somebody a misleading idea, and thereby causes material damage to that person or to another, shall be punished for deceit by imprisonment from one to six years.

(2) (Amended, SG No. 10/1993, SG No. 26/2010) A person who for the same purpose takes advantage of the misleading ideas, the inexperience or the lack of information of another and causes thereby material damage to that person or to another, shall be punished by imprisonment for up to five years.

(3) In minor cases under the preceding paragraphs, the punishment shall be imprisonment for up to one year, or probation.

Article 212a

(New, SG No. 92/2002)

(1) (Amended, SG No. 38/2007) Where an individual, in view of providing a benefit to him-/herself or another, brings or maintains misleading representations in someone through introducing, modifying, deleting, or erasing computerized data or through the use of an electronic signature of another causes him/her or another harm, shall be punished for computer fraud by imprisonment from one to six years and a fine from up to BGN 6,000.

(2) (Amended, SG No. 38/2007) The same form and amount of punishment shall be imposed to the individual who, without being entitled thereto, introduces, modifies, or erases computerized data in order to unduly obtain something, that should not go to him.

Question 4: What constitutes human trafficking and how is human trafficking facilitated by electronic means punished in your country? Are online grooming activities to find victims (e.g. lover boys) before the actual human trafficking punishable in itself? In addition, are these activities punishable as a separate crime if human trafficking does take place afterward?

Answer:

Section IX (New, SG No. 92/2002) Trafficking of People

Article 159a

(1) (Amended, SG No. 27/2009, SG No. 84/2013) An individual who recruits, transports, hides or admits individuals or groups of people in view of using them for sexual activities, forced labour or begging, dispossession of a body organ, tissue, cell or body fluid or holding them in forceful subjection, regardless of their consent, shall be punished by imprisonment of two to eight years and a fine from BGN three thousand to twelve thousand.

(2) Where the act under Paragraph 1 has been committed:
1. with regard to an individual who has not turned eighteen years of age;
2. through the use of coercion or by misleading the individual;
3. through kidnapping or illegal imprisonment;
4. through abuse of a status of dependency;
5. through the abuse of power;
6. through promising, giving away or receiving benefits;
7. (new, SG No. 84/2013) by an official during or in connection with the fulfilment of

his/her official duties,
(amended, SG No. 27/2009) punishment shall be imprisonment from three to ten years and

a fine from BGN ten thousand to twenty thousand.
(3) (New, SG No. 75/2006, amended, SG No. 27/2009) Where the act under para 1 has

been committed in respect to a pregnant woman to the purpose of selling her child, the punishment shall be imprisonment from three to fifteen years and a fine from BGN twenty thousand to fifty thousand.

Article 159b

(1) (Amended, SG No. 27/2009) An individual who recruits, transports, hides or admits individuals or groups of people and guides them over the border of the country with the objectives under Article 159a, Paragraph 1, shall be punished by imprisonment from three to twelve years and a fine of up to BGN 10,000 to 20,000.

(2) (Supplemented, SG No. 75/2006, amended, SG No. 27/2009) Where the act under Paragraph 1 has been committed in presence of characteristics under Article 159a, Paragraph 2 and 3, the punishment shall be imprisonment from five to twelve years and a fine from BGN twenty thousand to fifty thousand.

Article 159c

(New, SG No. 27/2009, amended, SG No. 84/2013)

A person who takes advantage of a person who suffered from human trafficking for acts of debauchery, forced labour or begging, dispossession of a body organ, tissue, cell or body fluid or holding him in forceful subjection, regardless of his consent shall be punished by imprisonment from three to ten years and a fine from BGN ten thousand to twenty thousand.

Article 159d

(Previous text of Article 159c, amended, SG No. 27/2009)
Where acts under articles 159a - 159c qualify as dangerous recidivism or have been

committed at the orders or in implementing a decision of an organized criminal group, the punishment shall be imprisonment from five to fifteen years and a fine from BGN twenty thousand to one hundred thousand, the courts being also competent to impose confiscation of some or all possessions of the perpetrator.

Questions regarding cybercrime or cyber-facilitated crime committed by minors

Question 5: How is crime committed by minors dealt with in your country, in general? Is there a specific juvenile justice system? If yes, please explain in detail how this works.

Answer:

Section III
Release from Penal Responsibility of Underage Persons with Application of Educational Measures

Article 78

In the cases indicated in Article 61 the underage person may be released from penal responsibility by applying an appropriate educational measure.

Chapter Six
SPECIAL RULES FOR UNDERAGE PERSONS

Article 60

Punishment shall be imposed on underage persons above all with the objective to

re-educate and prepare them for socially useful work.

Article 61

(1) (Amended, SG No. 89/1986, SG No. 75/2006) With respect to an underage person who has committed a crime carried away by circumstances or because of thoughtlessness, which does not constitute great social danger, the prosecutor may decide to abstain from instigating pre-trial proceedings or to terminate the instigated proceedings, and the court may decide not to have him brought to court or not to have him tried, provided with regard to him educative measures can successfully be applied pursuant to the Control of Juvenile Anti-Social Behaviour Act.

(2) In such cases the court itself may impose an educative measure, informing thereof the local Commission Against Anti-Social Acts of Minors and Underage Persons, or forwarding thereto the court file for imposition of such a measure.

(3) (Amended, SG No. 89/1986, SG No. 107/1996, SG No. 26/2004, SG No. 75/2006) Where the prosecutor decides not to institute pre-trial proceedings or to put an end to pre-trial proceedings which have been formed, he shall send the case-file to the Commission, which shall impose a measure of education.

Article 62

Imposed on underage persons may be only the following punishments:
1) imprisonment;
1a) (new, SG No. 92/2002 - effective 1.01.2005 with respect to the punishment of

probation - amended, SG No. 26/2004, effective 1.01.2004, SG No. 103/2004) probation; 2) public censure;

3) (amended, SG No. 103/2004) deprivation of the right to exercise certain vocation or activity under Article 37. Paragraph 1, sub-paragraph 7.

Article 63

(1) For underage persons the punishments provided in the Special Part of this Code shall be a chance of commuting as follows:

1) (supplemented, SG No. 50/1995, amended, SG No. 153/1998) life imprisonment without substitution and life imprisonment - for imprisonment for a term of from three up to ten years;

2) imprisonment for more than ten years - for imprisonment for a term of up to five years;

3) imprisonment for more than five years - for deprivation of liberty for a term of up to three years;

4) imprisonment for a term of up to five years inclusive - for imprisonment for a term of up to two years, but not more than as provided by the law;

5) (amended, SG No. 92/2002 - effective 1.01.2005 - amended, SG No. 26/2004, effective 1.01.2004, SG No. 103/2004, SG No. 75/2006) fine - for public censure;

6) (new, SG No. 92/2002 - effective 1.01.2005 with respect to the punishment of probation - amended, SG No. 26/2004, effective 1.01.2004) probation for juveniles below 16 years of age - for public censure.

(2) (Amended, SG No. 28/1982) For underage persons who have turned sixteen years of age, the punishments provided in the Special Part of this Code shall be substituted as follows:

1) (supplemented, SG No. 50/1995, amended, SG No. 153/1998) life imprisonment without a chance of commuting and imprisonment for more than fifteen years - for imprisonment for a term of five to twelve years;

2) imprisonment for more than ten years - for imprisonment for a term of two to eight

years.
(3) (Amended, SG No. 28/1982) Within the limits of the preceding paragraphs, the court

shall determine the punishment in compliance with the provisions of Chapter Five hereof.

Article 64

(1) (Amended, SG No. 107/1996) Where the punishment as determined is imprisonment for less than one (1) year and its serving has not been suspended pursuant to Article 66, the underage convict shall be exempted from serving it and the court shall assign him to a correctional boarding school or shall impose on him another educational corrections measure provided by the Control of Juvenile Anti-Social Behaviour Act.

(2) (Amended, SG No. 107/1996) Upon the proposal of the prosecutor or the respective local Commission Against Anti-Social Acts of Minors and Underage Persons, the court may also, after pronouncement of the sentence, substitute the commission to a correctional boarding school for another educational corrective measure.

(3) The rule of paragraph (1) shall not apply: a) where the underage convict has committed a crime during the serving of punishment by deprivation of liberty, and b) where he has been convicted after completing full age.

(4) The rule of paragraph (1) shall not be applied also in cases of second conviction, provided the court finds that for the correction and re- education of the perpetrator it is necessary for him to serve the sentence of imprisonment and where: a) the term is not less than six months, or b) the perpetrator has already served a punishment by imprisonment.

Article 65

(1) Before reaching full age underage persons shall serve punishments by imprisonment in reformatory establishments.

(2) (Amended, SG No. 75/2006) After reaching full age they shall be transferred to prison or prison hostel. In view of completing their education or vocational training, upon the proposal of the Pedagogical Council and with permission of the prosecutor, they may be admitted to reformatory establishment until completion of twenty years of age.

Question 6: Are there specific rules or is there a specific policy that deals with cybercrime by minors as a special topic, acknowledging the special characteristics of crime by minors in the cyber environment, and the fact that minors may not knowingly or intentionally break rules (issues with criminal intent)? Even absent a written policy, are minors prosecuted for cybercrime in practice?

Answer:

The provisions in the answer to question 5 apply. There are no specifics in the case of a cybercrime committed by a minor. A crime is a crime, it doesn't matter that it's a computer crime.

Question 7: Can minors be punished for online grooming in your country? I.e. the situation of a minor capable of providing sexual consent (e.g. 17 year-old) grooming a minor who has not reached the age of sexual consent (e.g. 13 years old) to meet up with the intent to perform sexual

activities? Please focus not only on the specific crime of online grooming (which, if present as a separate crime in your jurisdiction, often requires an adult perpetrator), but also on other crimes that would punish the activities that constitute online grooming (i.e. the use of different strategies to force a meeting with the minor victim with the intent to perform sexual activities). If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

The provisions in the answer to question 5 apply. There is usually no prosecution of minors.

Question 8: Can minors be punished for purely online behaviour with a sexual intent when other minors are the victim? E.g. the situation where a minor perpetrator obtains sexually explicit material from the minor victim in order to sell this or to force the victim to do something. If criminal sanctions could apply, are minors prosecuted in practice?

Answer: .

The provisions in the answer to question 5 apply. There is usually no prosecution of minors

Question 9: Can minors be punished for cyberbullying behaviour, without there being a physical component to the crime? This includes behaviours such as cyberstalking and cyberharassment. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

The provisions in the answer to question 5 apply. There is usually no prosecution of minors.

Question 9: Can minors be punished for wilful misinformation or deception online (sharing false news, false information, pretending to be someone else, pretending to be an expert, etc.)? Which crimes/qualifications could possibly apply? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Article 212a

(New, SG No. 92/2002)

(1) (Amended, SG No. 38/2007) Where an individual, in view of providing a benefit to him-/herself or another, brings or maintains misleading representations in someone through introducing, modifying, deleting, or erasing computerized data or through the use of an electronic signature of another causes him/her or another harm, shall be punished for computer fraud by imprisonment from one to six years and a fine from up to BGN 6,000.

(2) (Amended, SG No. 38/2007) The same form and amount of punishment shall be imposed to the individual who, without being entitled thereto, introduces, modifies, or erases computerized data in order to unduly obtain something, that should not go to him.

The provisions in the answer to question 5 apply. There is usually no prosecution of minors.

Question 10: Can minors be punished for online actions facilitating human trafficking? Typically this includes the selection and grooming of victims (e.g. lover boy phenomenon). If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Section III Complicity

(1) Accomplices in the perpetration of intentional crime shall be: perpetrators, abettors and accessories.

(2) A perpetrator shall be a person who took part in the perpetration itself of the crime.
(3) An abettor shall be a person who intentionally incited another to commit a crime.
(4) An accessory shall be a person who intentionally facilitated the perpetration of a crime

through advice, explanations, promises to render assistance after the act, removal of obstacles, supply of means or in any other way.

Article 21

(1) All accomplices shall be punished by the punishment provided for the perpetrated crime, with due consideration of the nature and degree of their participation.

(2) Abettors and accessories shall be held responsible only for what they have intentionally abetted or by what they have assisted the perpetrator.

(3) Where because of certain personal characteristics or attitude of the perpetrator the law treats the perpetrated act as a crime, liable for this crime shall be both the abettor and the accessory with respect of whom such circumstances do not exist.

(4) The special circumstances, due to which the law excludes, reduces or increases the punishment for some of the accomplices, shall not be taken into account for the remaining accomplices with respect to whom such circumstances do not exist.

Article 22

(1) The abettor and the accessory shall not be punished, if of their own accord they have given up further participation and hindered the perpetration of the act or averted the occurrence of criminal consequences.

(2) In such cases the provisions of Article 19 shall apply, respectively.

The provisions in the answer to question 5 apply. There is usually no prosecution of minors.

Question 11: Can minors be punished for acts of online piracy in your jurisdiction, i.e. the illegal use and/or distribution of content protected by intellectual property rights? Please focus on the elements of criminal nature. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Section VII
Crimes Against Intellectual Property (Title amended, SG No. 50/1995)

Article 172a

(New, SG No. 50/1995)

(1) (Amended, SG No. 62/1997, SG No. 75/2006) A person who makes records, reproduces, distributes, broadcasts or transmits, or makes any other use the object of a copyright

or neighbouring right without the consent of the owner of holder of such right as required by law, shall be punished by imprisonment for up to five years and a fine from up to BGN 5,000.

(2) (Amended, SG No. 62/1997, SG No. 75/2006) Anyone who, without consent from the person required by law, detains material carriers containing the object of copyright or a neighbouring right, amounting to a large-scale value, or who detains a matrix for the reproduction of such carriers, shall be punished by imprisonment from two to five years and a fine from BGN 2,000 to 5,000.

(3) (Amended, SG No. 62/1997, SG No. 75/2006) If the act under Paragraphs (1) and (2) has been repeated or considerable damaging consequences have occurred, the punishment shall be imprisonment from one to six years and a fine from BGN 3,000 to 10,000.

(4) (New, SG No. 75/2006) Where the act under Paragraph 2 amounts to a particularly large-scale value, the punishment shall be imprisonment from two to eight years and a fine from BGN 10,000 to 50,000.

(5) (Renumbered from Paragraph 4, SG No. 75/2006) For minor cases the perpetrator shall be punished under the administrative procedure in compliance with the Copyright and Neighbouring Rights Act.

(6) (Renumbered from Paragraph 5, amended, SG No. 75/2006) The object of the crime shall be appropriated in favour of the state, irrespective of the fact whose property it is.

Article 172b

(New, SG No. 75/2006)

(1) Anyone who, without consent from the owner of the exclusive right thereupon, makes use in commercial operations of a trademark, industrial model, a variety of plant or race of animal, making the object of said exclusive right, or makes use of a geographical indication or a counterfeit thereof without a legal justification, shall be punished by imprisonment of up to five years and a fine from up to BGN 5,000.

(2) Where the act under Paragraph 1 is repeated or significant damages have been caused, the punishment shall be imprisonment from five to eight years and a fine from BGN 5,000 to BGN 8,000.

(3) The object of the crime shall be taken to the benefit of the state, irrespective of the fact whose property it is, and it shall then be destroyed.

Article 173

(1) (Amended, SG No. 10/1993) A person who publishes or uses under his own name or under a pen name the work of another person in the field of science, literature or arts or a considerable part thereof, shall be punished by imprisonment for up to two years or by a fine from BGN one hundred to three hundred

(2) (Amended, SG No. 81/1999) By the same punishment shall also be punished the person who presents for registration or registers in his own name invention, workable model or industrial design of another person.

Article 174

(Amended, SG No. 10/1993, SG No. 81/1999)

A person who, by abusing his official position, gets himself included as a co-author of an invention, workable model or industrial design or of a work of science, literature or arts, without having taken part in the creative work for its elaboration, shall be punished by imprisonment for up to two years or by a fine from BGN one hundred to three hundred, as well as by public censure.

The provisions in the answer to question 5 apply. There is usually no prosecution of minors.

Question 12: Can minors be punished for acts of hacking (i.e. unauthorized access to a computer system)? In particular, would this also apply to various scenarios exploiting vulnerabilities in IoT and connected devices? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Main article for hacking is article 319a.

The provisions about minors in the answer to question 5 apply. There is usually no prosecution of minors.

Chapter Nine "A" (New, SG No. 92/2002) Cybercrime

Article 319a

(1) (Amended, SG No. 38/2007) Anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required, shall be punished by a fine from up to BGN 3,000.

(2) Where the act under Paragraph 1 has been committed by two or more people, who have previously agreed so to do, the punishment shall be imprisonment of up to one year or a fine from up to BGN 3,000.

(3) (Supplemented, SG No. 38/2007) Where the act under Paragraph 1 is repeated or is with regard to data for creation of an electronic signature, the punishment shall be imprisonment of up three years or a fine of up to BGN 5,000.

(4) (Amended, SG No. 26/2004, supplemented, SG No. 38/2007) Where acts under paragraphs 1 - 3 have been committed with regard to information that qualifies as a secret of the State or to another information protected by the law, the punishment shall be imprisonment from one to three years, unless severer punishment has been envisaged.

(5) Where grave consequences have occurred as a result of the acts under Paragraph 4, punishment shall be of one to eight years.

Article 319b

(1) (Amended, SG No. 38/2007) Anyone who, without consent by a person administering or using a computer system, installs, modifies, deletes or destroys a computer program or computer data, where the occurrence is not considered insignificant, shall be punished by imprisonment of up to one year or a fine from up to BGN 2,000.

(2) Where significant damage or other grave consequences have occurred as a result of an act under Paragraph 1, the punishment shall be a imprisonment of up to two years and a fine from up to BGN three thousand.

(3) Where the act under Paragraph 1 has been committed in view of obtaining a material benefit, the punishment shall be imprisonment from one to three years and a fine from up to BGN 5,000.

Article 319c

(1) (Supplemented, SG No. 38/2007) Anyone who commits the act under art. 319b with regard to data that are provided electronically or upon magnet, electronic, optic or other carriers by virtue of the law shall be punished by imprisonment of up to two years and a fine from up to BGN 3,000.

(2) Where the act under Paragraph 1 was intended to prevent the fulfilment of an obligation, the punishment shall be imprisonment of up to three years and a fine from up to BGN 5,000.

Article 319d

(1) (Amended, SG No. 38/2007) Anyone who introduces a computer virus in a computer system or in a computer network, shall be punished by a fine of up to BGN three thousand.

(2) (New, SG No. 38/2007) The punishment under Paragraph 1 shall be imposed also on that person who introduces another computer program which is intended to disrupt the work of a computer system or a computer network or to discover, erase, delete, modify or copy computer data without permission, where such is required, as long as it is not a graver crime.

(3) (Renumbered from Paragraph 2 and amended, SG No. 38/2007) Where considerable damage has occurred as a result of the act under paras. 1 and 2 or it has been repeated, the punishment shall be imprisonment of up to three years and a fine from up to BGN 1,000.

Article 319e

(1) (Amended, SG No. 26/2004, SG No. 38/2007) Anyone who discloses passwords or codes for access to a computer system or to computer data, and personal data or information which qualifies as secret of the State or another secret protected by the law are thus revealed, shall be punished by imprisonment of up to one year.

(2) (Supplemented, SG No. 38/2007) With regard to an act under Paragraph 1, committed with a venal goal in mind, or where it has caused considerable damage or other grave consequences have occurred, punishment shall be imprisonment of up to three years.

Article 319f

(Amended, SG No. 85/2017) Where a provider of information services acting in this capacity violates provision of Article 6, Paragraph 2, sub-paragraph 5 of the Electronic Document and Electronic Trust Services Act, he/she shall be punished by fine of up to BGN five thousand, unless subject to severer punishment.

General questions regarding cross border cybercrime, international legal instruments applicable to fighting cybercrime and regarding international cooperation

Question 13: How does your country deal with the cross-border nature of many cybercrimes? When is jurisdiction established? Can judgements have extra-territorial effect?

Answer:

When it comes to cybercrime there is almost always a cross – border activities.

We use 24/7 National Contact Point for preservation of information/computer data on Budapest Convention, 2001.

The act committed must be a crime in the relevant jurisdictions where it was committed.

The institutes of requesting MLA /mutual legal assistance/ or a European investigation order are used.

Question 14: What international legal instruments (bi-lateral, multi-lateral) apply in your country to the fight against (cross-border) cybercrime and how have they been implemented in national law (if implementation is necessary)?

Answer:

Budapest Convention from 2001 is implemented at national law in 2006.

The institutes of requesting MLA /mutual legal assistance/ or a European investigation order are used when it comes to prosecutors' activities.

Police use Europol and Interpol channels for information exchange.

Question 15: What forms of international cooperation exist in your country to the fight against cross-border cybercrime? Please describe different routes/options/procedures and the measures that can be requested (e.g. asking for investigative actions, exchange of information/evidence, etc.)?

Answer:

Applicable forms of international cooperation are the following:

The institutes of requesting MLA /mutual legal assistance/ or a European investigation order are used when it comes to prosecutors' activities. Eurojust.

Police use Europol and Interpol channels for information exchange.

Question 16: Do the rules (national, international) and policies mentioned in your answers in this section have any particular effect or impact on cybercrime committed by minors?

Answer:

When we talk about crimes committed by minors, the legal provisions for minors apply:

The provisions about minors in the answer to question 5 apply. There is usually no prosecution of minors.

Other

Question 17: Do you have any information on the rates/statistics of cybercrime in your country and their recent evolution? Of particular interest would be statistics related specifically to the

crimes covered in this questionnaire and statistics on cybercrime by minors (ideally also specifically for the crimes covered above)? If there were any (relatively) recent legislative or policy changes, please try to find statistical information on how this has impacted the incidence of cybercrime in practice, and in particular cybercrime by minors.

Answer:

Legislative changes are forthcoming to increase the number of penalties for computer crimes and crimes committed through computer networks and systems, whose penalties are up to 5 years in prison. When the sentences become more than 5 years of imprisonment, the crimes become severe and special intelligence tools / wiretapping, surveillance, etc./ means can be used for them. Currently, some of the computer crimes from Bulgarian Criminal Code are minor and this don't allow the use of a special intelligence tools for investigating them.

Question 18: Do you have any other comments to make that may be relevant to your jurisdiction?

Answer:

Local legislation is being updated, in most cases trying to follow the European example and progress.