VARSTVOSLOVJE,
Journal of Criminal Justice and Security,
year 17
no. 2
pp. 230–242

Specialization of Criminal Justice Authorities in Dealing with Cybercrime

Milana Pisarić

Purpose:

This paper deals with specialized cybercrime units within the criminal justice system as one of the key elements of proper response to cybercrime. The author emphasizes the need for the establishment and/or improvement of such an organization with specific powers within law enforcement and prosecution authorities as well as within courts, in order to tackle problematic issues raised by computer-related crimes, especially the ones concerning investigation and prosecution of offences committed against and/or by means of computer data and systems, and carrying out computer forensics with respect to electronic evidence in general.

Design/Methods/Approach:

The author analyses the relevant international legal framework and various national legislation chosen as examples of good practice in order to present the justification and purpose of specialization, types of specialized law enforcement units, their organization, functions, strategic and tactical responsibilities.

Findings:

Investigation and prosecution of cybercrime and forensic analysis of electronic evidence require specific skills within criminal justice authorities. Therefore, it is advisable to set up or consolidate police-type and prosecution-type cybercrime units with strategic and operational responsibilities and computer forensic capabilities within cybercrime units or as separate structures. As for judiciary, dealing with computer-related crimes requires particular knowledge and skills, and where it is compatible with the legal system of the respective country, the creation of specialized courts may be considered. In addition to the existing legal mechanisms for dealing with transnational crime, the creation of an international court or tribunal that would have jurisdiction over individuals who committed the most serious cybercrimes of global concern may also be a good solution in order to prevent serious cyber attacks from going unpunished.

Research Limitations/Implications:

The results presented in this paper are to be seen as de lege ferenda proposals for the improvement of the existing legislation related to organization and powers of authority vested in combating cybercrime.

Originality/Value:

Despite the existence of a significant number of essays dealing with cybercrime, not many of them are concerned with tactical and procedural issues of investigation and prosecution of this specific kind of crimes. The results presented in this paper are de lege ferenda proposals for the improvement of the existing legislation related to organization and powers of authority vested in combating cybercrime. Accordingly, the value of this paper may be recognized in the analysis of legal solutions regarding law enforcement and prosecution response to computer-related crime, with the emphasis on specialization of authorities involved.

UDC: 343.3/.7:004

Keywords: cybercrime, investigation, prosecution, court, specialization

Specializacija organov za kazenski pregon za obravnavo kibernetske kriminalitete

Namen prispevka:

Članek obravnava specializirane enote za kibernetsko kriminaliteto znotraj kazenskopravnega sistema kot enega izmed ključnih elementov ustreznega odzivanja na kibernetsko kriminaliteto. Avtorji poudarjajo potrebo po vzpostavitvi in/ali izboljšanju takih organizacij s posebnimi pooblastili tako v okviru organov kazenskopravnega pregona kot tudi v okviru sodišč, da bi odpravili težave, ki se pojavljajo v zvezi s kaznivimi dejanji, ki so povezani z računalniki, še posebej tistimi, ki se tičejo preiskovanja in pregona kaznivih dejanj nasproti in/ali preko računalniških podatkov in sistemov ter izvajanja računalniške forenzike v zvezi z elektronskimi dokazi na splošno.

Metode:

Avtorji analizirajo relevantni mednarodni pravni okvir in različne nacionalne zakonodaje, izbrane kot primer dobre prakse z namenom predstaviti utemeljitev in namen specializacije, vrste specializiranih enot za kazenski pregon, njihovih organizacij, funkcij, strateške in taktične odgovornosti.

Ugotovitve:

Preiskovanje in pregon kibernetske kriminalitete in forenzična analiza elektronskih dokazov zahteva specifična znanja v okviru organov kazenskega pregona. Priporočljivo je oblikovati ali konsolidirati policijske in preiskovalne enote za kibernetsko kriminaliteto s strateškimi in operacijskimi odgovornostmi ter zmožnostmi za računalniško forenziko znotraj enot za kibernetsko kriminaliteto ali kot ločene strukture. Kar se tiče sodstva, delo s kaznivimi dejanji, povezanimi z računalniki, zahteva posebno znanje in sposobnosti ter, kjer je to združljivo s pravnim sistemom posamezne države, obravnavo oblikovanja specializiranih sodišč. Kot dopolnitev obstoječih pravnih mehanizmov za obravnavo mednarodnih kaznivih dejanj in v izogib nekaznovanja resnih kibernetskih napadov bi bila dobra rešitev ustanovitev mednarodnega sodišča ali razsodišča, ki bi imelo jurisdikcijo nad posamezniki, ki so storili najhujša kibernetska kazniva dejanja globalnega pomena.

Omejitve/uporabnost raziskave:

Rezultati, predstavljeni v tem članku, so predlogi de lege ferenda za izboljšave obstoječe zakonodaje, povezanih z organizacijo in močjo organov, pristojnih za boj proti kibernetski kriminaliteti.

Izvirnost/pomembnost prispevka:

Kljub obstoju velikega števila esejev na temo kibernetske kriminalitete jih veliko ne obravnava taktičnih in proceduralnih težav preiskovanja in pregona teh specifičnih vrst kaznivih dejanj. Rezultati, ki so predstavljeni v tem članku, so predlogi de lege ferenda za izboljšave obstoječe zakonodaje, povezanih z organizacijo in močjo organov, pristojnih za boj proti kibernetski kriminaliteti. Skladno s tem je vrednost tega članka mogoče prepoznati v analizi pravnih rešitev glede kazenskega pregona in odgovorov na kazniva dejanja, povezana z računalniki, s poudarkom na specializaciji vključenih organov.

UDK: 343.3/.7:004

Ključne besede: kibernetska kriminaliteta, preiskava, pregon, sodišče, specializacija

1 INTRODUCTION

It is generally accepted that some form of regulation of cyberspace is required, but the issue at hand is which form this regulation should take. Regulation of cyberspace could be argued from one of the following four standpoints: the introduction of new laws, improvement of the existing laws, or the combination thereof, or otherwise the adoption of alternative forms of regulation. Although much of the monitoring, regulation, protection, and enforcement related to cybercrime is not the responsibility of state-controlled public police forces, while Internet Service Providers and users bear the primary responsibility for cleaning up cyberspace, it is necessary to mark the application of a legal model of governance by a body of substantive criminal law in order to deal with the most extreme forms of behaviour. As cyberspace has become a common aspect of human existence, the number of behaviours that could be defined as cyber crimes will not only increase, but the nature of their victimization will also expand.

To face the problem of policing and prosecuting cybercrime, the area of legislation requires constant updating of substantial and procedural criminal laws in order to make it clear which criminal activity in cyberspace is to be considered a cybercrime, and also to create a legal framework for its investigation. Cybercrime and cybercrime investigations pose significant challenges to law and law enforcement. There are many reasons for that. Challenges arisen from the context and scope of **c**yber crimes and technical expertise required to investigate them led to re-examination of police capacity to respond.

Creation or further consolidation of specialized cybercrime units is commonly recognized as the key element of the effective response to cybercrime. There is no single solution, which could be considered appropriate or best for all countries, as its creation and evolution depends on the needs of each particular country, based upon its legislation, reliance on IT, prevalence of different types of criminal activity and other matters.

Both law enforcement and prosecution authorities require a specialized response to the issues raised by cybercrime. Cybercrime is considered to cover offences against computer systems, offences by means of computer systems, in particular those that have acquired a new quality through the use of ICT (according to the CoE Convention on Cybercrime – Council of Europe, 2001). Important evidence for any offence may be located on a computer, and even though this offence is otherwise unrelated to computer systems and not considered cybercrime as such, the criminal justice system needs to be able to recognize and handle electronic evidence in exercising digital forensics.

2 ROLE OF SPECIALIZED CYBERCRIME UNITS

The primary role of specialized cybercrime units may be divided into three functions: 1) investigating and/or prosecuting offences against computer data and systems; 2) investigating and/or prosecuting offences committed by means of computer data and systems; 3) carrying out computer forensics with respect to electronic evidence in general (Specialised cybercrime units: Good practice study, 2011: 4). Criminal justice authorities need to be able to deal with all three aspects: offences committed against computer data and systems (such as those defined in Articles 2 to 6 of the CoE Convention on Cybercrime – Council of Europe, 2001); offences committed by means of computers (such as those defined in Articles 7 to 10 of the CoE Convention on Cybercrime – Council of Europe, 2001), and other articles as well); electronic evidence on the computer related to any type of offence (Article 14 of the CoE Convention on Cybercrime – Council of Europe, 2001).

Specialized cybercrime units cannot be effective in isolation. The creation or consolidation of specialized cybercrime units should be part of an effective cybercrime strategy in which the police unit could be a driving force on the national level. Cybercrime often involves a combination of offences committed against and by means of computers, which is why different law enforcement and other services share a responsibility. Interagency cooperation is therefore essential, and a specialized cybercrime unit may provide technical support and know-how to other agencies.

In order for the criminal justice system to be capable of coping with such a large number of offences and cases, functions and responsibilities of law enforcement agencies specialized for cybercrime may include all or a combination of investigations, collection of data and forensic analysis, intelligence collection, analysis and dissemination assessment, and analysis of cybercrime phenomena, etc. Nevertheless, the role of a specialized unit depends on general police unit organization and its place within it, material and territorial jurisdiction of police units, and procedural powers and tools to be used by police units in their investigations or in specific activities. More precisely, the role is defined by the organization and functioning of a police unit, its jurisdiction (defined and clearly separated from other units), definition of the limits of jurisdiction between police units and collaboration and hierarchical relation between them, and staff positions in the unit (Specialised cybercrime units: Good practice study, 2011: 16).

3 TYPES OF SPECIALIZED CYBERCRIME UNITS

The investigation of cybercrime, forensic analysis of electronic evidence, and prosecution of cybercrime require specific skills. Therefore, criminal justice authorities should be supported in creation or consolidation of: police-type cybercrime or high-tech units with strategic and operational responsibilities; prosecution-type cybercrime units; computer forensic capabilities within cybercrime units, or as separate structures; skills within the judiciary. The creation of specialized courts may be considered where this is compatible with the legal system of the respective country; interagency cooperation. This is essential due to the fact that cybercrime units are to cooperate with other police services (such as economic crime units, child protection units) and institutions (such as financial intelligence units, Computer Emergency Response Teams, and others).

Given the name and their place in internal organization, several categories of specialist units dealing with cybercrime may be recognized: 1) as scientific support units or forensic investigation units carrying out forensic examination of seized computer devices and data recovery; 2) as departments collecting intelligence on major cross-boundary investigations usually linked to terrorism or fraud (known as Specialist Investigations Departments or Intelligence and Specialist Operations); 3) as units with broader remit to investigate offences committed against computer systems and traditional crimes with high-tech elements; 4) as units which investigate child pornography cases (Jewkes, 2010: 540).

On the basis of the analysis of current types of cybercrime units, it appears that a cybercrime unit should be structured in three sections: 1) investigation; 2) data and information analysis; 3) computer forensics. One unit at the central level coordinating a number of field offices seems to be an efficient formula. However, the units should remain flexible enough to respond to the evolution of cybercrime and technology, and to changes in the environment in which they operate.

The following types of specialized cybercrime units are found: cybercrime units, high-tech crime units, computer forensic units, central units, crime-specific units, specialized prosecution units (Specialised cybercrime units: Good practice study, 2011: 5).

Cybercrime units. Cybercrime units investigate all types of cybercrime committed against and by means of computer data and systems, and also have computer forensic functions (e.g. specialized units within the police forces of Cyprus, the Czech Republic, France (Gendarmerie), Mauritius, Romania, or Spain) (Specialised cybercrime units: Good practice study, 2011: 13). The Spanish Cybercrime Unit was created according to the National Law 1/86, developing from a small group in 1995 to a brigade in 2000. It operates within Spanish Police as a specialized structure for investigating crimes against computer systems and crimes through computer systems. At present, it includes a central unit and specialized units consisting of 4–7 investigators in the field offices. The central unit has three sections: the first one, responsible for investigations related to crimes against person (child pornography, threats, etc.); the second one, responsible for investigations of economic crimes (frauds, piracy, hacking, etc.); the third one, responsible for forensic activities (related to the analysis and forensics of computer systems and computer data storage devices during their investigations) and authorized to coordinate territorial units (Specialised cybercrime units: Good practice study, 2011: 94).

High-tech crime units. High-tech crime units are mainly competent for investigating offences against computers (not other crimes committed through computer systems, such as electronic payment frauds, Internet frauds), and they include computer forensic functions providing technical support to investigations carried out by other units or agencies.

In *Austria*, there is the Criminal Intelligence Service responsible for the investigation of crimes committed against computer systems, but not for crimes committed by means of computer systems (unlawful access, privacy of telecommunication, unlawful interception of data, damaging of data, interference in the functioning of a computer system, misuse of a computer program, falsification of data, fraudulent misuse of data processing), which are investigated by the Criminal Intelligence Service Austria Departments 3 and 7.

In *Belgium,* there is one Federal Computer Crime Unit (FCCU) at central level and 26 Regional Computer Crime Units (RCCU) at district level. All offences committed against computer systems and data (e.g. illegal access) are handled by the RCCU, whereas FCCU can support and assist them whenever they need specialized competences or centralized equipment. The FCCU is able to handle cases autonomously in the case of a need for an urgent intervention or attack on critical information infrastructure. FCCU/RCCU do not handle offences committed through or by means of computer systems (e.g. child pornography), but can provide support (sometimes to a very large extent) in forensic ICT analysis and internet investigations (Specialised cybercrime units: Good practice study, 2011: 63).

Computer forensic units. Computer forensic units are separate units responsible for collection and analysis of electronic evidence – they often have computer forensic functions, meaning that they analyse the evidence related to their own investigations or investigations of other services. For example, there is the “Forensics Unit” functioning within the Cybercrime Unit in Romania (Specialised cybercrime units: Good practice study, 2011: 19).

Central units. Central units are without investigative functions but are responsible for coordination and strategic and intelligence functions – the power of these units is limited to collection of information or assistance to other police structures in computer forensics, cybercrime investigations, or other types of criminal investigations (for example, in the United Kingdom, the Cybercrime Unit from SOCA has primarily intelligence function (collection of data), with the purpose of defining national policies and threat assessments, and initiating major investigations. In these police systems, the actual cybercrime investigation is a task of the local police, with the assistance of a specialized unit) (Specialised cybercrime units: Good practice study, 2011: 14).

Crime-specific units. Crime-specific units have been created to deal with specific types of crime: child pornography and other forms of sexual exploitation and sexual abuse of children, IPR-related offences, or specific types of fraud. For example, in the United Kingdom there is the CEOP - Child Exploitation Online Protection launched in 2006, which underlines the commitment of the UK police to stem the global Internet trade in child pornography. They have developed a proactive strategy based on specialist intelligence and technical expertise (Specialised cybercrime units: Good practice study, 2011: 14).

Specialized prosecution units. Serbia has established a department for fighting cybercrime within the Ministry of Internal Affairs, as well as the special department within Higher Public Prosecutor’s Office in Belgrade (the Law on Organization and Competence of Government Authorities for Suppression of High-Tech Crime, 2005, 2009) with nationwide competence and Special Prosecutor for High-Tech Crime in charge. Special Prosecutor’s Office for High-Tech Crime was established in 2006 within the Higher Public Prosecutor’s Office in Belgrade with jurisdiction over the territory of the Republic of Serbia. The specialized prosecutor’s unit is authorized to: contribute to national cybercrime policies, draft internal procedures, coordinate field offices, prepare and implement training programs for police officers, participate in international judicial cooperation, and cooperate with international organizations and LEA. The Special Prosecutor’s Office is managed by the Special Prosecutor for High-Tech Crime who is appointed by the Republic Public Prosecutor. The specialized prosecutor’s unit consists of one prosecutor (Head of the Office), two deputy public prosecutors, two prosecutor advisers, and two administrative workers. The personnel has undergone basic training and continuously participates in training programs organized by the Judicial Academy of Serbia, cybercrime programs of the Council of Europe, OSCE, EUROPOL, U.S. DOJ, TAIEX, etc.

4 ESSENTIAL REQUIREMENTS FOR SPECIALIZED CYBERCRIME UNITS

There are some key considerations that have to be taken into account when “setting up a specialized cybercrime unit: the national legislation that provides the legal basis, the internal orders and regulations for the functioning of the unit, the police department to which the unit is attached, the premises of the unit (the personnel, training and equipment), the internal organization and structure” (Specialised cybercrime units: Good practice study, 2011: 16).

The performance of a specialized cybercrime unit depends to a large extent on the quality of its staff and determination and motivation of its leadership, cooperation with prosecutors and courts and other agencies at the domestic level, cooperation with the private sector, as well as international cooperation. However, personnel, equipment, and training are the main challenges that have to be kept in mind constantly.

4.1 Personnel

The selection of the right personnel to perform various functions within any specialist investigative unit is absolutely vital. Therefore, it is important to have in place a selection procedure for personnel which identifies those best suited for a role within that department. Essential personnel requirements to combat cybercrime reflect the basic functions of a cybercrime unit: investigation, prosecution, legislative assistance, education and/or public outreach, and training.

Investigators. Well-trained law enforcement officers are essential for conducting cybercrime investigations. Investigations include traditional crimes facilitated by the use of computer technology, as well as crimes in which computers are used as an instrument. In addition to traditional skills, training and qualifications, specialized skills and knowledge of cybercrime technology and legal requirements are also needed. The officers need to have knowledge of computers, Internet, police investigations, legislation governing cybercrime, and foreign languages.

Depending on their function, they have specific qualifications – mostly in criminal investigation and ICT, and, depending on the size of the cybercrime unit and its jurisdiction and tasks, the selection process must take place within a reasonable period of time, and have as criteria the skills and integrity of candidates.

The structure of the cybercrime unit has to be considered and a distinction has to be made between the officers who perform investigations in various areas and the officers who, in addition to having knowledge of computers and legislation, must also possess subject-matter knowledge. For example, the personnel to investigate child pornography on the Internet will also have to possess knowledge of psychology and investigations related to minors, whereas those investigating intellectual property crime will have to possess knowledge of intellectual property rights. National units tend to employ more specialized personnel. In a local unit, a specialized generalist is often preferred. These are some of the specialized skills needed for all cybercrime investigations: ability to prepare and conduct search and arrest warrants for digital evidence; knowledge of how computers work in order to effectively interrogate the suspect and establish culpability of evidence found on his/her computer; willingness and capacity to receive continual specialized training and certifications in specialties such as digital evidence, computers, networks, and forensic analysis; specialized crime scene preservation and examination skills; working knowledge of the Internet; ability to work with representatives from other jurisdictions (National Center for Justice and the Rule of Law, 2007: 24).

Covert, proactive investigations require the investigator to “role-play”. Investigators must be acquainted with various facets of popular culture and the “slang” used in e-mail and instant messaging communications to effectively pose as underage persons. Furthermore, investigators must be familiar with the typology of Internet predators.

Cybercrime prosecutors. Cybercrime prosecutors typically team with investigators and computer forensic examiners to investigate and prosecute cases. *Cybercrime Prosecutors o*versee operations of cybercrime unit or task force; advise investigators and computer forensic examiners regarding the amount and type of evidence necessary for arresting and conviction; develop forms, protocols, and procedures for the writing, execution, and return of search and arrest warrants. In order to do the former, c*ybercrime prosecutors have to possess the following essential skills:* 1) knowledge of cybercrime statutes and other relevant crimes; 2) familiarity with computer technology and computer forensics; 3) commitment to continued education in both legal and technical aspects of cybercrime prosecution (National Center for Justice and the Rule of Law, 2007: 26).

Computer forensic examiners. Virtually every criminal investigation involves some form of digital evidence or communications data, requiring investigators to seek the assistance or advice of the in-house specialist staff. Digital evidence and communications data are integral to an ever increasing number of mainstream criminal investigations. Therefore, proliferation of and close linkage between digital and computer evidence and the work of prosecutors and investigators indicates a strong need for the in-house computer forensic examiners. There are actually two general roles within e-crime unit, which may be recognized: forensic analysis of digital evidence and network investigations. Forensic analysis of digital evidence means that the role of a technician is to secure and retrieve evidential material from digital media, mainly computers, to produce such evidence in the form which is admissible in the court, and to provide technical advice and support to the officers encountering such media during investigations into computer crime or where a computer or digital media have been used in the commission of such crime. The other role is conducting network investigations and operations into network-based criminal activity to detect high-tech crime, gathering and disseminating relevant and quality intelligence, providing technical advice and assistance to officers engaged in the investigation of high-tech crime, and producing evidence in the form admissible in the court (Association of Chief Police Officers, 2012: 5–6).

The role of this staff within specialized cybercrime unit has to be extended and developed in respect of their role and the skill base, which they require. They closely cooperate with investigators on issues such as preparation and execution of search warrants, devising surveillance schemes, and other issues related to technical aspects of an investigation. Their primary responsibility is for the analysis of digital evidence, and their functions include disk imaging, data recovery, data extraction, and system analysis. In doing that, they are responsible for the maintenance of hardware and software utilized to obtain and analyse digital evidence, for maintaining condition and security of forensic computer laboratory, and for maintaining procedures for handling and securing evidence in the forensic laboratory.

Due to the fact that computer forensic examiners should be able to provide testimony concerning technical aspects of data recovery and analysis, an important skill they need to have is the ability to testify in the court.

In staffing these experts, the following essential skills are required: extensive experience with computers, particularly in the law enforcement context; degree in computer science or related field is a plus; experience and certification with the design and maintenance of computers and computer networks; comprehensive knowledge of computer operating systems; training and certification in computer forensics; commitment to continued education in computer forensics.

In staffing the units with forensic experts, employing the right mix of staff and roles in a unit and finding the right individuals represent a challenge for any branch, and the following should be considered: 1) programmers: there is a need for quick-and-dirty one-time solutions on a daily basis, e.g. for extraction of non-standardized data using customized scripts; 2) analysts: close cooperation between cybercrime specialists and analysts has proven gainful, especially for intelligence purposes; 3) technicians: they offload the specialists by managing internal networks and equipment; 4) administrative personnel: offloading administrative duties from specialists will obviously lead to the most cost-effective utilization of their expertise; 5) outsourcing/consultants, if it is legally possible to outsource investigative or forensic tasks (Specialised cybercrime units: Good practice study, 2011: 45).

4.2 Infrastructure

The costs associated with running a specialist investigative unit within a law enforcement agency, in terms of personnel, equipment, and training, represent a significant drain of resources, but the budget for the specialized unit is usually part of the general police budget. Tasks and priorities of the unit will determine the equipment and other necessary resources. Due to the rapid evolution of software and hardware on the one hand, and techniques for committing cybercrime on the other hand, the equipment needs to be at the cutting edge of technology and constantly updated. In order to create effective cybercrime investigative and prosecution capacity, specific hardware, software, physical space, and other components are needed or desirable. Primary needs involve forensic capacity – the ability to obtain, preserve, and analyse digital evidence. To accomplish its mission, cybercrime capacity demands a commitment of resources to infrastructure. In addition, the needs of investigators and prosecutors must be met. The quantity of items will vary, depending on the size and mission of the unit or task force. The necessary equipment and software should be related to computer systems investigations, digital computer forensic activities, undercover operations through the Internet, lawful access to computer systems, databases operation, and lawful interception of computer systems. Since these infrastructure needs constantly evolve and often exceed financial resources allocated to a police unit, the *minimum requirements* to set up an effective cybercrime unit have to be kept in mind. Accordingly, a budget allocated to this unit has to be based on personnel costs, costs of the necessary equipment and software, as well as the costs of using special techniques of investigation. The minimum equipment of the cybercrime unit, nevertheless adapted to the needs of the unit, should include: adequate space for computer equipment; secure storage for exhibits; sufficiently powerful computers for workers; covert Internet connections; necessary software and devices for forensically processing computer systems, and other devices (Association of Chief Police Officers, 2012: 15–16).

5 GOOD PRACTICE

Since the early 1990s, specialized units that investigate cybercrime and carry out computer forensics have been created in different countries, and they have been evolving ever since. As cybercrime and other types of crime involving electronic evidence are growing exponentially, it can be expected that more countries will establish such units, and that their size and scope of work will increase substantially in the future.

Three different approaches taken by state Attorneys General (AG) in the United States to create capacity to combat cybercrime will be presented as examples of good practice.

Dedicated In-House Cyber Crime Unit in Mississippi. AG office has statewide jurisdiction and arrest powers, and the authority to impanel a statewide grand jury to investigate and indict. Prosecutors from the Attorney General's office can try cases in any court in the state. A dedicated cybercrime unit is established within an AG's office (within Public Integrity Division, as the head of cybercrime unit reports to the Division head), and it has self-contained prosecution, investigative and forensics capacities. The Unit consists of one attorney (unit head), three investigators, and one forensics examiner (some investigators have become qualified to do forensic examinations as well). The Unit has an in-house computer forensics lab, which accepts cases for analysis from throughout the state. Considering the Unit's caseload and sources of cases, 40% of the cases are the unit's own investigations. The Unit has been working in 72 out of 82 state's counties, accepting cases involving any dollar amount – if it cannot take the case, the Unit refers the case to the Internet Crime Complaint Center. 36% of the cases are requests for computer forensics analysis received from a DA's office or local law enforcement, and the sole reason to deny forensic service is if forensics had previously started elsewhere. The rest (24%) are the requests for assistance from a DA's office or local law enforcement. The Unit has been funded from the following sources: Start-up funding from the National Center for Justice and the Rule of Law at the University of Mississippi (three years), as a sub grantee of the federal grant awarded to the NCJRL, Follow-on $300,000 grant from the Center for Computer Security Research at Mississippi State University. The Cyber Crime Unit also receives for its operations a portion of the legislative appropriations for the Attorney General's Public Integrity Division. There is no separate line item for the Unit (National Center for Justice and the Rule of Law, 2007: 17–19).

Statewide Cyber Crime Task Force Model in Maine. A task force model is a pooling of prosecution, forensics, and investigative resources from a variety of independent agencies. Lewiston, Maine Police Department promoted the idea and formed a partnership in 1999 with the following authorities: the Office of the Attorney General of Maine; Brunswick, Maine Police Department; Maine State Police and Portsmouth, Maine Police Department, and, lately, Maine task force has formed a partnership with Vermont and New Hampshire police to apply for and receive funding from OJJDP as Northern New England Internet Crimes Against Children (ICAC) Task Force. It includes members of local law enforcement, designated by their agency as responsible for investigating computer crime: three investigators and three computer forensics examiners and two AAGs from Maine AG Office provide legal support. MCCTF coordinates computer crime investigations statewide; conducts computer forensic examinations; responds to requests for assistance from other law enforcement agencies - *e.g.,* drafting subpoenas, contacting Internet Service Providers; conducts training programs for law enforcement agencies on investigation of Internet cases; conducts Internet safety programs for the public. Each member agency is responsible for cases within its own jurisdiction, and is trained in cybercrime investigative techniques, and encouraged to perform outreach on Internet safety. When first established, it received about 20 cases a month from the National Center for Missing and Exploited Children (NCMEC), and the cases of Internet Crimes Against Children

(ICAC) are still its priority, representing 80% of its workload (National Center for Justice and the Rule of Law, 2007: 19–22).

New Hampshire – Model of Distributed Forensics/Prosecution of Cybercrime. This model was structured in order for local prosecutors and investigators to handle cybercrime cases instead of the AG office. In 2003, New Hampshire AG invited state decision-makers to a meeting to develop a plan to address cybercrime, get consensus, and set up task force. After all task force members were asked to identify point person and complete survey of needs, law enforcement task force members established a plan to meet quarterly to discuss status of computer crimes in their jurisdictions. Implementation of the plan means that forensic examiners at state lab receive and image devices, run verifications and indexing, and store indexed images on Storage Area Network. Using viewing stations, local investigators ("case agents") access forensic images via secure, remote access to forensic machines, and conduct analysis on read-only prepared media (National Center for Justice and the Rule of Law, 2007: 22–24).

6 CONCLUSION

Cybercrime requires a specialized response by criminal justice authorities. Law enforcement authorities and prosecution services have to be able to investigate and prosecute offences against computer data and systems, offences committed by means of computers, as well as electronic evidence in relation to any crime. Although there is no single solution to the creation or further strengthening of specialized cybercrime units that would be recognized as appropriate or best for all countries, due to the fact that their creation and evolution depends on the needs of each particular country, based on its legislation, reliance on IT, prevalence of different types of criminal activity, and other matters, good practice could be found in comparative law. With the inevitable growth of the number of crimes committed by computer generated electronic evidence, special cybercrime units will not be able to handle on their own all the offences committed against or by means of computer systems, or conduct the analysis of electronic devices related to any crime. Accordingly, it would be advisable to establish a form of cooperation in which those specialized units would assist other police units and provide them with at least basic know-how in cybercrime investigation and securing electronic evidence.

REFERENCES

Association of Chief Police Officers. (2012). *Good practice and advice guide for managers of e-crime investigation: ACPO managers guide*. Retrieved from www.4matdata.co.uk/LiteratureRetrieve.aspx?ID=116738.

Council of Europe. (2001). *Convention on cybercrime.* Budapest: Council of Europe. Retrieved from www.coe.int/cybercrime.

Jewkes, Y. (2010). Public policing and internet crime. In Y. Jewkes, & M. Yar (Eds.), *Handbook of internet crime* (pp. 525–545). Cullompton: Willan.

Law on organization and competence of government authorities for suppression of high-tech crime. (2005, 2009). *Službeni glasnik Republike Srbije*, (61/05, 104/09).

National Center for Justice and the Rule of Law. (2007). *Combating cyber crime: Essential tools and effective organizational structures: A guide for policy makers and managers*. Retrieved from http://www.olemiss.edu/depts/ncjrl/pdf/Cyber-Crimebooklet.pdf

Specialised cybercrime units: Good practice study. (2011). Strasbourg: Data Protection and Cybercrime Division Directorate General of Human Rights and Rule of Law. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf

About the Author:

Milana Pisarić, Assistant at the University of Novi Sad, Faculty of Law; Ph.D. student at the Faculty of Law of the University of Belgrade, currently writing Ph.D. thesis "Specificities of Evidence in Criminal Procedure Relating to Cybercrime". E-mail: mpisaric@pf.uns.ac.rs