FIGHT AGAINST CYBERCRIME IN SERBIA

Achievements and Challenges

Marija Pavlović
Belgrade Centre for Security Policy

Belgrade, May 2022

prEUgovor
policy paper

B | T | D The Balkan Trust for Democracy
A PROJECT OF THE GERMAN MARSHALL FUND

Norway

FIGHT AGAINST CYBERCRIME IN SERBIA

Achievements and Challenges

Marija Pavlović
Belgrade Centre for Security Policy

Belgrade, May 2022

FIGHT AGAINST CYBERCRIME IN SERBIA
ACHIEVEMENTS AND CHALLENGES

Publisher
For the prEUgovor coalition:

Belgrade Centre for Security Policy
Đure Jakšića 6/5, Belgrade
www.bezbednost.org

Transparency Serbia
Palmotićeva 31/III Belgrade
www.transparentnost.org.rs

Author
Marija Pavlović (Belgrade Centre for Security Policy)

Translation
Alisa Radić

Design and layout
Jelena Pejić Nikić

ISBN-978-86-84711-54-2

The publication is published as part of the project *PrEUgovor for Rule of Law and EU integration of Serbia* supported by Balkan Trust for Democracy, a project of the German Marshall Fund of the United States and the Royal Norwegian Embassy in Belgrade. Opinions expressed in this publication do not necessarily represent those of the abovementioned donors, or its partners.

Introduction

Official statistics indicate an increasing trend in the number of cybercrime (CC) cases in Serbia. According to the Report of the National Centre for the Prevention of Security Risks in Information and Communication (ICT) Systems (National CERT), there have been about 26 million cyber attacks on ICT systems of particular significance in Serbia in 2020, of which the most common group of incidents involved attempted intrusions into ICT systems and unauthorised data collection.[1] Since the beginning of 2022, there have been several attempts to commit Internet fraud and steal the identities and data of users of the Raiffeisen Bank and the Post of Serbia. Threats to journalists via social networks have also become more frequent. The last in the series was the case of mass reports, via e-mail, about bombs planted in various public and private institutions such as hospitals, schools, airports, railway stations, shopping malls, zoological garden and so on. Although the competent authorities have established that the reports were false, they caused worries in the society and temporarily disabled the regular work of the affected institutions.

Cyber attacks have become part of our daily lives and it can be expected that threats made through the Internet and social networks will intensify and become more complicated in the future, which is why it is important that state authorities be prepared to respond to any challenge, risk and threat quickly and effectively, while simultaneously respecting human rights and the rule of law. Cooperation between the state authorities of Serbia and other countries and international organisations such as INTERPOL and EUROPOL will be essential due to the anonymity of the attackers and the cross-border nature of this form of crime.

The Belgrade Centre for Security Policy deals with the topic of cybercrime from the point of view of Serbia's accession negotiations with the European Union and monitoring the progress in Cluster 1 (Basics), i.e. Chapter 24 (Justice, Freedom, Security). In this context, we will present the achievements in the legal and institutional development of the competent authorities in the fight against cybercrime, i.e. the analysis of current trends and challenges in the fight against this type of crime in Serbia.

[1] Attacks on ICT systems are recorded in N-CERT, for the statistical purposes and for the purpose of possible gathering of evidence, while the MoI's Special Prosecutor's Office and the Department for the Suppression of CC are in charge of prosecuting attackers. The same provisions from Chapter 27 of the Criminal Code apply to them.

Legal and Institutional Framework

Legal Framework

The legal framework for the fight against CC has existed in Serbia since 2005, when, after the signing of the Convention on Cybercrime of the Council of Europe (the Budapest Convention), a special Law defined the concept and competencies of state authorities to fight this form of crime.[2] In order to harmonise its legislation with the strategic and operational approach of the European Union in this area, the Government of Serbia has adjusted the regulations by making partial targeted changes to certain laws, namely the Criminal Code and the Criminal Procedure Code. The Criminal Code, which entered into force in 2005, contained Chapter 27, entitled "Criminal Offence against Security of Computer Data", which included cybercrimes. Amendments to the Law on the Organisation and Competence of State Authorities in the Fight against High-Tech Crime and the Criminal Code were adopted after the ratification of the Budapest Convention in 2009.

As for the high-tech criminal acts prescribed in the Criminal Code, they can be conditionally divided into two groups – those that concern only cybercrime, and those that have elements of cyber-crime, but do not fall exclusively within the competence of bodies specialised in combating cybercrime (see below). The first group includes 8 crimes against computer data security.[3] The second group of crimes is more diverse and includes crimes against intellectual property (Articles 198, 199 and 202), as well as individual crimes such as endangerment of security, most often through social networks (Article 138), unauthorised publication and presentation of another's texts, portraits and recordings (Article 145), unauthorised collection of personal data (Article 146), showing, procuring and possessing pornographic material and minor person pornography (Article 185), abuse of computer networks or other technical means of communication for committing criminal offences against sexual freedom of a minor (Article 185b), forgery and abuse of payment cards (Article 243), as well as any other criminal offences in which computers or computer networks are used as a means or method of execution.

The Criminal Procedure Code prescribes evidentiary actions that can be applied in criminal proceedings conducted for these criminal offences. Due to the specifics of these crimes, the Code was amended in 2011. The amendments defined the terms used when dealing with high-tech crime, such as "*electronic record*", "*electronic address*", "*electronic document*" and "*electronic signature*" (Article 2, paragraphs 29, 30, 31 and 32), but it also listed criminal offences that merit special evidentiary actions (Articles 161 and 162) for which a special law stipulates that they fall under the jurisdiction of the Public Prosecutor's Office of Special Jurisdiction, which in this case is the Special Prosecutor's Office for Combating Cybercrime.[4]

[2] The Convention on Cybercrime of the Council of Europe was adopted in 2001 and entered into force in 2004. Serbia signed the Convention in 2005 and immediately started working on creating a legal framework, but ratified the Convention only in 2009.

[3] These acts, listed in the Criminal Code of the Republic of Serbia, include all criminal acts from Chapter 27, namely: damaging computer data and programmes (Article 298), computer sabotage (Article 299), creating and introducing computer viruses (Article 300), computer fraud (Article 301), unauthorised access to computer, computer network or electronic data processing (Article 302), preventing or restricting access to public computer network (Article 303), unauthorised use of computer or computer network (Article 304), and creating, obtaining and providing another person with means for committing criminal offences against the security of computer data (304a).

[4] In the case of cybercrime, special evidentiary actions may be applied to the following criminal offences in this area: showing, procuring and possessing pornographic material and minor person pornography (Article 185, paragraphs 2

Other laws of importance in this area are: the Law on Ratification of the Protocol to the Convention on High-Tech Crime Relating to the Incrimination of Racist and Xenophobic Acts Committed through Computer Systems, the Law on Ratification of the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, the Law on Electronic Communications, the Law on Information Security, the Law on Organisation and Competences of State Authorities in the Fight against High-Tech Crime, the Law on International Legal Assistance in Criminal Matters, and so on.

In the context of Serbia's accession to the European Union and the harmonisation of its legislation with EU policies and the *acquis*, in 2018 the Government of Serbia adopted the Strategy for the Fight against High-Tech Crime 2019-2023 and the accompanying Action Plan for the implementation of the Strategy for the period 2019-2020. The Action Plan expired in 2020, yet the Ministry of the Interior (MoI) has not drafted a new one. The professional public is not aware of how the Strategy has been implemented after the expiry of the Action Plan, and there is no possibility to adequately assess what has been done in the meantime as there is no publicly available report of the Ministry of the Interior. The Strategy will expire next year, and it is unlikely that a new Action Plan will be adopted by that time. In addition, in May 2022, Serbia was among the first countries to sign the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, approved by the Council of Europe at the end of 2021. The ratification of this Protocol will imply further alignment of various regulations with its provisions. The significance of the Protocol lies in the fact that it strengthens the states' cooperation with the private sector in order to protect the rights of all Internet users and collect electronic evidence more efficiently, in accordance with technological developments and new forms of CC. It was necessary to produce such a document because of the increasing complexity of obtaining electronic evidence, which can be kept by different countries with different legal systems.

Institutions Responsible for the Fight against Cybercrime

In accordance with the Law on Organisation and Competences of State Authorities in Combating High-Tech Crime, a Special Prosecutor's Office for Combating High-Tech Crime was established in Belgrade in 2007, within the Higher Public Prosecutor's Office, with jurisdiction over the entire territory of Serbia. When it comes to courts, until 2009 it was the specialised department of the Higher Court in Belgrade that was competent to try disputes in the field of CC, while the Appellate Court in Belgrade decided in the second instance. However, since the specialised department of the Higher Court in Belgrade ceased to exist in 2009, all the judges of this court now adjudicate in high-tech crime cases. All the panels of the Appellate Court in Belgrade, as the second instance body, also receive such cases. The abolition of the specialised court department has caused numerous problems in practice. The biggest one is that judges who do not sufficiently understand the technology or the specifics of electronic evidence are now adjudicating in cases involving cybercrime. Insufficient training of judges for trying such cases, which require knowledge of

and 3 of the Criminal Code), unauthorised use of copyrighted work or other work protected by similar right (Article 199), damaging computer data and programmes (Article 298, paragraph 3), computer sabotage (Article 299), computer fraud (Article 301, paragraph 3), unauthorised access to computer, computer network or electronic data processing (Article 302).

cybercrime terminology, leads to difficulties throughout the proceedings. In practice, there are situations when entire proceedings are rejected due to insufficient digital literacy of judges and their ignorance of the specificities of the matter at hand.

The Ministry of the Interior, with its special Department for the Suppression of High-Tech Crime, which operates as part of the Sector for the Fight against Organised Crime (*SBPOK*), is also responsible for the fight against cybercrime. The Department was established in 2008 and was divided into two sections – the Section for the Suppression of Intellectual Property Crime and the Section for the Suppression of Electronic Crime. Due to the emergence of increasingly complex and diverse criminal CC acts, the department was reorganised into four sections in 2019: the Section for Combating Intellectual Property Crime, the Section for Combating Electronic Crime, the Section for Combating Illicit and Harmful Content on the Internet, and the Section for Combating Misuse in the areas of e-commerce, e-banking and online payment cards. The Department acts on the requests of the Special Prosecutor's Office, which manages the pre-investigation procedure, but also on the requests of other prosecutor's offices if there is a need to collect and interpret evidence in electronic form. The division within the Department is important because the complexity of these crimes requires specially trained officers who work only on crimes for which they are specialised.

In addition to the Special Prosecutor's Office and the Department for the Suppression of High-Tech Crime within the Ministry of the Interior, there are other bodies whose competencies are important in this area. The Ministry of Justice is charged with harmonising domestic criminal legislation with the regulations of the European Union. Within its Customs Administration, the Ministry of Finance was supposed to create conditions for the establishment of the Cyber Customs unit to fight cybercrime, with the aim of identifying criminal acts that are in conflict with customs regulations on the Internet.[5] However, the Ministry of Finance and the Customs Administration have not established this unit to date. The Ministry of Finance also has the Directorate for the Prevention of Money Laundering, which is in charge of collecting, processing and analysing data related to money laundering and financing of terrorism. If it finds evidence of criminal offences, the Administration forwards information, data and documents to the competent authorities, in accordance with the law. Since financial transactions and fraud involving money can take place through computers and computer systems, this Directorate plays a significant role in detecting cybercrimes.

The Strategy also envisions the establishment of special organisational units to fight cybercrime within the Security Information Agency (*BIA*) and the Military Security Agency (*VBA*). In accordance with the Law on the Security Information Agency, the BIA is responsible for combating all forms of cybercrime if its consequences are such that they could destabilise national security. Pursuant to the Law on the Military Security Agency and the Military Intelligence Agency, the Military Security Agency performs tasks related to the security and counter-intelligence protection of the Ministry of Defence and the Serbian Army. Within this, it also performs the tasks of detecting, preventing and proving criminal acts against the security of computer data. The Military Security Agency is also authorised to implement the protection of the ICT systems of the Ministry of Defence and the Serbian Army.

[5] The obligation prescribed in the Strategy for the Fight against High-Tech Crime 2019-2013, p. 26

The National Bank of Serbia, the Ministry of Trade, Tourism and Telecommunications (*MTTT*) and the Regulatory Agency for Electronic Communications and Postal Services (*RATEL*) also play significant roles in this area. The National Bank of Serbia is responsible for supervising all ICT systems of financial institutions under its control. The MTTT is charged with information security in Serbia, that is, for the security of particularly important ICT systems. In addition to this competency, the MTTT has established the National Contact for the Safety of Children on the Internet 19833, which aims to raise awareness of the dangers that threaten children on the Internet. If a crime is reported in this area, they forward information about it to the authorities competent for the fight against cybercrime. RATEL, on the other hand, includes the National Centre for the Prevention of Security Risks in ICT Systems (National CERT). The tasks of the National CERT are to coordinate the prevention and protection against security risks in ICT systems at the national level, collect and exchange data on possible risks, and inform the public and persons managing ICT systems about incidents.

Cooperation between the competent authorities and civil society organisations (CSOs) does exist, but is limited to several international and domestic organisations such as *Save the Children* and the B92 Fund, implementing the project "Click Safe", the Loop [*Petlja*] Foundation and the Centre for Missing and Abused Children (the former Tijana Jurić Foundation). However, other interested civil society organisations, such as women's organisations, LGBTIQ organisations, Roma and other organisations advocating for the rights of marginalised groups in Serbia, are not involved in this cooperation. Civil society organisations point to various forms of threats to rights and freedoms of multiple-marginalised groups in Serbia through the use of modern technologies, but the strategic and legal framework in this area does not recognise the impact of modern technology on various social groups, with the exception children and youth. Civil society organisations dealing with human rights believe that this is a consequence of the insufficiently inclusive process of drafting political documents and legislation, as they are neither consulted nor involved in the drafting process in any fashion.[6]

Current Trends in the Field of Cybercrime in Serbia

According to the survey conducted by the Registry of the National Internet Domain of Serbia (*RNIDS*) in 2022, approximately 74% of Serbian citizens use the Internet, which represents an increase of 25% in the last decade. The growing number of users of Internet, computers and mobile devices, as well as the growing Internet connectivity, is increasing the security risks. According to the RNIDS report, 41% of Internet users who experienced an attack do not know who their attackers were, while a quarter of the users do not even know that they were targets of cyber attacks. It should also be noted that the majority of Serbian citizens are not aware of the types of crimes that are deemed cybercrime acts.

[6] Interview with representatives of the Autonomous Women's Centre, March 2022

Based on the MoI statistics, there has been a noticeable increase in cyber-related crimes in Serbia. The MoI's Report on the State of Public Safety states that 622 criminal acts in this area were discovered in 2018, 946 in 2019, and 760 in 2020. When it comes to (just) criminal offences against computer data, there is a difference between the number of filed criminal charges against adults in relation to the number of persons who are in fact accused (Chart 1).

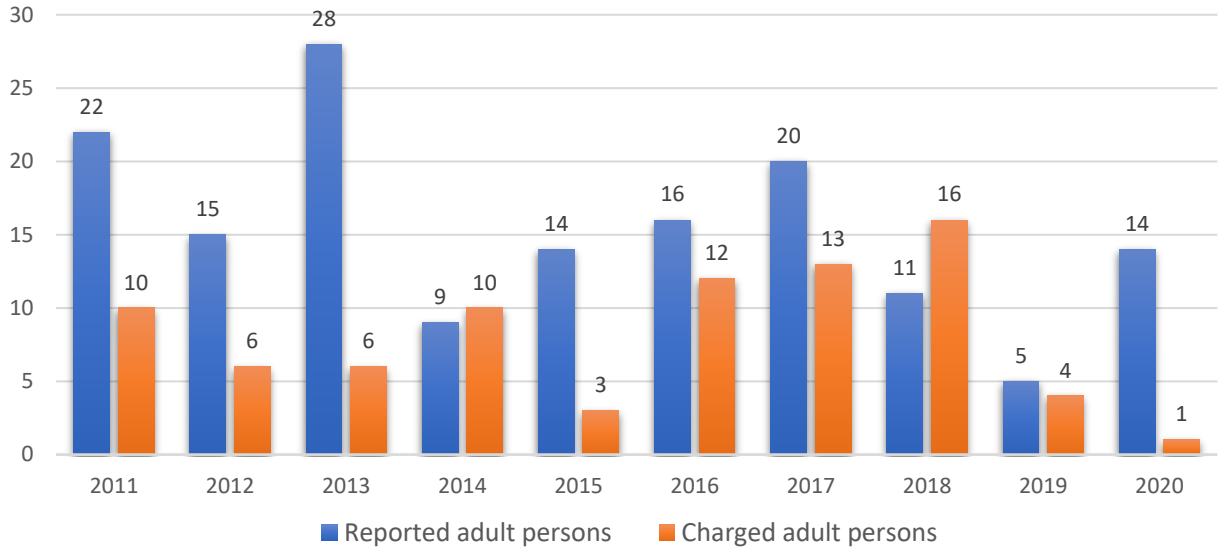

Chart 1. Adult perpetrators of crimes against computer data in the Republic of Serbia in 2020
Source: Statistical Office of the Republic of Serbia

The noticeable difference between the number of filed criminal charges and the number of accused persons can be explained by the fact that the Special Prosecutor's Office has 14 employees, while the Department for Suppression of Cybercrime has 22, which is insufficient to process and file that many cases. Besides the lack of staffing capacities, it should be noted that there are also shortcomings in terms of technical and spatial capacities of the Special Prosecutor's Office, which certainly affect its work.

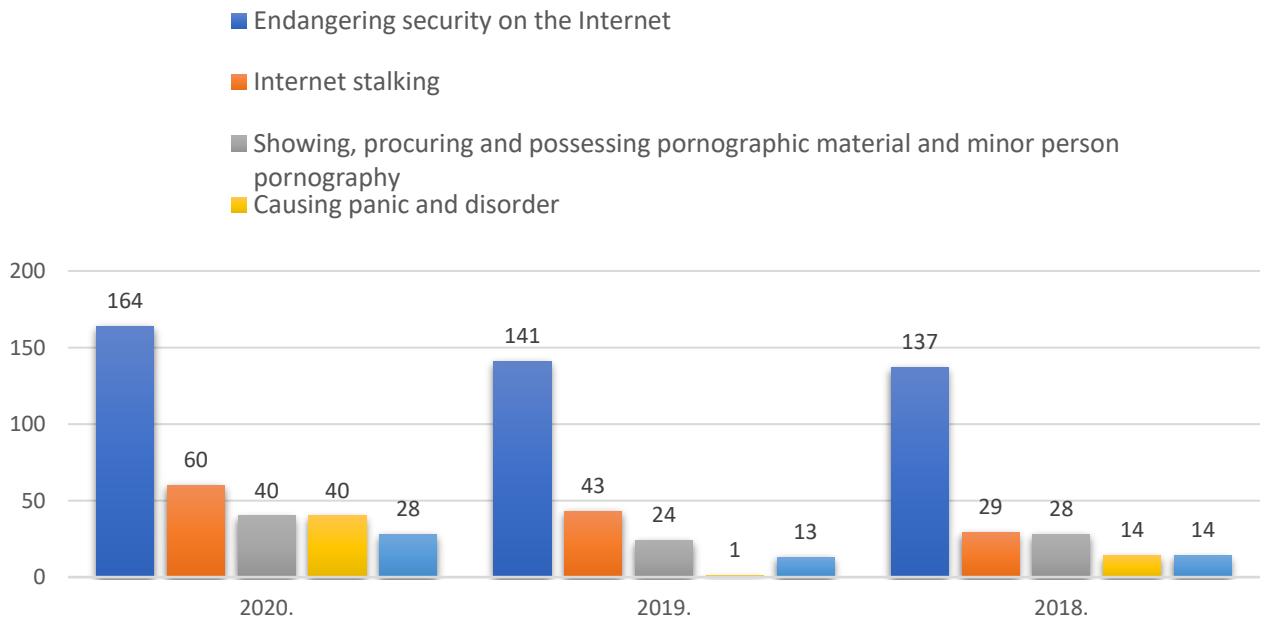

Chart 2. Five most common types of cybercrime in Serbia
Source: Republic Public Prosecutor's Office

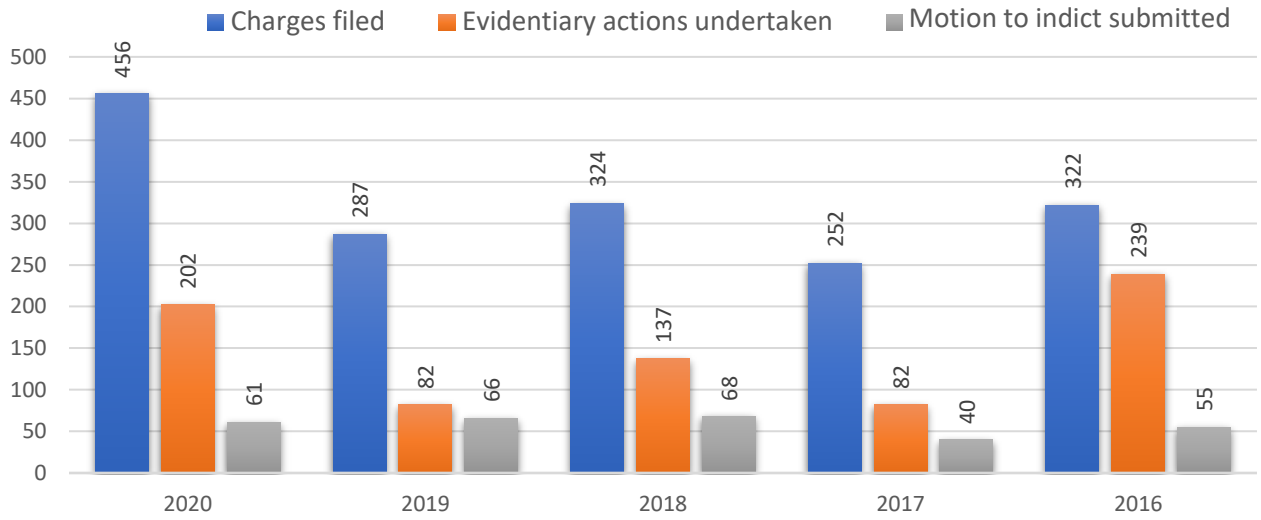

Chart 3. Statistical data on the work of the Special Prosecutor's Office for Cybercrime

Sources: Information Booklet on the work of the Republic Public Prosecutor's Office for 2020, 2019, 2018, 2017 and 2016

The crime of 'endangering security' has been on the rise in Serbia for the last three years. When threats are made through social media, they include elements of a high-tech crime. In Serbia, it is the security of human rights defenders, (environmental) activists and journalists that is especially endangered. For example, the SHARE Foundation keeps a record on its website of threats to digital rights and freedoms, as well as of online attacks on citizens, public figures, journalists, activists and human rights defenders. It is stated in their report that in the last three years (from January 2019 to June 2022) a total of 92 criminal charges were filed against endangering security of these groups of people. Attacks on the above mentioned social groups have become everyday and are now almost normalised; the main problem is the absence of sanctioning of these types of crimes, which only leads to their increase.

Besides this crime, the second most common crime with elements of CC in Serbia is the misuse of children for pornographic purposes via the Internet (Article 185). According to EUROPOL's "2021 Organised Crime Threat Assessment", Europe is experiencing a growing trend in online material related to child pornography, which represents an increase that is seriously overloading the capacity of police and prosecutors of all the countries of the world, including Serbia.

Challenges in the Fight against Cybercrime in Serbia

The development of new technologies brings about new forms of challenges, risks and threats that are not covered by the existing criminal legislation. The practice shows that there is a need to amend and supplement the Criminal Code by adding certain criminal acts from the area of CC. For example, revenge pornography is not recognised as a crime in Serbian legislation, although it should be, considering its consequences for the victims and the society. There are initiatives to define this act and include it in the Criminal Code of the Republic of Serbia. As there are plans to amend and supplement the Criminal Code by the end of 2022, the prEUgovor coalition has prepared draft amendments proposing, among other things, to include a new criminal act in Chapter 14 – Crimes against the Freedoms and Rights of Man and Citizen, by adding a new Article 145a titled "Misuse of a Recording of a Sexual Content" after Article 145. The proposed amendment

would sanction a highly widespread act that causes great and compensable consequences for the victims.[7]

A good statutory solution would be to prosecute unauthorised collection of personal data - which in some cases is conducted in massive proportions - *ex officio* instead of in private lawsuits.[8] According to the current legislation, the victims of this crime are left to independently seek evidence of the crime from private companies. Private companies are not obliged to assist them and can deny physical persons the requested information and evidence. This complicates the process of gathering evidence and leads to injured parties most often withdrawing from criminal prosecution.

As regards the capacities of the authorities competent to fight CC, the capacities of the Special Prosecutor's Office have been strengthened in the course of the previous period. The Prosecutor's Office now has a special prosecutor in charge of CC, five deputy special prosecutors, five assistant special prosecutors and three administrative employees. So, there are a total of 14 employees, who, due to the increase in the number of cases, need to be provided with more office space in order to be able to work properly. In the reports on its work for 2018, 2019 and 2020, the Special Prosecutor's Office stated that "*the current technical equipment of the Special Prosecutor's Office does not meet the requirements imposed on the prosecution in terms of the pre-investigation procedure, i.e. the need to inspect evidence discovered in the course of the criminal proceedings*", which means that the Special Prosecutor's Office, in addition to not having a sufficient number of people and office space, also does not have the technical capacity to perform its duties in an adequate fashion.

Although a good legal framework has now existed for more than ten years, limited resources to combat CC are spent largely on criminal acts that threaten security via the social networks, where police officers monitor the actions of people who post negative comments about politicians on social media.[9] This type of politicisation of the police affects the activities and practical work of the Department, as well as the work of the Special Prosecutor's Office, causing various criminal acts to remain undetected. Apart from reducing the influence of politics on the operational work of the police, a great challenge is also the low level of knowledge and familiarity with the procedures of police officers outside the Department for the Suppression of CC, especially in smaller cities, where insufficient knowledge of police officers about criminal offences in the field of CC discourages citizens from reporting such criminal offences.

Finally, the low level of security culture of the citizens of Serbia, that is, their lack of awareness about the problem and opportunities for protection against this type of crime, happens to be another great challenge in the fight against CC. The authorities are making efforts to provide better information to the professional and general public about the dangers of CC and its impact on society, but this is not enough since the risks of this type of crime are constantly increasing.

[7] At the beginning of 2021, the Serbian public learned of dozens of Telegram groups with several tens of thousands of members who exchange pornographic recordings and images of their former girlfriends, as well as personal data of girls that are in said recordings and images. The largest such group had 36,000 members and was called the EX YU Balkan Room. There were also individual groups, divided by cities such as Niš and Belgrade.

[8] Article 153 in conjunction with Article 146 of the Criminal Code

[9] Jelena Pejić Nikić (ed), prEUgovor Alarm Report on the Progress of Serbia in Chapters 23 and 24, prEUgovor, Belgrade, May 2021, pp. 97-98.

Conclusion and Recommendations

Despite a good legal framework, the fight against CC in Serbia is facing a chronic shortage of qualified staff, as well as politicised priorities of the relevant institutions. The sluggishness of the criminal justice system does not keep pace with advances in technology, which is why new forms of crime, where computers or computer networks appear as a means or method of execution, remain outside the framework of criminal law. Insufficient training and knowledge of all the actors involved in the fight against CC, especially judges, attorneys and police officers outside the CC Department, leads to a large number of unprocessed crimes that fall under the above category. To achieve the highest level of fight against CC, it is necessary to also educate the general public about the types of cybercrimes, as well as ways to protect themselves from them and prevent them.

We hereby highlight the following recommendations:

- It is necessary to develop a new Action Plan for the implementation of the Strategy for Combating High-Tech Crime for the period 2022-2023.
- It is necessary to increase the number of trained police officers in four sections of the Department for the Suppression of High-Tech Crime, to enable them to fight this type of crime more effectively.
- It is necessary to conduct trainings for police officers outside the Department for the Suppression of CC to get them acquainted with the procedures for gathering evidence and reporting crimes.
- The Special Prosecutor's Office for High-Tech Crime needs to be provided with larger accommodation capacities, an increased number of employees, and adequate technical equipment which would enable them to perform their tasks without hindrances.
- It is necessary to introduce continuous training for judges and attorneys dealing with high-tech crime cases in order to avoid problems in proceedings, which could occur due to their insufficient knowledge of the matter.
- There is a need for better cooperation at the national level between the private, public and civil sectors to make the fight against high-tech crime more successful. This cooperation must be continuous, because in this area, the technology and the accompanying security challenges, risks and threats are constantly evolving.
- It is necessary to amend and supplement relevant articles of the Criminal Code in order to provide for the criminal offence 'abuse of sexual content'. As for the criminal offence 'unauthorised collection of personal data', it is necessary to add that, when this is done on a larger scale, such an act is to be prosecuted *ex officio*.

About prEUgovor

Coalition prEUgovor is a network of civil society organisations formed in order to monitor the implementation of policies relating to the accession negotiations between Serbia and the EU, with an emphasis on Chapters 23 and 24 of the Acquis. In doing so, the coalition aims to use the EU integration process to help accomplish substantial progress in the further democratisation of the Serbian society.

Members of the coalition are:

ASTRA – Anti-Trafficking Action
www.astra.rs

Autonomous Women's Centre (AWC)
www.womenngo.org.rs

Belgrade Centre for Security Policy (BCSP)
www.bezbednost.org

Centre for Investigative Journalism in Serbia (CINS)
www.cins.rs

Centre for Applied European Studies (CPES)
www.cpes.org.rs

Group 484
www.grupa484.org

Transparency Serbia (TS)
www.transparentnost.org.rs

PrEUgovor's key product is the semiannual report on the progress of Serbia in Cluster 1.

Follow prEUgovor activities on the official website, Facebook page and Twitter account.

ISBN-978-86-84711-54-2

B | T | D The Balkan Trust for Democracy
A PROJECT OF THE GERMAN MARSHALL FUND

Norway