XII INTERNATIONAL SCIENTIFIC CONFERENCE "ARCHIBALD REISS DAYS"
THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE
Investigating and Proving Contemporary Forms of Crime: Scientific Approaches

XII INTERNATIONAL SCIENTIFIC CONFERENCE

"ARCHIBALD REISS DAYS"

Belgrade, 8-9 November 2022

THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE

Investigating and Proving Contemporary Forms of Crime: Scientific Approaches

University of Criminal Investigation and Police Studies
Belgrade, 2023

Publisher

UNIVERSITY OF CRIMINAL INVESTIGATION AND POLICE STUDIES
Belgrade, 196 Cara Dušana Street (Zemun)

Impression
150 copies

Printed by
Birograf, Belgrade

The conference and the publishing of proceedings were supported by the Ministry of Science, Technological Development and Inovations of the Republic of Serbia

ISBN 978-86-7020-496-6
ISBN 978-86-7020-190-3

HONORARY COMMITTEE

Zoran Đurđević, PhD, Rector of the University of Criminal Investigation and Police Studies, Belgrade, **President**

Zoran Mirković, LLD, Dean of the Faculty of Law, University of Belgrade

Lieutenant General **Goran Radovanović**, PhD, Rector of the University of Defence, Belgrade

Norbert Leitner, PhD, President of the Association of European Police Colleges

Christophe Champod, PhD, Director of the School of Criminal Justice, Faculty of Law, Criminal Justice and Public Administration, University of Laussane, Switzerland

José García Molina, PhD, Director of the National Police Academy, Ávila, Spain

Zoltán Rajnai, PhD, Dean of the Donát Bánki Faculty of Mechanical and Safety Engineering, Óbuda University, Budapest, Hungary

Cao Shiquan, PhD, President of the People's Public Security University Of China, Beijing

Hao Hongkui, PhD, President of the National Police University of China, Shenyang

Lieutenant-General of Police **Igor Alexandrovich Kalinichenko**, PhD, Head of the Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V. Y. Kikot

Major-General **Alexander Vladimirovich Travnikov**, PhD, Head of the St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation

Lieutenant-General of Police **Alexander Viktorovich Simonenko**, PhD, Head of the Krasnodar University of the Ministry of Internal Affairs of the Russian Federation

Major-General **Vladimir Ivanovich Tretyakov**, PhD, Chief of the Volgograd Academy of the Ministry of Internal Affairs of the Russian Federation

German Priorov, PhD, Faculty of Life Safety, Moscow Regional State University, Russia

Major-General of the Militia **Alexander Vasiliev**, PhD, Head of the Academy of the Ministry of Internal Affairs of the Republic of Belarus

Colonel **Roman Blahuta**, PhD, Rector of the Lviv State University of Internal Affairs, Ukraine

Iwona Klonowska, PhD, Commandant-Rector of the Police Academy, Szczytno, Poland

Lucia Kurilovská, PhD, Rector of the Academy of the Police Force, Bratislava, Slovakia

Colonel **Claudiu-Ştefan Chindriş**, PhD, Comandant-Rector of the Police Academy "Alexandru Ioan Cuza", Bucharest, Romania

Dinu Ostavciuc, PhD, Rector of the Academy "Stefan cel Mare" of the Ministry of the Interior of the Republic of Moldova, Kishinev

Andrej Sotlar, PhD, Dean of the Faculty of Criminal Justice and Security, Ljubljana, Slovenia

Yilmaz Çolak, PhD, President of the Turkish National Police Academy, Ankara

PROGRAMME COMMITTEE

Tanja Kesić, PhD, University of Criminal Investigation and Police Studies, Belgrade, **President**

Nenad Radović, PhD, University of Criminal Investigation and Police Studies, Belgrade

Aleksandar Bošković, PhD, University of Criminal Investigation and Police Studies, Belgrade

Nenad Milić, PhD, University of Criminal Investigation and Police Studies, Belgrade

Brankica Popović, PhD, University of Criminal Investigation and Police Studies, Belgrade

Radomir Zekavica, PhD, University of Criminal Investigation and Police Studies, Belgrade

Nikola Milašinović, PhD, PhD, University of Criminal Investigation and Police Studies, Belgrade

Goran Bošković, PhD, University of Criminal Investigation and Police Studies, Belgrade

TABLE OF CONTENTS

FOREWORD

The Thematic Conference Proceedings of International Significance titled "Investigating and Proving Contemporary Forms of Crime: Scientific Approaches" is the result of the XII International Scientific Conference "Archibald Reiss Days," which was held on November 8 and 9, 2022 in Belgrade and organized by the University of Criminal Investigation and Police Studies in collaboration with the Ministry of Interior of the Republic of Serbia, Ministry of Education, Science and Technological Development of the Republic of Serbia, National Police University of China, Volgograd Academy of the Russian Ministry of Internal Affairs, Lviv State University of Internal Affairs, Faculty of Security in Skopje, Faculty of Criminal Justice and Security in Ljubljana, Police Academy "Alexandru Ioan Cuza" in Bucharest, Academy of Police Force in Bratislava, and the University of Banja Luka Faculty of Security Science.

The Thematic Conference Proceedings of International Significance include papers by eminent scientists and experts from six countries who analyzed the most current issues in investigating and proving modern forms of crime, guided by scientific achievements in their respective fields of research. The papers published in the Thematic Conference Proceedings of International Significance belong to the natural-mathematical, technical-technological, and social-humanistic scientific fields and meet all of the requirements outlined in the Rulebook on Acquiring Research and Scientific Titles ("Official Gazette of RS," Nos. 159/2020 and 14/2023) for classification in category M14, i.e., thematic collection of papers of international significance. The papers are original scientific papers that have been double-blind peer-reviewed by two reviewers, the contributions are one author's sheet, and they contain the required number of self-citations in clearly stated categories according to the scientific field.

The papers critically analyze a wide range of themes relevant to scientific approaches to investigating and proving modern forms of crime, such as: hybrid control flow and dataflow architectures; analysis of DDOS attack detection techniques for securing software-defined networks; management in the prevention of malpractice in electronic refereeing systems in sports; development of latent fingermarks on different substrates using polyaniline-based powder obtained by simple precipitating method; the online drug market as a current law enforcement challenge; the possibilities of using unmanned aerial vehicles – drones in crime scene investigation; secret as an object of criminal law protection in the Republic

of Serbia; the characteristics of environmental crimes as challenges for their detection and proving; the international legal framework against corruption; historical development of the polygraph and its application in Hungary, and mobbing as a harmful present-day phenomenon.

The Thematic Conference Proceedings of International Significance is a publication that contributes significantly to the pool of scientific knowledge from a variety of scientific subfields, including computer and forensic sciences, criminology, criminal investigation, and criminal and criminal procedural law. We hope that the wider scientific and professional public will find this publication interesting and useful. Lastly, we would like to thank all of the conference authors and attendees for their contributions to both the conference's realization and the publication of the proceedings, as well as the reviewers who played a key role in the selection of scientific papers.

Belgrade, March 2023 *The Programme and Organizing Committees*

TOWARDS HYBRID CONTROL-FLOW AND DATAFLOW ARCHITECTURES

Nenad Korolija, PhD[1]
School of Electrical Engineering, University of Belgrade, Serbia

Vladisav Jelisavčić, PhD
Mathematical Institute of the Serbian Academy of Sciences and Arts, Serbia

Zlatogor Minchev, PhD
Institute of Information and Communication Technologies,
Bulgarian Academy of Sciences, Sofia, Bulgaria

Veljko Milutinović, PhD
Department of Computer Science,
University of Indiana in Bloomington, Indiana, USA

PURPOSE

According to Moore's law, number of transistors per integrated circuit doubles about every two years (Moore, 1998). This is predominantly achieved by making transistors smaller and smaller through advances in photolithography. However, the number of transistors per integrated circuit was not at its maximum at all times, but the density of transistors at which the cost per transistor was relatively close to the lowest. Namely, as the number of transistors increases, so does the probability of failure. It is well known that companies which were producing processors had even the possibility to reduce number of active cores if the production of any of cores went wrong.

For decades, the increase in frequencies of processors was almost following the Moore's law, by doubling about every two years. Unlike it is the case with increasing the number of transistors per unit measure of a surface, increasing the frequencies also increases the power consumption and therefore heating as well. It can be roughly estimated that the power consumption is proportional to the

1 nenadko@etf.bg.ac.rs

square of the integrated circuit frequency. More importantly, the increased power consumption leads to the higher cooling requirements. As a result, recent generations of central processing units (CPUs) are usually limited around 3GHz, while the number of cores keeps growing.

High performance computing (HPC) benefits from increased number of cores of today's CPUs. However, in order for an algorithm to benefit from relatively high number of available cores, the algorithm has to be scalable enough. The scalability is limited not only by properties of an algorithm, but by the architecture it is executed on. For example, by increasing the communication time between two cores, the algorithm benefits less from using multiple cores in parallel. In order to justify the usage of another core, the algorithm has to run faster by utilizing the core than it otherwise would.

Control-flow architectures, also referred to as von Neumann architectures, define the temporal sequence of individual instructions of a computer algorithm. As such, they are complex enough to be able to execute all instructions defined by the architecture. On the other hand, they can execute only a single instruction without multiplying control-flow computational units or dividing them onto instruction phases they are responsible for. One way of parallelizing instruction execution is using the pipeline. Multicore computer architectures consist of multiple control-flow type of processors that further increase the number of instructions that can be run in parallel.

So-called manycore architectures are based on control-flow principles, but the number of processing elements they include is usually couple of orders of magnitude greater than of CPUs. Processing elements are usually simpler and suitable for scalable algorithms. The primary purpose of manycore architectures was to support the necessity for fast processing in order to render screen frames in graphics demanding applications. Later, their capability of executing multiple instructions in parallel was utilized for parallelizing and therefore accelerating many control-flow applications.

Unlike it is the case with control-flow architectures, dataflow architectures are configured to execute a single algorithm before they are reconfigured for a new purpose (Trifunovic, Milutinovic, Salom & Kos, 2015). Reconfigurability is usually achieved using the Field-programmable gate array (FPGA). In the case of dataflow architectures, data literally flows through the hardware, producing results at the output based on the data received at the input. There are many advantages of this approach. For example, processing element responsible for executing a single instruction can be configured to be able to execute only that instruction. As such, processing element is less complex comparing to the control-flow architecture, and therefore smaller. Another benefit is that the data travels in parallel from any processing element producing semi-result to those that consume the result. Data-

flow architectures are suitable for executing algorithms that include considerable amount of repetition.

With raising number of transistors per chip, one could argument for combining multiple computing architectures at the same chip die, forming a hybrid architecture. Some of the benefits include reduced hardware size comparing to the size of multiple computer architectures separately, reduced power consumption, but, more importantly, improvements in communication speed between control-flow and dataflow hardware.

Multiple computer architecture paradigms available in a single desktop computer or server node impose relatively slow communication speed due to the distance between them. In addition, powering multiple architectures might require more efforts in terms of cooling comparing to the cooling of a single chip.

A hybrid control-flow and dataflow architecture on a single chip might solve these issues, enabling certain algorithms to be transformed and programmed for the execution on merged control-flow and dataflow hardware simultaneously.

Many high performance algorithms perform certain operations on a matrix of data, where edge elements are processed differently than the rest of the matrix. Auxiliary processing might be required between two consecutive processing of a matrix, where the amount of processing would be neglectable comparing to the processing of a matrix. There are few possibilities to implement this using the dataflow paradigm. One is to create separate kernels for processing middle matrix elements and edge elements, and even another one for processing corner elements. However, due to the complexity of orchestrating streams of the input data, leading them to appropriate kernels, as well as collecting results from the output of kernels, one could implement a single kernel to handle all the cases, where conditionals would be used to cope with the differences in processing. Similarly, separate kernels could handle processing of vectors between two consecutive processing of matrices, or a single kernel could be extended to handle this scenario as well. In any case, the complexity of dataflow hardware grows reasonably (e.g. could be increased more than twice), where the execution time of the CPU needed for processing edge elements and auxiliary processing is less than 1% of the total execution time that a CPU will need to process the whole algorithm. Dataflow implementation of the Lattice-Boltzmann algorithm is one example application that matches the previous scenario (Korolija, Djukic, Milutinovic & Filipovic, 2013).

The goal of this research is to exploit the possibility of merging dataflow and control-flow paradigms on the same chip die with communication speed matching those of cache memories, and to show on the example of the Lattice-Boltzmann algorithm the potential benefits.

Further sections describe control-flow, multicore, manycore, and dataflow architectures in more detail, and explain the proposed hybrid architecture. The presentation is based on the proposed method (Milutinovic, 1996), and is reviewed by authors in accordance with the proposed activity diagram (Banković et al., 2020).

DESIGN/METHODS/APPROACH

This section sheds some light on available computing paradigms used in high performance computing. Therefore, although control-flow single-core processors have been replaced by multicore processors since relatively long time ago, the paradigm will be explained, as most computer clusters and computer clouds include processors based on the control-flow.

Control-flow computer architectures are based on the principles defined by John von Neumann. First control-flow processors consisted only of a single-core, being capable of executing one instruction at any particular moment. This imposes relatively high complexity for a processor that can execute only one instruction at any given moment. The utilization of transistors raised with the introduction of pipelines that enabled executing few instructions simultaneously, but in different stages – while one instruction was being fetched, another one is being executed, and another one is writing results, etc. The improvement in the capacity of executing many instructions per second has been improving predominantly due to the constant raise of frequencies the processors operated at, approximately doubling each second year. Due to the relatively high increase in power consumption with raising frequencies, multicore processors appeared as a logical consequence, enabling faster execution at a smaller price.

Multicore computer architectures are based on the same principles as control-flow computer architectures. Unlike first single-core architectures, multicore architectures include multiple cores, where each core can execute multiple instructions simultaneously. Advances in technology of producing processors led to reducing transistor sizes. As a result, more CPUs could have fit within the same chip die. However, multicore computers suffer from the same problems as conventional single-core computers. The internal bus can become the bottleneck, as many instructions that run in parallel on a single-core, but in different phases of instruction execution, try to write results back to e.g. a cache memory or registers and to read from the memory/registers simultaneously. The number of instructions is limited by the architecture, allowing running only few instructions per core in parallel.

Advances in computer graphics in recent decades lead to defining a term many-core used for control-flow type of processing on graphics card that can include

thousands of processing units. Manycore computer architectures, or so-called graphics processing unit (GPU) processors, are based on the same principles as other control-flow processors. However, unlike it is the case with single-core and multicore processors, manycore processors can include thousands of processors. As a result, they are highly utilized for parallelizing execution of highly scalable computing algorithms. The lack of these architectures is that they are usually simpler than conventional multicore processors. Therefore, they cannot execute all instructions defined by the multicore processors. It is worth saying that computer architectures that include GPUs usually include also multicore processors, where a multicore processor is responsible for initializing the data for GPUs, starting the processing, and collecting results, while GPUs are utilized for the portion of algorithm or algorithms that are highly scalable.

Dataflow computing paradigm is based on the data flowing through the hardware (Trifunovic et al., 2015). Fig. 1 depicts an example processing implemented using the dataflow paradigm. Function elements from the figure can be observed as processing elements that are mutually connected. The memory could either be placed on the same chip with the dataflow hardware, or on a CPU that is used along with the dataflow hardware, or as a separate unit. The input data would be streamed into the dataflow hardware, and results of the execution would be streamed back to the CPU in order to be further processed or stored in the main memory.

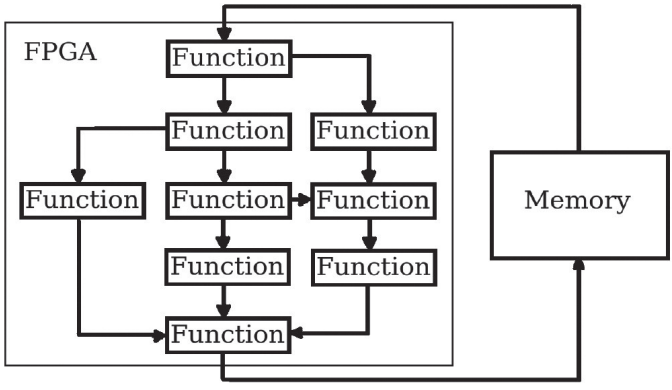


Figure 1. *Dataflow programming model*

Main benefits of dataflow hardware comparing to the control-flow hardware are the following:

- Data produced at a processing element travels directly to those processing elements that need this data. This way, many data transfers can be processed in parallel. This solves the previously mentioned problem of a bus as a bottleneck of the control-flow type of architecture.

- Processing elements are simpler than conventional control-flow type of processors, as they are utilized for a single instruction. This makes them smaller than conventional control-flow processors.
- Higher density in processing elements comparing to the manycore enables more processing elements to be placed on the same chip die. Besides that, it also affects the performance of algorithm execution directly, as the time needed to send the data from one processing element to another is nearly proportional to the distance between them.

The algorithm execution is performed using the dataflow hardware in the following steps:

- Control-flow processor prepares the data to be processed by the dataflow kernels.
- Control-flow processor initializes the dataflow hardware. In some cases, data is streamed to the dataflow kernels for processing. In other cases, the data is copied into the dataflow hardware memory, so that the data can be processed faster by kernels.
- Dataflow hardware processes the data, streaming the output back to the CPU, or streaming the results into the dataflow hardware memory that can be later read by the CPU, or another dataflow hardware kernel.
- Control-flow processor collects results of executing the dataflow hardware and processes it further.

Dataflow architectures are capable of accelerating many high performance computing algorithms (Milutinović, Furht, Obradović & Korolija, 2016). Examples include, but are not limited to, sorting (Kos, Ranković, & Tomažič, 2015) and providing biofeedback in sport (Umek & Kos, 2016).

However, compared to the control-flow applications, developing dataflow applications usually requires more time due to the constraints imposed by the dataflow hardware. These constraints lead to considerably higher programmer task-type efforts (Popovic, Bojic & Korolija, 2015), especially with non-functional requirements (Popović, Korolija, Marković, & Bojić, 2017).

Application-specific integrated circuit (ASIC) is an integrated circuit (IC) chip capable of executing on a hardware the algorithm that the hardware is designed for. Algorithms for ASIC can usually be implemented using the dataflow programming model. As a result, ASIC is expected to be highly optimized, allowing many instructions to be executed in parallel. Example include Google Cloud Tensor Processing Units (TPUs) used for machine learning algorithms. This kind of architecture can exist in a cluster or cloud, where one could expect a range of algorithms utilizing the dedicated hardware, but it is not that common in desktop

computers, as it is hard to justify why an ordinary user would have the need for a specialized hardware for multiple algorithms.

In contrast to ASIC, dataflow architectures based on FPGAs can be reconfigured, so that they can support implementation of many algorithms using the dataflow paradigm. One of the biggest challenges in developing algorithms for dataflow architectures is the configuring of FPGAs. Researchers have developed a method for automatically translating algorithms from the control-flow to dataflow paradigm (Milutinovic et al., 2017; Korolija, Popović, Cvetanović & Bojović, 2017). Although the dataflow paradigm exists since 1960s, programmers are usually specialized in programming control-flow architectures. Most of the computer programs are written for computer architectures based on control-flow. The same applies to the development of compilers and frameworks. Authors of this manuscript believe that recent advances in dataflow architectures along with the raise of the need for machine learning algorithms will lead to the increase in usage of dataflow architectures and the percentage of programming community educated for dataflow programming.

HPC solutions can include a wide range of building blocks, from custom motherboard designs, to system configurations, rack designs along with cooling systems, etc. At the beginning of HPC, most HPC solutions were built for general purpose compute intensive workloads, and were used for various purposes such as digital manufacturing, banking services, medical research, oil and gas production, etc. Today's HPC architectures can include relatively high amount of racks filling a big room with multiple nodes per rack (e.g. around 100) and thousands of processor cores per rack. In terms of computing paradigms, HPC architectures may include dataflow cards attached on some or all nodes, but they almost always include control-flow type of processors, including multicore processors and, optionally, manycore processors.

For already decades, the frequencies of processors are not doubling any more. Instead, the transistor count per chip die is increasing, which allows putting more and more cores onto a single chip die. Authors of this manuscript believe that, in the near future, it will be beneficial for the processor to include not only few cores, but in addition manycore architecture and dataflow architecture. Such a hybrid processor can have higher communication speed between the control-flow and the dataflow hardware, since they could share the same cache, or communicate directly using the internal bus. The chip could also include Network on chip (NoC), ethernet support, and appropriate control logic. Fig. 2 depicts a hybrid control-flow and dataflow computer architecture on a single chip die.

The idea of combining control-flow and dataflow hardware on the same chip die is not new (Yazdanpanah, Alvarez-Martinez, Jimenez-Gonzalez & Etsion, 2013). Researchers have achieved an average speedup factor of 3 to 11 over an NVIDIA GPGPU, while having better energy efficiency (Voitsechov & Etsion, 2015). There

is a research that proposes including also Internet of things on the same chip die (Milutinović et al., 2021). Efforts on combining control-flow and dataflow architectures can be roughly divided onto:

- Solutions including control-flow hardware with a software dataflow;
- Control-flow hardware controlling distant dataflow hardware usually accessed via PCIe bus.

One of the key benefits of the proposed architecture is that it allows defining computer architecture in the run time by defining a set of instructions that the architecture will be capable of executing, where these instructions could be executed much faster than it would be possible on a conventional CPU. For example, one could configure FPGAs for certain instructions, and automatically generate the compiler for such an architecture, where instructions supported by the dataflow hardware would execute on the dataflow hardware, while other instructions would be executed using one of the CPUs. This feature is not explored in more detail in this manuscript.

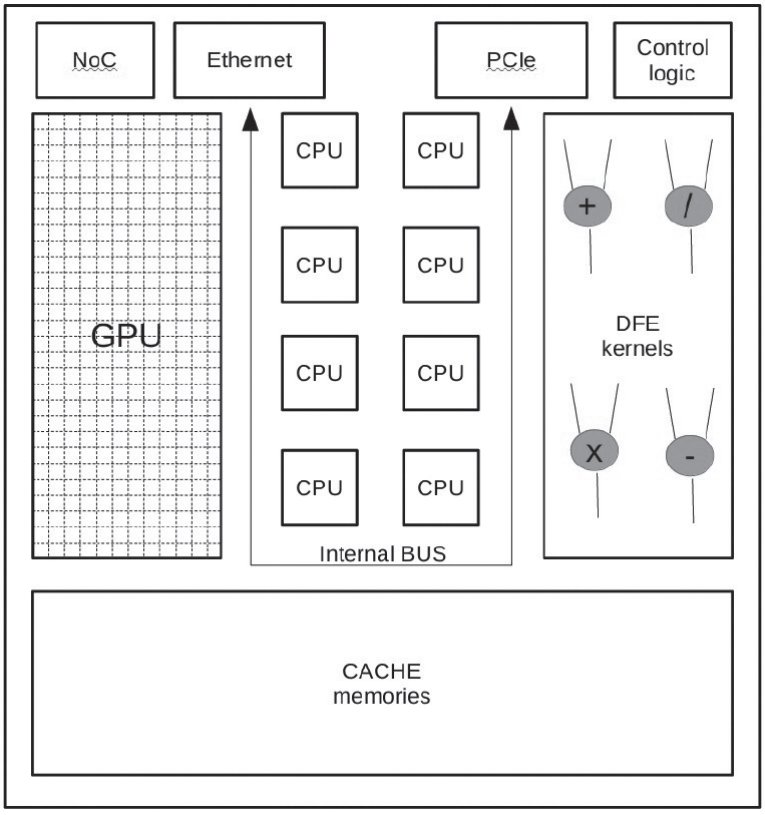


Figure 2. *Hybrid control-flow and dataflow computer architecture*

Control logic would need to be much more sophisticated comparing to the existing to support cache sharing across heterogeneous architectures. Similar problem was already tackled with the research that, to some extent, splits temporal and spatial cache data (Sustran, Rakocevic, Milutinovic, 2015), proving that such a concept is implementable.

FINDINGS

The analysis of the potentials for accelerating algorithms using the proposed hybrid computer architecture is divided into four stages. First, the communication speed between the control-flow and the dataflow hardware is calculated and compared to the speed of PCIe bus. Second, the benchmark is defined by analyzing open source implementations of dataflow algorithms for the same dataflow hardware type. Third, the simulation analysis is performed assuming various ratios of jobs from the benchmark. Fourth, the comparison between the proposed hybrid architecture and existing architectures is performed.

The communication speed of the PCIe 6.0 is 128GB/s, where the latency is less than 10ns. If the hybrid architecture has similar cache to the one of processor i9-9900k, running at 3.6GHZ, the L3 cache speed would be 300GB/s with the latency around 11ns, and the L1 cache speed would be around 3TB/s with the latency of 0.8ns. The speed of communication with the main memory is 47GB/s with the latency of 45ns. In the most rigorous approach, one could expect the dataflow hardware to be connected with the manycore architecture over the L3 cache (not L1 or L2), resulting in the communication acceleration factor of 2,34375 comparing to the PCIe 6.0.

In order to provide a fair comparison, first four dataflow applications from the Application gallery available in the open literature (Trifunovic, Milutinovic, Korolija & Gaydadjiev, 2016), for which there were enough data to estimate the possibility for acceleration using the proposed hybrid architecture, are chosen.

First application is Huxley muscle model with claimed acceleration factor of around 33. As the problem size is not given for this application, the worst case is considered, which includes neglectable amount of edge elements comparing to the total number of elements to be processed. Therefore, assuming that the edge elements can be calculated using the manycore architecture, the middle elements can be calculated using simpler kernels. Current dataflow implementation of the Huxley muscle model includes four conditional arithmetical statements out of the total of 14 arithmetical statements that include these four as well. CPU execution time varies between 5s and 60s. For the four conditional arithmetical statements, it is estimated that they can be accelerated by the factor of two in the case there is

no need to check for boundary conditions. It is also assumed that the complexity of arithmetical statements doesn't vary. The total acceleration possibility is roughly calculated as a reduction from 14 to 12, i.e. the acceleration factor is around 1,167. This is the worst case application, as boundary elements are not included into the calculation, neither the speed of the communication between the control-flow and the dataflow hardware.

The second application is Poisson solver. It can be measured only for 32x32x32 space as input, because for greater input design cannot fit. The acceleration factor is claimed to be around 124. From the total input space, there are 32*32*6 - 8*2 edge elements, which is 18.7%. If we run 18.7% of calculations using the manycore architecture, and (1–0,187)% using the dataflow architecture, we will achieve the acceleration factor of 1.23, assuming that manycore architecture can process these 18.7% of data in parallel with dataflow hardware processing the rest of the data.

The third application is Simplex. The bottleneck for both implementations is the bandwidth between the control-flow and the dataflow hardware. The acceleration factor is claimed to be around 5. According to the acceleration graph based on the problem size, the steep curve flattens at about 5, resulting in the limited acceleration for problems of sizes greater than 10 to the power of four. If the communication speed is 2.34 times faster, the resulting acceleration factor would be 11.7, while the relative acceleration introduced by the proposed hybrid architecture would be 2.34.

The fourth dataflow application is Network sorting. The acceleration factor is claimed to be in the ranges between 7 and 12, if the sorting times include communication delays between the control-flow and the dataflow hardware, and between 100 and 160 when considering only the sorting time inside the FPGA. If we consider the mathematical average accelerations of 9.5 and 130 for both scenarios respectively, the difference of 120.5 corresponds to the communication. If we multiply the acceleration with the communication included by 2.34, this will result in 22.2 acceleration factor with the communication included. Compared to the acceleration factor of 130 in the case that no communication is performed, one can conclude that even with the proposed hybrid model the communication speed would still be the bottleneck.

In average, the acceleration factor for all dataflow applications from the benchmark is around 1.77. By tuning the ratio between dataflow jobs, it can reach close to the 2.34, or drop to 1.17. However, there is a threat to validity due to relatively small subset of dataflow applications that are used in the evaluation of the proposed hybrid architecture, but the simple analysis reveals that there are potentials to accelerate the dataflow application, whose bottleneck is in the communication between the control-flow and dataflow hardware, by the factor of 2.34 or even more.

Some of the potentials of combining control-flow and dataflow architectures are already known (Milutinović, Trifunović, Korolija, Popović & Bojić, 2017). Authors have also been working on recovering network connectivity structure, developing a very fast Scale-Free Networks Estimation Through Cholesky factorization (SNETCH) optimization algorithm based on coordinate descent. This highly parallelizable algorithm is suitable for dataflow architectures. The topological problem it solves can be matched in detecting crimes (Jelisavcic, Stojkovic, Milutinovic & Obradovic, 2018). Dataflow processing can improve video surveillance in terms of better real-time face recognition (Bhowmik, Garcia, Wallace, Stewart & Michaelson, 2017), but also in terms of tracking subjects based on video streams from multiple locations, reducing the total power consumption at the same time.

Another advantage of the proposed hybrid architecture compared to the typical dataflow architectures that are connected to CPUs is in the fact that the dataflow hardware can be better utilized, since only those parts of algorithms that are executed repeatedly again could be executed using the dataflow hardware, while instructions that are not that often executed could be executed using the many-core. As an example, the Lattice-Boltzmann algorithm predominantly calculates matrix element values. The processing differs for the elements in four corners of the matrix from those belonging to edges of the matrix, and the rest of elements require different processing. Although this processing doesn't differ much, and can be achieved using a single dataflow kernel, this kernel has higher complexity and more electrical power and time is required for processing a single value.

When it comes to using the proposed hybrid architecture in a computer cluster, one can think of dividing the matrix by X and Y coordinates onto multiple hybrid processors that would be responsible each for their own domain of data. As a result, edge and corner elements would have to be exchanged with neighborhood processors so that the time needed for processing these elements and the communication with neighborhood processors differs by orders of magnitude from the time needed to process matrix elements that can be processed independently from other processors.

The additional constraint to using the proposed hybrid architecture in clusters is scheduling for hybrid control-flow and dataflow architectures. Researchers have developed relatively fast scheduling algorithms comparing to the usual duration time of dataflow jobs (Korolija, Bojic, Hurson & Milutinovic, 2022).

One important aspect of the combined control-flow and dataflow hybrid processor is the expected lifetime and counterfeit detection. The duration is expected to be around the shortest lasting from the three incorporated architectures, and the possible counterfeit hybrid processor chips could be identified using existing statistical methods (Huang, Liu, Korolija, Carulli & Makris, 2015).

ORIGINALITY/VALUE

This manuscript presents relevant aspects of control-flow and dataflow paradigms for running scalable algorithms in parallel, and advocates for a hybrid hardware available on the same chip die.

The control-flow computing paradigm assumes that the computer architecture is able to execute any of the instructions defined by the instruction set at any given moment. This imposes that the hardware must be relatively complex comparing to the one needed for executing a single instruction. Modern trend is increasing the number of processing units within a central processor or graphics card, often referred to as multicore or manycore GPUs, respectively. This increases the parallelism of scalable algorithms, but the number of transistors divided by number of instructions that can run in parallel is still relatively high.

Dataflow paradigm reduces this number by an order of magnitude or more by allowing data to flow through the hardware. The downsides of using the dataflow paradigm are that one needs to configure the dataflow hardware and that the control-flow type of processor is usually needed for initialization of the data, starting the dataflow hardware, and collecting results. Communication lag between control-flow and dataflow hardware reduces the possibility of parallelizing certain algorithms that have low computation to communication ratio.

Hybrid multicore, manycore, and dataflow computer architecture can fit within a single chip. As a result, the communication speed drops comparing to the communication between a processor and a distant dataflow hardware. This offers new possibilities in terms of algorithms that can be accelerated using both paradigms, but also in terms of execution times of algorithms for the dataflow architectures. Authors believe that this can improve important aspects of modular technical system modelling and real-time analysis of complex signals obtained from multiple locations (Minchev and Atanassov 2005; Popivanov et al., 2006).
The idea of combining multiple computing paradigms in order to accelerate high performance computing algorithms is not new, but the presented work sheds light on one possible implementation of the chip that includes both multicore, manycore, and dataflow architecture. Based on real problems that are implemented for dataflow paradigm using a single framework, and the appropriate scheduling algorithm, the presented approach proved to have potentials to accelerate certain high performance algorithms by factors higher than two, reducing the energy consumption at the same time.

ABBREVIATIONS

CPU – Central processing units

HPC – High performance computing

FPGA – Field-programmable gate array

GPU – Graphics processing unit

ASIC – Application-specific integrated circuit

IC – Integrated circuit

TPU – Tensor Processing Unit

NoC – Network on chip

SNETCH – Scale-Free Networks Estimation Through Cholesky factorization

REFERENCES

Moore, G. E. (1998). Cramming more components onto integrated circuits. Proceedings of the IEEE, 86(1), 82–85.

Trifunovic, N., Milutinovic, V., Salom, J., & Kos, A. (2015). Paradigm shift in big data supercomputing: dataflow vs. controlflow. Journal of Big Data, 2(1), 1–9.

Korolija, N., Djukic, T., Milutinovic, V., & Filipovic, N. (2013). Accelerating Lattice-Boltzman method using Maxeler dataflow approach. The IPSI BgD Transactions on Internet Research, 34.

Milutinovic, V. (1996). The best method for presentation of research results. IEEE TCCA Newsletter, (9), 1–6.

Banković, M., Filipović, V., Graovac, J., Hadži-Purić, J., Hurson, A. R., Kartelj, A., ... & Živković, M. (2020). Teaching graduate students how to review research articles and respond to reviewer comments. In Advances in Computers (Vol. 116, No. 1, pp. 1–63). Elsevier.

Milutinović, V., Furht, B., Obradović, Z., & Korolija, N. (2016). Advances in high performance computing and related issues. Mathematical problems in engineering, 2016.

Kos, A., Ranković, V., & Tomažič, S. (2015). Sorting networks on Maxeler dataflow supercomputing systems. In Advances in Computers (Vol. 96, pp. 139–186). Elsevier.

Umek, A., & Kos, A. (2016). The role of high performance computing and communication for real-time biofeedback in sport. Mathematical problems in engineering, 2016.

Popovic, J., Bojic, D., & Korolija, N. (2015). Analysis of task effort estimation accuracy based on use case point size. IET Software, 9(6), 166-173.

Popović, J., Korolija, N., Marković, Ž., & Bojić, D. (2017, November). The influence of non-functional requirements in UCP method on the accuracy of effort estimates. In 2017 25th Telecommunication Forum (TELFOR) (pp. 1–4). IEEE.

Milutinovic, V., Salom, J., Veljovic, D., Korolija, N., Markovic, D., & Petrovic, L. (2017). Transforming applications from the control flow to the dataflow paradigm. In Dataflow supercomputing essentials (pp. 107–129). Springer, Cham.

Korolija, N., Popović, J., Cvetanović, M., & Bojović, M. (2017). Dataflow-based parallelization of control-flow algorithms. In Advances in computers (Vol. 104, pp. 73–124). Elsevier.

Yazdanpanah, F., Alvarez-Martinez, C., Jimenez-Gonzalez, D., & Etsion, Y. (2013). Hybrid dataflow/von-Neumann architectures. IEEE Transactions on Parallel and Distributed Systems, 25(6), 1489–1509.

Voitsechov, D., & Etsion, Y. (2015, December). Control flow coalescing on a hybrid dataflow/von Neumann GPGPU. In Proceedings of the 48th International Symposium on Microarchitecture (pp. 216–227).

Milutinović, V., Azer, E. S., Yoshimoto, K., Klimeck, G., Djordjevic, M., Kotlar, M., ... & Ratkovic, I. (2021, June). The ultimate dataflow for ultimate supercomputers-on-a-chip, for scientific computing, geo physics, complex mathematics, and information processing. In 2021 10th Mediterranean Conference on Embedded Computing (MECO) (pp. 1–6). IEEE.

Sustran, Z., Rakocevic, G., & Milutinovic, V. (2015). Dual Data Cache Systems: Architecture and Analysis. Advances in Computers, 96.

Trifunovic, N., Milutinovic, V., Korolija, N., & Gaydadjiev, G. (2016). An AppGallery for dataflow computing. Journal of Big Data, 3(1), 1–30.

Milutinović, V., Trifunović, N., Korolija, N., Popović, J., & Bojić, D. (2017, November). Accelerating program execution using hybrid control flow and dataflow architectures. In 2017 25th Telecommunication Forum (TELFOR) (pp. 1–4). IEEE.

Jelisavcic, V., Stojkovic, I., Milutinovic, V., & Obradovic, Z. (2018). Fast learning of scale-free networks based on Cholesky factorization. International Journal of Intelligent Systems, 33(6), 1322–1339.

Bhowmik, D., Garcia, P., Wallace, A., Stewart, R., & Michaelson, G. (2017). Power efficient dataflow design for a heterogeneous smart camera architecture.

Korolija, N., Bojic, D., Hurson, A. R., & Milutinovic, V. (2022). A runtime job scheduling algorithm for cluster architectures with dataflow accelerators. Advances in Computers, 201.

Huang, K., Liu, Y., Korolija, N., Carulli, J. M., & Makris, Y. (2015). Recycled IC detection based on statistical methods. IEEE transactions on computer-aided design of integrated circuits and systems, 34(6), 947–960.

Popivanov, D., Stomonyakov, V., Minchev, Z., Jivkova, S., Dojnov, P., Jivkov, S., Christova, E., & Kosev, S. (2006). Multifractality of decomposed EEG during imaginary and real visual-motor tracking. Biological Cybernetics, 94(2), pp. 149–156.

Minchev, Z., & Atanassov, K. (2005). On the possibility for generalized nets modelling of modular robotic system. Advanced Studies on Contemporary Mathematics, 10(2), pp. 169–174.

ANALYSIS OF DDoS ATTACK DETECTION TECHNIQUES FOR SECURING SOFTWARE-DEFINED NETWORKS

Danijel Čabarkapa, MSc[1]
Academy of Professional Studies Šabac, Serbia

Brankica Popović, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Petar Čisar, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Kristijan Kuk, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

INTRODUCTION

Some serious problems arise in the traditional TCP/IP networks, such as the limitations of standardized equipment that runs proprietary software, the difficulty of deploying and managing, the complexity of congestion control, and the large number of applications that create network bottlenecks. Today, network systems are becoming more complex and feature-rich, and network designers often need to modify network software to achieve their requirements (Dudeja, R. K. et al., 2022). The Software-Defined Networking (SDN) paradigm breaks vertical integration by radically separating the packet forwarding and the control plane, providing applications with a centralized and abstract view of network distribution. SDN attempts to move as much network functionality as possible into user-definable software, making more of the network system components programmable. Network virtualization is one of the key features facilitated by the SDN, and it allows multiple virtual networks and the SDN controllers to share the same physical network infrastructure (Villota et al., 2018).

1 d.cabarkapa@gmail.com

However, with the popularity of SDN, their security has become one of the key research subjects. The recent changes in the cyber threat scope indicate the increased activities of cybercriminal communities mostly focusing on malware, Web-based attacks, DDoS attacks, and various social engineering attacks. Today malware, ransomware, DDoS attacks, and phishing are the most important security threats particularly dangerous in SDN due to their strong destructiveness, simple implementation, and lack of simple and feasible countermeasures (Dong S. et al., 2019). Considering the SDN network programmability and automation, the question of how to develop more efficient defense solutions against DDoS in SDN has attracted intense research in recent years. There is a fact that there are different types of DDoS attacks on SDN and therefore any effort to secure those networks requires a comprehensive understanding of SDN architecture and recent technological advances used to address security issues.

From the perspective of the SDN which is a flow-based network model, we can classify DDoS attacks into two major types: attacks based on the volume of packets, and attacks based on the number of flows. Novel DDoS detection techniques are mostly flow-based, and with an aid of specific approaches can provide faster and more accurate results. Entropy-based network traffic anomaly detection techniques are attractive due to their simplicity and applicability in a real-time network environment. The main issue of the entropy approach is the fine-grained traffic analysis, accuracy of traffic variation detection, and the choice of the features that would provide accurate detection (Ibrahim J. et al., 2022). Machine learning (ML) algorithms can automatically build classification models based on training data, and classify traffic based on the features of flows. The authors' contribution in this paper involves presenting the problem and making an overview of protection against DDoS detection in SDN networks that encompasses techniques for entropy-based data processing and ML attack detection. We have extended the entropy-based attack detection approach with the anomaly classification method to ensure that the attack traffic can be identified quickly and effectively. A certain number of research papers show that the combination of the entropy approaches in the SDN traffic data processing and ML classification algorithms for attack detection are in line with the needs of the enterprise environments, which are specifically attractive for DDoS attacks.

The other part of this paper is organized as follows. Section 2 gives an overview of DDoS attack mechanisms and taxonomy. SDN layered architecture, virtualization, and DDoS security solutions for each of the three planes in SDN and they are discussed in Section 3. Section 4 addresses a brief introduction to the used entropy-based traffic analysis and DDoS attack detection and a discussion on the ML attack detection systems. In Section 5 we highlight some experimental works related to entropy and ML-based DDoS detection mechanisms. The conclusion of the paper is in Section 6.

DDoS ATTACKS OVERVIEW

DDoS attack aims at disrupting the availability of resources in the network. This task is achieved by a group of devices that are knowingly or unknowingly involved in the attack. Malicious user floods the network resources with a large amount of useless traffic to exhaust them as a result, malicious traffic gets served but legitimate packets starve for services because of packet overflow or congestion.

The operation of DDoS attacks follows several consecutive phases. The intruder initially starts to compromise multiple agent machines that are widely distributed geographically by scanning the vulnerabilities in these devices. Once an intruder successfully identifies certain system vulnerabilities, he can compromise these machines using a malicious program. By replicating the malicious file in multiple agents, the intruder can control many devices that can reach several thousands or millions (commonly referred to as bots) to initiate DDoS attacks without the awareness of the rightful owner of the device. The discovery of vulnerabilities and exploitation process of the agents are usually performed automatically, for instance, by sending e-mail messages with the attack code attachment. The groups of bots, known as a botnet can get orders remotely from an intruder, i.e. botmaster. The botmaster can perform large-scale DDoS attacks to flood a legitimate service or network by sending a control command to the botnet agents to generate useless traffic without getting noticed. Consequently, the victim resources become overwhelmed with a crushing volume of traffic in a short duration, which significantly slows down the system service or the ability of the network to respond to legitimate users (Gupta B. et al., 2009).

DDoS attacks could be broadly classified as volume-based attacks, protocol-based attacks, and application-based attacks (Zargar S. et al., 2013; Bonguet, A. et al., 2017). A taxonomy of some common types of DDoS attacks is presented in Fig. 1.

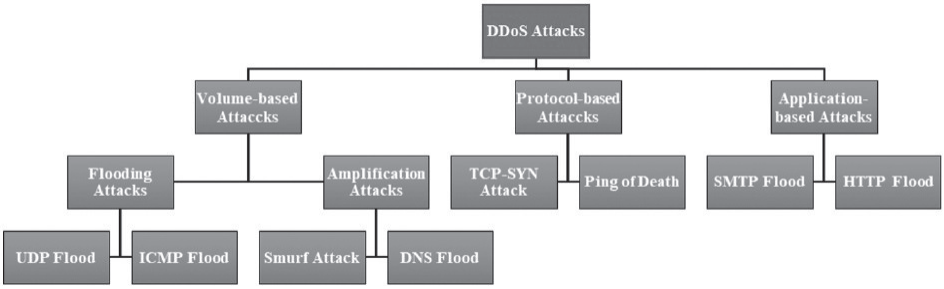


Figure 1. *Taxonomy of DDoS attacks (adopted from [4])*

In a volume-based (volumetric) DDoS attack, the target is flooded with heavy traffic, aiming at exhausting its bandwidth. It results in congesting the bandwidth of attacked target. These attacks include flooding and amplification attacks (Ding

D. et al., 2021). There are three common types of volumetric flood attacks: User Datagram Protocol (UDP) flooding, Domain Name System (DNS) flooding, and Internet Control Message Protocol (ICMP) flooding. Amplification attacks exploit a disparity in bandwidth consumption between an attacker and the targeted network resource. Protocol-based DDoS attacks exhaust the resources of devices by exploiting the network protocols. These attacks do not rely on the volume of traffic but on the combination of traffic that could affect the application. TCP-SYN flood and Ping of Death are examples of such attacks. Application-based DDoS attacks aim at crashing the application or underlying device itself by exploiting application layer protocols. Such attacks include Hypertext Transfer Protocol (HTTP) flooding and Simple Mail Transfer Protocol (SMTP) flooding (Zhou L. et al., 2022).

TCP-SYN flood attack exploits the 3-way handshake protocol of TCP. The targeted host receives SYN messages from the attacker, opens a TCP connection with it and waits for acknowledgement (ACK) message, but it never gets the response as the attacker never replies or the request is sent from spoofed IP addresses. The host keeps on waiting for replies, resulting in DDoS to legitimate requests. HTTP flood attack does not require spoofed addresses or a high amount of data to be sent to attack a server. Simple HTTP requests GET and POST are sent requiring a huge amount of data in response consuming a large amount of bandwidth and taking down the server. These attacks are the most common DDoS attacks, as they are difficult to detect. In UDP flood attack, the attacker sends a large number of packets to random ports on the target and the targeted host constantly checks for applications on that port. As no listening application on that port is found, it replies with ICMP destination unreachable packet. This process consumes more resources, ultimately making the host unreachable. In Ping of Death, the attacker sends malicious packets to the target. In general, the maximum allowed packet size with a header is 65.535 bytes, and the Ethernet frame size is 1500 bytes. Attacker sends an ICMP echo-request (ping) with more than 65.535 bytes that may cause memory buffer overflow at the target host while reassembling the packet, resulting in DDoS to legitimate packets.

SOFTWARE-DEFINED NETWORKING ARCHITECTURE AND DDoS SECURITY MECHANISMS

The architecture of a SDN network can be divided into three planes: data plane, control plane, and application plane (Cabarkapa D. et al., 2022) considering a three-layer SDN architecture model, as we can see in Fig. 2. The control plane contains one or more logically centralized SDN controllers where the logic is centralized, as well as the global view of the network. Such a control plane manages the network, including applications in the application plane and the OpenFlow

switches in the data plane. Control functionality is removed from network devices, which will become simple packet forwarding network nodes. The application plane contains SDN applications that are intended to perform various functionalities: enforcing security mechanisms, performing network traffic management and virtualization, or running services on the SDN. SDN application plane consists of one Application Logic module and one or more NorthBound Interface (NBI) Drivers. The SDN is programmable through applications that interact with the underlying data plane devices. Higher-level logic can be implemented directly through these applications on top of controllers, which communicate through NBI Agents APIs (REST, JSON, etc.) (Zhou W. et al., 2014). The SDN Datapath comprises a SouthBound Interface (SBI) Agent and a set of one or more traffic forwarding engines and processing functions. The data plane is the combination of forwarding devices managed by the control plane through its SBI that implements the OpenFlow protocol.

OpenFlow is the most widely accepted and deployed SBI standard for SDN and represents a protocol that is used for the communication between the controller and forwarding devices. An OpenFlow protocol can handle high-level routing, packet forwarding, and secure connection between the control plane and data plane. The main component of a SDN network is the OpenFlow switch. The OpenFlow switch specification determines the components and basic functions of the SDN-enabled switch. OpenFlow switch consists of one or more flow tables. Flow tables determine data processing and forwarding with the help of flow entries. Each flow entry determines how data will be processed and forwarded in a network (Open Networking Foundation, 2015).

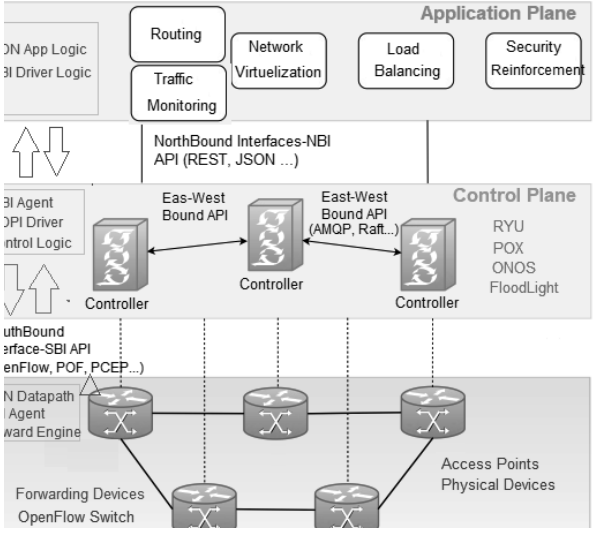


Figure 2. *Overview of a typical layered SDN architecture (adopted from [6])*

A fundamental characteristic of SDN is the logically centralized, but physically distributed controller component. The controller maintains a global network view of the underlying forwarding infrastructure and programs the forwarding entries based on the policies defined by network services running on top of it. The controller tracks the topology by learning the existence of OpenFlow switches and other SDN devices and by tracking the connectivity between them. All the controller functions are implemented via changeable modules, and the feature set of the controller may be adjusted to specific requirements of SDN networks. Currently, there is a variety of open-source SDN controllers available for the community: POX, RYU, FloodLight, ONOS, ODL, OpenDayLight, etc. (Berde P. et al., 2014; POX Github). To evaluate the controller performance in a detailed way, the paper (Cabarkapa D. et al., 2021) presented different performance aspects of the RYU and POX controller, such as throughput and latency, under simple tree-based and complex fat-tree-based network topologies. Work (Shalimov A. et al., 2013) presented a framework named HCprobe to compare seven different SDN controllers. To compare the effectiveness of these controllers, the authors performed additional measurements like scalability, reliability, and security along with latency and throughput.

The network virtualization (NV) process lies at the basis of SDN architecture. The SDN and the overlay concept were devised to adapt the network to global virtualization, as well as the necessary advanced technologies in software-defined data centers (Čisar P. et al., 2018). NV is one of the key features enabled by the SDN, and it allows multiple virtual networks and the SDN controllers to share the same physical network infrastructure. With the addition of NV techniques SDNs have gained a new dimension. This has allowed network slicing and multi-tenant hosting on existing physical network resources. FlowVisor (Sherwood, R. et al., 2009) is the most popular SDN-based implementation to utilize virtual networks by leveraging OpenFlow functionality to abstract the underlying hardware.

Security becomes more critical in the underlying SDN infrastructure and the rapid increase in the number of devices connected to the SDN networks not only increasing the data traffic but also raising concerns on security aspects of communications. SDN provides increased security features as the network control plane is detached from the forwarding plane and is programmed directly by the controller. Flow rules in the OpenFlow switches can be effectively modified for mitigation purposes. Due to SDN's programmable nature, whenever a malicious activity is detected in the network, required programs can be implemented for dealing with the malicious activities. However, this innovation also introduces various security challenges. Generally, DDoS attacks have become major threats to SDN networks. In such attacks, by exhausting resources, SDN application services are disabled, and the network performance is downgraded. Potential attacks can be executed in all three planes of

SDN architecture, and the DDoS attacks are divided into three categories: application-layer, control-layer, and data-layer attacks (Jimenez M. et al., 2021).

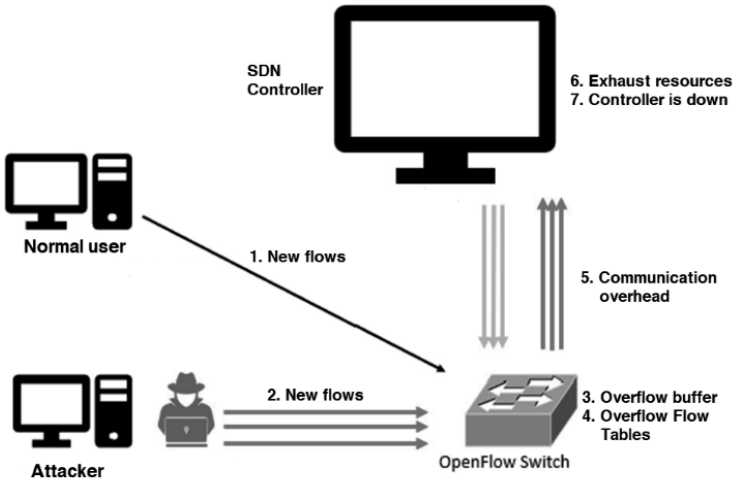


Figure 3. *Schematic view of DDoS attack in SDN (adopted from [16])*

DDoS attacks on the SDN controller are launched by sending a massive amount of network traffic with spoofed source IP addresses from different sources, as shown in Fig. 3 (1 and 2). These spoofed IP addresses do not match any existing flow rules in the flow table of the switch, resulting in a table miss case. Such a case results in generating massive packet-in messages sent to the SDN controller from the victim switch, which consumes communication bandwidth, memory, and CPU in both the control and the data plane of SDN. Since the victim switch buffers packet-in messages before sending them to the controller, if several new flows are received within a very short time, the buffer fills up (3). This results in higher consumption of the control plane bandwidth and delays the installation of new flow rules received from the controller. The forwarding table fills up, and therefore, upon receiving a new flow rule from the controller, it is unable to install it and hence dropping the packet (4). The switch would not be able to forward packets until there is free memory in its forwarding table, resulting in delays and dropping of incoming packets. On the controller side, a high arrival rate of packet-in messages exceeding the controller processing capability results in overwhelming the controller and making it unreachable to legitimate traffic (5, 6, and 7). This could fail the entire SDN network. Table 1 presents a few DDoS attacks possible on various SDN layers. Some of the DDoS attacks that are specific for the SDN networks are: buffer saturation attacks, flow table overflow, and resource exhausting (NBI interface, OpenFlow bandwidth, or TCAM memory of switches).

Table 1. An overview of DDoS attacks on SDN planes

SDN Plane	Possible attacks
Application plane	NBI API exhaustion, Application layer DDoS (HTTP flooding, SMTP flooding)
Control plane	Resource depletion, OpenFlow bandwidth exhaustion, Amplification attacks
Data plane	TCAM exhaustion, Switch DDoS, Traditional DDoS (TCP-SYN flood, TCP flood, ICMP flood …)

ENTROPY AND MACHINE LEARNING-BASED DDoS ATTACKS DETECTION IN SDNS

Entropy is a degree of the uncertainty and randomness of a certain stochastic process. In network traffic analysis entropy can measure the randomness of packets entering the network. Entropy-based techniques rely on the traffic feature distribution and are categorized as (1) TCP header-based (including IP addresses, ports, or flags) (2) volume-based (including IP or port-specific percentage of flows, packets, and bytes), and (3) behavior-based (dealing with the degree of inbound and outbound communications). In anomaly detection techniques entropy is used to present the level of randomness in a data distribution. The changes in a data structure in a distribution obtained from the acquisition process will change the entropy value. If the entropy change is significant, it is considered to be unusual behavior in network communication or an anomaly, which often indicates security threats. The main issue of the entropy approach is the accuracy of traffic variation detection and the choice of the features that would provide accurate detection.

For proper functioning of the entropy calculation, the flow-based anomaly detection relies on the Shannon information entropy H_{IE} given in equation (2):

$$p_i = \frac{x_i}{\sum_{i=1}^{N} x_i} \quad 0 \leq p_i \leq 1 \tag{1}$$

$$H_{IE}(X) = -\sum_{i=1}^{N} p_i \log(p_i) \tag{2}$$

The variable X_i represents the destination IP address of the *i-th* packet, and the empirical probability p_i of X_i is calculated by using equation (1). The total number of packets in the window is denoted as N and $i = 1, 2, \ldots N$. A window is an interval for which entropy is to be calculated and consists of a certain number of incoming packets (window size) and a fixed time interval.

The entropy threshold value is determined based on the entropy fluctuation in normal traffic scenarios. When multiple incoming data packets are received on the same switch/host port in a window and the number of data packets exceeds the size of the window, DDoS attacks are detected. If the entropy value is higher than or equal to the threshold, the next calculation will be carried out normally and entropy calculation for new incoming packets is performed. If the entropy value falls below the threshold, the incoming packet is recorded. During an attack, if the computation entropy of a specified window continuously drops below the threshold, the target port on the specified switch is blocked. The main issue of the entropy approach is the accuracy of traffic variation detection and the choice of the features that would provide accurate detection. To better characterize entropy deviation, some research papers have also used normalized entropy values (Tsallis and Rényi) relative to the margin of tolerance, allowing entropy analysis more directly (Basicevic I. et al., 2021). Several traffic features (e.g., flow size, source/destination ports, IP addresses, etc.) have been suggested as candidates for entropy-based anomaly detection. However, there may be difficulties in understanding the analysis capabilities provided by a set of entropy metrics used in conjunction with one another. The information entropy determination can quickly process a large amount of traffic data with little cost of calculation, but its accuracy relies on the selection of the threshold and it has certain drawbacks.

Recently, the implementation of ML techniques in network design, security, and management has provided the possibility of generating new network applications. ML tries to construct models that can learn to make decisions directly from data without following predefined rules. Data from past experiences is provided as input to the ML algorithm, which extracts patterns and builds a model to represent the data. This model describes the existing patterns in the data, so when it is given new unknown data, it should be able to make well-informed decisions. ML-based Intrusion Detection System (IDS) learns to classify events into the appropriate classes (normal or attack activity) based on experience given by the training set of rules. Each record, i.e. instance in the training set is represented by a given set of features and a class label indicating the attack type that the instance represents. Training sets for network attack detection contain records about network connections formed from the raw traffic data gathered from the network. Once trained and validated, the detection system is capable to detect both the attacks described in the database and their modifications, the attacks previously unknown to the system.

Detection of DDoS attacks at a proper time is crucial to protect normal activities on the SDN network. The important fact for any DDoS detection solution is distinguishing between legitimate traffic and DDoS attack traffic. It gets more challenging when the network is congested with legitimate traffic, and there is a need to segregate attack traffic safely without affecting the regular traffic. In such

cases, using statistical thresholds or a policy-based approach to detect threats may be inaccurate. This promotes the development of ML-based algorithms to categorize network data as either benign or malicious. Self-learning features of ML algorithms improve the efficiency of the detection strategy. ML-based DDoS detection usually involves the following three major steps, as shown in Fig. 4: (a) data preprocessing phase (b) training phase, and (c) testing phase. For all the proposed solutions in the available literature, the dataset is first preprocessed to transform it into the format suitable to be used by the ML algorithm. This stage typically involves encoding and normalization. Sometimes, the dataset requires cleaning in terms of removing entries with missing data and duplicate entries, which is also performed during this phase. The preprocessed data is then divided randomly into two portions, the training dataset, and the testing dataset. Typically, the training dataset comprises almost 80% of the original dataset size, and the remaining 20% forms the testing dataset. The ML algorithm is then trained using the training dataset in the training phase. The time taken by the algorithm in learning depends upon the size of the dataset and the complexity of the proposed model. The training time for the ML models requires more training time due to their deep and complex structure. Once the model is trained, it is tested using the testing dataset and evaluated based on the predictions it made. After that, the network traffic instance will be predicted to belong to either benign (normal) or attack class.

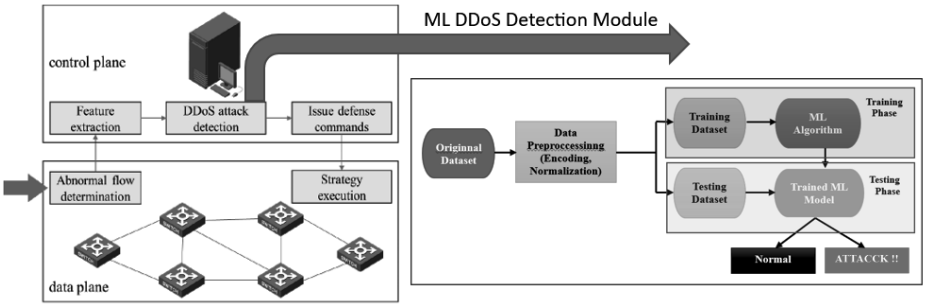


Figure 4. *Generalized SDN ML-based DDoS detection system*

Existing DDoS detection ML algorithms generally fall into three categories: supervised learning, unsupervised learning, and semi-supervised learning (Sudar K. et al., 2020). Supervised learning is a method in which training data are labeled. To construct the classifier, the computer "learns" from the labeled patterns and uses them to predict labels for new data. In unsupervised learning, the training data have not been labeled, and the computer "learns" by analyzing data features to create the classifier. In a semi-supervised approach, the input training dataset typically consists of both labeled and unlabeled data, usually a small amount of

labeled data and a large amount of unlabeled data. Each algorithm has its benefits and drawbacks, as well as its application domain. Among these algorithms, the accuracy of DDoS attack detection ranges from 95% to 99.9%. That means that no algorithm can guarantee 100% detection in all the available architectures and diverse situations. Therefore, if only one algorithm is used for all situations, the results may not be as reliable as the predictions based on the dataset that was used to train the model. Hence, the best performing algorithms have been identified and combined to get better results under varied circumstances. The set of optimal features which were selected by different feature selection methods is used as an input for different machine learning classifiers. Among the many available ML classifiers, Decision Tree, Naïve Bayes, Support Vector Machine (SVM), K-Nearest Neighbor (K-NN), Random Forest (RF), and Decision Tree (DT) are the most prominently used in DDoS detection systems (Ismail. et al., 2020).

There are two main ML-based approaches currently used to detect attacks on the SDN: simulation-based and public dataset-based approaches. In the first approach, researchers established SDN topology with legitimate hosts to generate normal traffics, and other hosts act as nodes to create DDoS attack traffics. They use public tools, such as Scapy, to simulate DDoS attacks. The network features, such as source/destination IP or port, entropy, flow packets, etc. are extracted from the collected traffic for normal and malicious data separately. All of these samples are random shuffling in a *.csv* file to create the row data which are used in the training model. The ML model can be used further to classify the normal and intruded DDoS packets inside the SDN network. This approach is fast and simple to analyze but with many restrictions. Firstly, the created dataset has a very small size and therefore, it is not enough to give accurate results, and these attacks are not realistic to represent the diversity of anomalies that are present in the current SDNs. Secondly, the number of extracted features is insignificant, and the small number of features is not enough to cover the behavior of all attacks (Ahuja N. et al., 2021). The selection of the proper public dataset has a significant impact on the evaluation of SDN IDS. Most of the publicly available datasets are not realistic, and they lack variety in the type of attack to cover all security trends found in the networks today. The most available datasets fail to give acceptable accuracy when deployed with intrusion systems. There are several datasets such as KDDCUP'99, CICIDS2017, ISCX2012, Kyoto, UMASS, ADFA, and DEFCON have been used for DDoS attack systems (Sahoo K. et al., 2020).

Table 2. *ML attack detection model performance metrics overview*

Accuracy $\frac{TP+TN}{TP+TN+FP+FN}$	Precision (PR) $\frac{TP}{TP+FP}$	Recall (TPR) $\frac{TP}{TP+FN}$	Specificity (TNR) $\frac{TN}{TN+FP}$
It is the ratio of correctly classified instances to the total number of instances	It is the ratio of correctly predicted attacks to all the instances predicted as attacks	It represents the ratio of all instances correctly classified as attacks to all the instances that are attacks	It represents the ratio of the number of correctly classified normal instances to all normal instances
True Positive (TP) - The number of correctly predicted attack instances			
True Negative (TN) - The number of correctly predicted normal instances			
False Positive (FP) - The number of incorrectly predicted attack instances			
False Negative (FN) - The number of incorrectly predicted normal instances			

The performance of the ML detection model is evaluated using the performance metrics like the accuracy, precision, recall, and specificity metrics and are computed as shown in Table 2. Recall (sensitivity, detection rate) is defined as true positive rate (TPR), i.e. the ratio of true positives and the sum of true positives and false negatives. The attack detection system with high recall has a low incidence of false negative alarms FNR (false negative rate), which means that a small number of attacks is incorrectly identified as normal network activities. The detection system with high TPR is used in critical areas of computer networks where the attack may not pass undetected. TNR (specificity) represents the ratio of true negatives and the sum of true negatives and false positives, and a detection system with high TNR has a low incidence of false positive alarms (FPR), which means that a small number of legitimate network activities are incorrectly identified as attacks. Although a compromise between TPR and TNR is usually made in practice, there are situations when it is necessary to use a system that will generate a small number of both false negatives and false positives. In these situations, a system with high detection accuracy is required.

To accurately distinguish entropy change caused by an anomaly, from the regular variation that is the result of stochastic traffic behavior, some approaches combine entropy and Artificial Intelligence (AI) techniques. AI is the development of intelligent machines representing a system that observes its environment and takes over activities that increase its chances of success using computer models. The advantages of applying AI are the ability to establish models that categorize the schemes used in detection, flexibility, and adaptability concerning precisely defining thresholds and rules, as well as the ability to learn. A group of authors in the paper (Vukovic I. et al., 2020) discusses the phases, components, categories,

and types of DDoS attacks and emphasizes detection solutions based on classification with information entropy and AI techniques. AI is used as an enhanced classification method, and the results in the paper (Kuk K. et al., 2017) highlight that the Monte Carlo approach presented via the BFTree classifier provides the best classification accuracy compared with other predictive models based on data mining classifiers. Furthermore, the authors in the paper (Cisar P., et al., 2022) represent an overview of the recently proposed artificial immune networks (AIN). The structures and learning algorithms of a few typical AINs are discussed.

HIGHLIGHTS OF EXPERIMENTAL WORKS

In this section, we highlight some experimental works related to the previously discussed entropy and ML-based DDoS detection mechanisms. Some works use statistical analysis, reporting on the complexity and operating costs of handling attacks. Other works have specific contexts to run the experiment, with particular configurations and constraints, and have designed the testing environment based on the specific parameters that correspond to their implemented approach. All experimental works are focused on the ML classification algorithms and consider the analysis of the entropy-based preprocessed network traffic data.

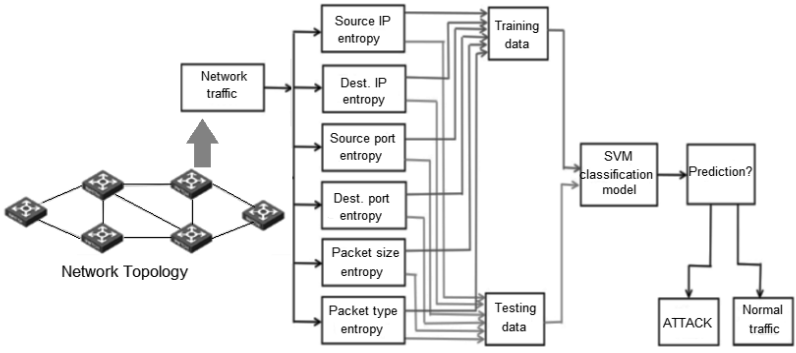


Figure 5. *An example of a hybrid Entropy-SVM attack detection system [10]*

Starting with the experimental work (Dong Li et al., 2018), the authors proposed a model to detect DDoS attacks in SDN that is a combination of both entropy of network features and a Support Vector Machine (SVM) supervised classification algorithm. The model extracts several key features from the packet-in messages and measures the distribution of each feature by using entropy, then uses a trained SVM algorithm to detect the DDoS attack. SVM attempts to solve an optimization

problem that consists of finding decisions boundary in the feature space that separates data from different classes. In this solution, the entropy of network features is calculated first. The five packet features (srcIP, srcPort, destIP, destPort, packIn) are all random variables, so we firstly extracted and then calculated their entropy in a one-time window according to equation (2). During the time of the attack, entropy values are derived from its normal behavior, and used for detecting the anomaly in the traffic.

The SVM algorithm is composed of two steps, the first one is the features extraction, and the second step is the classification. Step 1 (initialization) represents that the features are extracted from all the training packets set and the entropy will be used to measure the distribution of each feature. Then, the calculated feature entropy will be used to train nonlinear one-class SVM. Step 2 (DDoS attack detection) represents that for each new test packet, authors extract features and calculate the entropy which will be given to the trained SVM model to decide if it is normal or abnormal. If the result is abnormal, it means that a DDoS attack happens.

To evaluate the performance of the proposed solution, the authors used Mininet emulation software to build the SDN network topology. The controllers are Floodlight and the Virtual-Machine server that has 64GB RAM and 32 core CPU. The experimental network adopts a three-layer structure: core, convergence, and access layer. Two controllers belong to the core layer, four switches belong to the convergence layer, and another four belong to the access layer. There are 50 hosts in the experimental topology. For simulating a real network environment, normal traffic should be triggered as background traffic, and it is produced by the traffic generator D-ITG periodically and the traffic ratio is TCP:UDP:ICMP = 85:10:5. The packet sending speed is about 1000 packets/s.

In the training step, the normal traffic is generated by the hosts in the network. The software Hping3 is used to simulate DDoS attacks with the spoofed source and destination IP address with an attack duration of 30 seconds. Once the time window is determined, the entropy is calculated to be a 6-dimensional vector. These vectors are the sample of the SVM model. The sample is divided into two groups, one triggered by normal, and the other triggered by DDoS attack traffic. DARPA1999 public data set is also used to train the SVM model. In the training step, the parameters of SVM are set to be fixed and used to analyze the real testing data.

Once the model is trained, the next step is to identify the type of attack and attacked hosts in the testing phase. An ML model is accurate if it correctly predicts the attack type during the attack. Further, the performance of the detection model is measured using the following metrics: PR (Precision), TPR (Recall), and F-score (detection time). Besides, the authors have used other ML algorithms, such as Decision Tree, Naïve Bayes, KNN, and Random Forrest, to analyze the traffic and detect DDoS attacks. The proposed detection solution outperforms all

other ML algorithms with higher accuracy and shorter detection time. Experimental results show that this solution gives 97.25% correctly classified instances and 2.75% misclassified instances, and the expected effect was achieved. The low false alarm rate is a good result and, on the other hand, it may be the proposed simulation of normal data flow if it is not comprehensive enough, which is what needs to be done in the future.

In the research paper (Yu S., et al., 2021) the authors proposed a cooperative DDoS attack detection framework based on entropy and an ensemble learning approach in SDN network environment, as shown in Fig. 6. The authors tried to solve how to reduce the burden of the controller and the SBI interface, as well as how to improve the attack detection speed while ensuring DDoS attack detection accuracy. Considering the programmable ability of the OpenFlow switch, data statistics and analysis are arranged on the edge switch, which can implement a part of the attack detection function to reduce the burden on the controller and improve the response speed of attack detection.

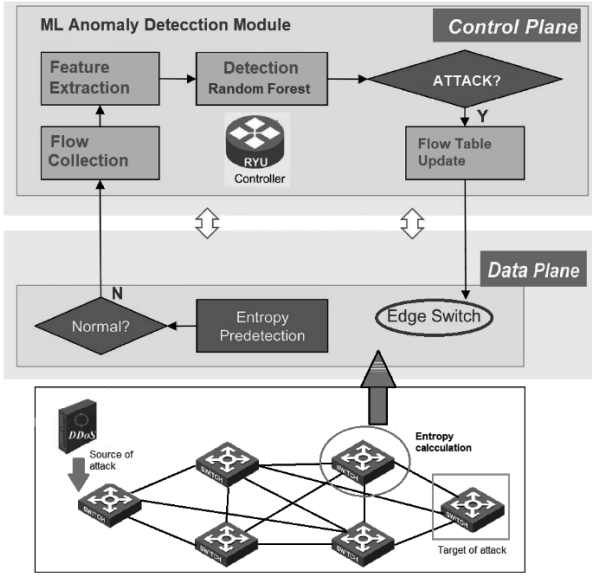


Figure 6. *An example of a cooperative Entropy-RF detection system [26]*

During the experiment, Scapy software was used to inject normal traffic into the network as the background traffic, and then a TCP-SYN and ICMP flood attack were launched from the first switch (source of attack) to the last host (target of attack). The corresponding fast anomaly detection algorithm based on information entropy of the destination IP in the edge switch has been based on information entropy $H_n(X)$ (normal state) and $H_a(X)$ (attack state) values. Under normal cir-

cumstances, the information entropy value will fluctuate up and down in a small range. When a DDoS attack occurs, $H_n(X)$ and $H_a(X)$ satisfies the $H_n(X) - H_a(X) > \delta$ expression, the value of δ is determined according to the statistical information entropy under normal network state.

Considering the multiple feature tuple and requirement of less overhead in the detection process, the authors proposed the random forest algorithm (RF) to further detect the suspicious flow. Based on the consideration of ensuring detection accuracy while minimizing system overhead, the authors selected five most typical features to construct a 5-feature tuple (average number of packets, average number of packet bits, growth rate of port, growth rate of flow, and growth rate of source IP) for subsequent machine learning training and testing. Compared with other ML algorithms, RF random algorithm is a very convenient and practical algorithm which is more suitable for multivariate classification with less resource consumption and fast training speed. In the RF modeling process, the bagging sampling method was exploited to randomly select multiple training subsets from the original training set, while the CART algorithm was leveraged to generate K-decision trees to form the RF according to the principle of minimum impurity. The final anomaly decision was determined by voting the results of K-trees in the test set. Therefore, the test accuracy of the trained classification model on the test set is 0.997, indicating that this classification model has a very high accuracy for the detection of DDoS attack traffic.

CONCLUSION

Although SDN has many advantages, it also faces the threat of DDoS attacks, the most common security threat in contemporary networks. In response to this problem, we analyze the detection mechanisms of DDoS attacks over SDN, which combines information entropy and ML classification algorithms. The main issue of the entropy-based approach is the fine-grained traffic analysis, and accuracy of traffic variation detection. We have extended the entropy-based attack detection approach with the ML anomaly classification method to ensure that the attack traffic can be identified quickly and effectively. Different ML classification models are applied to the created dataset for classifying the traffic while performance evaluation is done with the help of performance indicators. For the effective validation of the ML classifiers, Random Forest and SVM are used with different topology scenarios. The efficiency of the anomaly classification method is validated through the presented experimental results. Our contribution addresses a practical implementation of the proposed method, using defined comprehensive architecture for flow-based anomaly detection that is based on the combined application of the entropy-based and ML techniques.

Finally, we believe that our work contributes to a better understanding of the DDoS attacks detection in SDN networks, despite the limited number of papers in this research field. Our further work will be oriented to the full implementation of the proposed architecture in a multi-controller and more complex SDN networks, focusing on better predicting the degree of certainty of detected network traffic anomalies.

REFERENCES

Ahuja, N., Singal, G. et al., (2021) Automated DDOS Attack Detection in Software Defined Networking, In Journal of Network and Computer Applications, Vol. 187, 2021, 103-108, https://doi.org/10.1016/j.jnca.2021.103108.

Basicevic, I., Blazic, N., Ocovaj, S. (2021) On the Use of Principal Component Analysis in the Entropy Based Detection of Denial-of-Service Attacks, Security and Privacy, Wiley, Vol. 4, Issue 1, doi: 10.1002/spy2.

Berde, P., Gerola, M., Hart, J. et al., (2014) ONOS: Towards an Open, Distributed SDN OS, In HotSDN: Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, ACM 2014, pp. 1–6. https://doi.org/10.1145/2620728.2620744

Bonguet, A., Bellaiche, M. (2017) A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing, In Future Internet, 9(3):43. https://doi.org/10.3390/fi9030043

Cabarkapa, D., Rancic, D. (2021) Performance Analysis of Ryu-POX Controller in Different Tree-Based SDN Topologies, Advances in Electrical and Computer Engineering, vol. 21, no. 3, 31-38, doi:10.4316/AECE.2021.03004

Cabarkapa, D., Rancic, D., Pavlovic, P., Milicevic, M. (2022) Investigating the Impact of Tree-Based Network Topology on the SDN Controller Performance, Facta Universitatis, Series: Automatic Control and Robotics, Vol. 21, No 1, 25-35, doi: 10.22190/FUACR211223003C

Cisar, P., Erlenvajn, D., Maravic-Cisar, S. (2018) Implementation of Software-Defined Networks Using Open-Source Environment, In Technical gazette, Vol. 25, Suppl. 1, pp. 222-230, http://dx.doi.org/10.17559/TV-20160928094756

Cisar, P., Maravic Cisar, S., Popovic, B., Kuk, K., Vukovic I. (2022) Application of Artificial Immune Networks in Continuous Function Optimization, Acta Polytechnica Hungarica, 2022, accepted for publication

Ding, D., Savi, M., Pederzolli F., Campanella, M., Siracusa, D. (2021) In-Network Volumetric DDoS Victim Identification Using Programmable Commodity Switches, In IEEE Transactions on Network and Service Management, vol. 18, no. 2, 1191-1202, doi: 10.1109/TNSM.2021.3073597.

Dong, Li, Chang Yu et al. (2018) Using SVM to Detect DDoS Attack in SDN, In IOP Conf. Series: Materials Science and Engineering 466 (2018) doi:10.1088/1757-899X/466/1/012003

Dong, S., Abbas, K., Jain, R. (2019) A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments, In: IEEE Access, vol. 7, pp. 80813-80828, doi: 10.1109/ACCESS.2019.2922196.

Dudeja, R. K., Bali, R. S., Aujla, G. S. (2022) Internet of Everything: Background and Challenges, In: *Software Defined Internet of Everything*, 3-15, Springer, doi: 10.1007/978-3-030-89328-6_1

Gupta, B. B., Joshi, R. C., Misra, M. (2009) Defending against Distributed Denial of Service Attacks: Issues and Challenges, Information Security Journal: A Global Perspective, 18:5, 224-247, doi: 10.1080/19393550903317070

Ibrahim, J., Gajin, S. (2022) Entropy-based Network Traffic Anomaly Classification Method Resilient to Deception, Computer Science and Information Systems, Vol. 19, Issue 1, 87-116, doi:10.2298/CSIS201229045I

Ismail et al., (2022) A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks, In IEEE Access, vol. 10, pp. 21443-21454, doi: 10.1109/ACCESS.2022.3152577.

Jimenez, M. B., Fernandez, D., Rivadeneira, J. E. et al., (2021) A Survey of the Main Security Issues and Solutions for the SDN Architecture, In IEEE Access, vol. 9, pp. 122016-122038, doi: 10.1109/ACCESS.2021.3109564.

Kuk, K., Milentijevic, I., Randjelovic, D., Popovic B., Cisar P. (2017) The Design of the Personal Enemy - MIMLeBot as an Intelligent Agent in a Game-Based Learning Environment, Acta Polytechnica Hungarica, 14(4): 121-139, 2017, ISSN 1785-8860

Open Networking Foundation: OpenFlow Switch Specification, Version 1.5.1, (2015), https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf

POX Github Documentation, https://noxrepo.github.io/pox-doc/html/ (Last accessed on June 2022)

Sahoo, K. S. et al., (2020) An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks, In IEEE Access, vol. 8, pp. 132502-132513, 2020, doi: 10.1109/ACCESS.2020.3009733.

Shalimov, A., Zuikov, D., Zimarina, D. et al., (2013) Advanced study of SDN/OpenFlow controllers, CEE-SECR '13: Proceedings of the 9th Central & Eastern European Software Engineering Conference, no. 1, 1-6, https://doi.org/10.1145/2556610.2556621

Sherwood, R. et al., (2009) FlowVisor: A Network Virtualization Layer, Deutsche Telekom Inc., R&DLab, Stanford University, Nicira Networks, Tech. Rep. OPENFLOW-TR-2009-1.

Sudar, K., M., Deepalakshmi P. (2020) Comparative Study on IDS Using Machine Learning Approaches for Software Defined Networks, International Journal of Intelligent Enterprise, Vol. 7, no.1-3, pp. 15-27, doi: 10.1504/IJIE.2020.104642

Villota, W., Gironza, M., Ordoñez, A., Caicedo, R. O. M. (2018) On the Feasibility of Using Hierarchical Task Networks and Network Functions Virtualization for Managing Software-Defined Networks, In IEEE Access, vol. 6, 38026-38040, doi: 10.1109/ACCESS.2018.2852649.

Vukovic, I., Popovic, B., Cisar, P. (2020) Application of Artificial Intelligence in Detection of DDoS attacks, Thematic conference proceedings of international significance, International scientific conference 'Archibald Reiss Days', Belgrade, University of Criminal Investigation and Police Studies, Belgrade, 10(2): 557-566.

Yu, S., Zhang, J., Liu, J. et al. (2021) A Cooperative DDoS Attack Detection Scheme Based on Entropy and Ensemble Learning in SDN, EURASIP Journal on Wireless Communications and Networking, 90, 2021, https://doi.org/10.1186/s13638-021-01957-9

Zargar, S. T., Joshi, J., Tipper, D. (2013) A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, In IEEE Communications Surveys & Tutorials, vol. 15, no. 4, 2046-2069, doi: 10.1109/SURV.2013.031413.00127.

Zhou, L., Zhu, Y., Xiang, Y. (2022). A novel feature-based framework enabling multi-type DDoS attacks detection, In Special Issue on Decision Making in Heterogeneous Network Data Scenarios and Applications, Springer, https://doi.org/10.1007/s11280-022-01040-3

Zhou, W., Li, L., Luo M., Chou, W. (2014) REST API Design Patterns for SDN Northbound API, 28th International Conference on Advanced Information Networking and Applications Workshops, 358-365, doi: 10.1109/WAINA.2014.153.

MANAGEMENT IN THE PREVENTION OF MALPRACTICE IN ELECTRONIC REFEREEING SYSTEMS IN SPORTS

Bobana Berjan Bačvarević, PhD
Alfa BK University, Belgrade, Serbia

Dejan Rančić, PhD
Faculty of Electronic Engineering, University of Niš, Serbia

Vladan Borović, PhD[1]
Ministry of Interior, Belgrade, Serbia

PURPOSE

In the twenty-first century, the popularity of sports is growing day by day attracting an increasing number of people curiously watching their favorite players in all disciplines on all continents. With the increased share of sports on the global economic market, there is a growing interest in improving the game both in skills and in introducing new technologies. It is the new technologies that bring a novel long-awaited wave of attractiveness and opportunities for marketing and business.

The main feature of the existing systems is the extremely high financial cost of use, as well as the veil of secrecy with which the used technology is covered. Therefore, most sport events could not be covered by these systems for many years. The chance of potential new systems increases with possible multipurpose use. In the world of modern sports, where the stakes increase with each passing minute and where one wrong referee decision for the ball means a change in "sports luck", we rely on the modern technology ensuring that judges' decisions are impartial.

The component of human error in making important decisions is often decisive. There is a great need to implement technology that would reduce the chances of human errors in such important decisions. Furthermore, technological systems

1 vladan.borovic@mup.gov.rs

provide the analysis and improvement of the game. Systems based on such technology are used to collect a variety of data and use it for a number of purposes not restricted just to the sport area. Today, the most common applications of such systems are in tennis (Official Hawk-Eye Challenge System), football (*VAR*) and cricket, then for police and military purposes (Borović et al., 2018), as well as in the production, industrial branches of society such as the automotive industry. Apart from that, sport bet facilities certainly have impact on decisions of such electronic computer systems.

The aim of the authors of this paper was to discover potential malpractice in the use of these electronic systems and mark the points of potential malpractice, and also propose a new malpractice-prevention model on lowering the damage done by tampering the results.

EXISTING SYSTEMS OVERVIEW

The system that has attracted most attention so far and gained most popularity is the famous Hawk-Eye system, represented in almost every country in the world. At the same time, it is the adopted name of the first technology used to detect the position of objects in space, primarily in sports. It is a complex computer system that is officially used in making referee decisions in sports, such as: tennis, football, cricket, Gaelic football, bocce and basketball. This system graphically simulates the visual tracking of the path of a moving ball and shows the calculated record of the statistically most probable path in the form of a moving image, i.e. computer *3D* animation.

The Hawk-Eye system was developed in Great Britain by Dr. Paul Hawkins at the beginning of the 21st century, in 2001. At the beginning of 1999, he began research at the British company Roke Manor Research Ltd, founded in 1956, which already had more than 30 years of professional experience in the fields of image processing. The project was led by Dr. Paul Hawkins and funded by the Television Corporation, (Roke Manor Research Limited, 2019). The current owner of the Hawk-Eye system is Hawk-Eye Innovations Ltd. from the UK which has been part of the Japanese corporation Sony since March 2011. (BBC News, 2011)

The theoretical basis of the Hawk-Eye system is the principle of triangulation using visual images and weather data collected from a large number of high-speed video cameras that are placed at different predetermined places and angles around the observed terrain. Therefore, if we talk about tennis, there are ten cameras installed. The system quickly processes signals from video cameras. A predefined model of the control area with precise dimensions is given in the system before

the start of signal collection, and includes important data on the basic rules of the observed game. Precisely, on each individual image from the video camera, the system identifies a group of pixels that correspond to the image and appearance of the ball. Then, using modern computer equipment, primarily high-speed personal computers, the *3D* position of the ball on each individual image is calculated while simultaneously comparing images in two physically separated video cameras at the same time. Thus, it is possible to make an accurate record of the exact path of the ball in space in a large series of images and mathematical calculations. It is also important to note that the system can predict the future trajectory of the ball using mathematical approximations and statistical calculations. In the end, based on the data recorded in the databases of the predefined game area and the video camera system, the exact place where the ball touches the observed terrain is calculated at the height of 0. This is also the final expert goal of all calculations. By simulating, system generates the *3D* animation - Automated Referee Decision, as seen in Figure 1.

Figure 1. *Hawk-Eye computer system, operator and 2 of 10 computers*

ORIGINAL OBJECT TRACKING SYSTEM

During 2010, a completely new advanced tracking system for moving objects in sports was designed by the authors of this research paper. (Borović, 2019)

The advanced tracking system has the following functional parts, independent subsystems, each of which has certain roles:

- Signal collection subsystem (video-cameras, computers and computer network)
- Subsystem for advanced detection of objects and positions in three-dimensional space
- System for *3D* simulation, animation and graphical display of calculation results

In the following years, 2015 and 2019, a number of professional experiments, thorough tests and comparative analysis have been done through these sequential phases:

- Simulation of the whole system
- Home system testing
- Testing the system in real conditions
- Preparation of documentation for official testing to gain the tennis federation certificate

The basis of the system are video cameras with appropriate technical characteristics placed in precisely defined and predefined places together with software applications for object detection and tracking of the ball. Up to six video cameras placed around the surveillance area were used at the locations where the experiments and tests were performed. As seen in the following figure, in Figure 2, we have 10 video cameras set up around the monitored play area together with separate units:

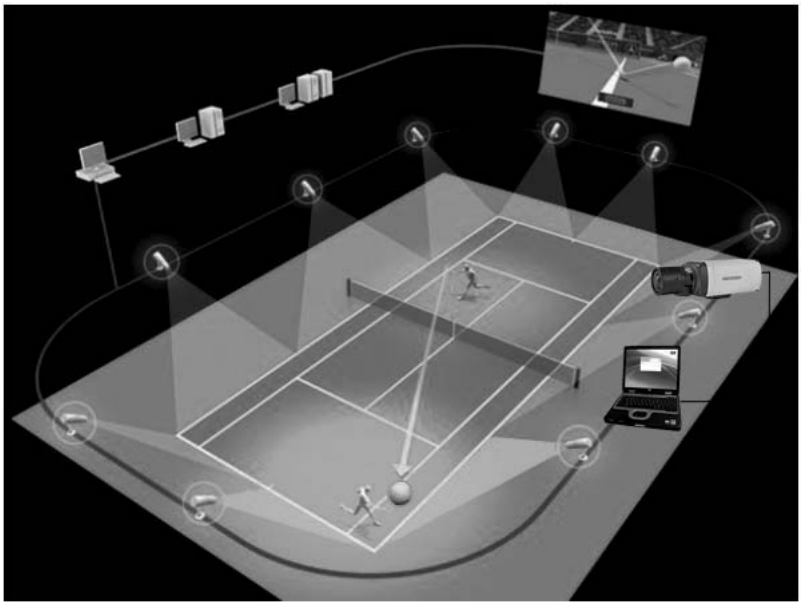


Figure 2. *Video-cameras set around the game area*

The first subsystem, an independent unit, is a mandatory system of video cameras and technical equipment that monitors and records a sports match or training. It is possible to record other areas with different tasks. At the same time, this system collects signals in real time on a certain larger number of computers according to the following model:

1 camera = 1 associated computer.

The second part consists of a subsystem that determines the position based on the image from the camera (on-line) or on the image from the recorded video (off-line) and simulates the trajectory of the observed object in space, e.g. a ball in sports. The system consists of software developed in the Microsoft programming environment with program code written in *MS Visual Studio C* ++ and *C* # 98, 2010, 2013 programming languages and uses the *AForge.NET* framework for ball detection and tracking, with the addition of the original author's algorithm. Testing and practical implementation was done for the system of detection and monitoring of objects based on the recorded video. By the way, the basis of this system for the detection and monitoring of moving objects in space are new, up-to-date improved publicly available mathematical algorithms with the application of mathematical principles. The original, designed system is shown in Figures 3 and 4 (Borović et al., 2019).

The third independent functional part consists of a system that, based on the calculation of the path of the object in space, performs a graphic simulation of *3D* animation in an attractive and visually appealing way. Software application for accurate, photorealistic *3D* visual animation was developed in *MS Visual C* ++ programming language using *OpenGL* graphics library.

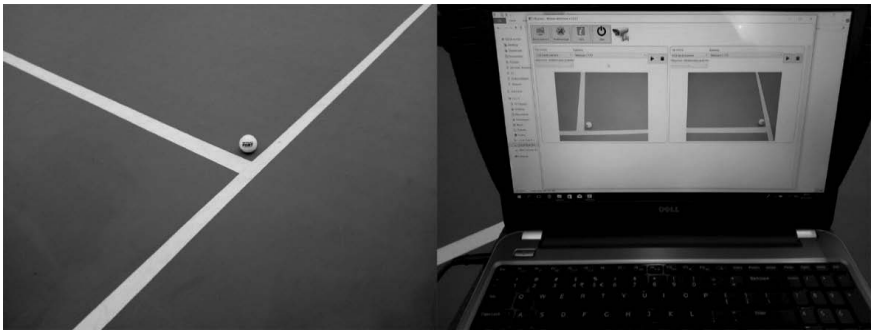


Figure 3. *Ball view, camera test and the original application*

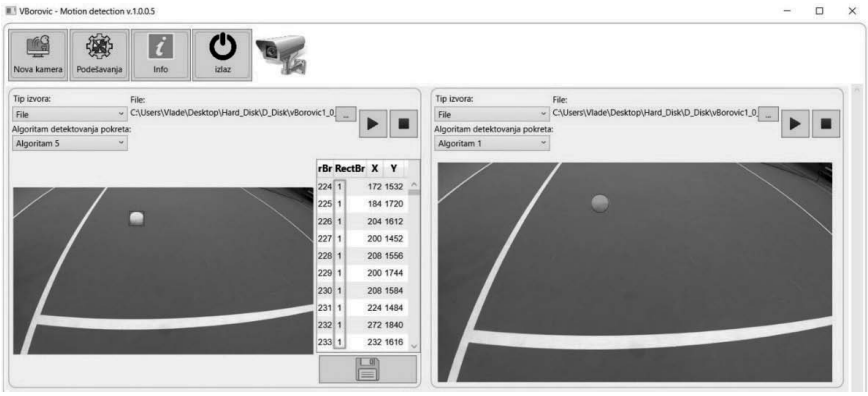


Figure 4. *Ball detection in the tracking system*

DESIGN/METHODS/APPROACH

If a simple question is asked: *Are existing systems infallible?* The answer to this question is precise: *No!*

There are three dimensions to this issue:

- Technical
- Psychological
- Intentional

Based on numerous publicly published articles, expert debates, dedicated studies and statements of numerous actors, primarily in the world of tennis, football and cricket, the authors of this paper can say with certainty that all existing systems in the world have a certain margin of error and potential making the wrong electronic referee's decision accompanied with malpractice (Phys. Science X, 2008). As the authors above all know the process of functioning of this technology down to the smallest details, technical approach and procedures for detecting and tracking moving objects in space, it is clear that potentially and often detection errors occur, first of all positions of objects and graphical simulations of the path of their movement.

Perhaps these claims are best demonstrated by the public, written comment of one forum participant on one of the official websites of the manufacturer and owner of the Hawk-Eye system (pscaife3, 2016): "But none of Hawk-Eye's iterations show such a level of ground contact. Is this a design feature or the system is not able to show the actual level of contact with the terrain? Ten centimeters is a considerable distance and will vary depending on the type of tennis kick and the type of playing surface. The definition in Wikipedia also states projected (and predicted), but incorrect levels of contact." The comment was given on an accurate video recording

of the functioning and explanation of the functioning of the mentioned system for position detection and tracking of moving objects which are frequent situations in the difficult detection of the exact contact and position of the observed object with the ground by the method of projection and prediction, and not entirely on the basis of images from video.

As clearly stated in an article from 2013 in a renowned magazine (Hawk-Eye at Wimbledon, 2013), the mentioned system is not infallible as spectators of sports events think. The question is how accurate the Hawk-Eye system really is. Back in 2008, a scientific paper entitled "Public Understanding of Science" (Collins & Evans, 2008) was published stating that the way in which the system presents its calculations and analyses in sports can easily lead people to mistakenly conclude that graphic, animated representations of results are a real picture of what actually happened. That system is an excellent opportunity to discuss uncertainty, reliability intervals of the detection process and mathematical-statistical visual delight.

It is also noted that public understanding of science, although approaching expertise only on rare occasions, can be improved in terms of science and technology processes. As the public understands and accepts measurement errors, the confidence interval can also be improved if electronic systems for referee decisions present the results of their calculations differently.

Psychologically, there is a great chance and danger that this system, in the way it is used, inadvertently leads technically insufficiently informed viewers to overestimate the ability of technical devices to resolve misunderstandings among people because measurement errors are not publicly highlighted. Thus, for example, virtual *3D* simulations and photorealistic animations can as reconstructions of events be easily used to show "what really happened".

In the mentioned scientific paper (Collins & Evans, 2008), several real documented examples of controversial situations of using this system and the results of calculations with potential errors in international tennis tournaments are given. It has been mentioned several times that the way in which the results of this system are used and presented today can lead the public to the wrong conclusion about the degree of reliability of scientific measurements – it has been noticed for a long time, since the beginning of its application in sports. The authors of the mentioned paper believe that the lack of understanding of the possibilities and reliability of this system could be reduced by including information on the potential error of measurement and calculation that are presented graphically.

People and technical devices make two types of mistakes:

- Systematic errors
- Random errors.

The first are mistakes that are repeated and have a similar effect every time. The causes of such errors can often be technically understood and their negative impact on calculations can be predicted and compensated.

Other types of errors cannot be predicted except that their typical magnitude can be estimated mathematically using probability and statistics, the shape of the random distribution. They cannot be compensated, but can be taken into account when assigning confidence levels to the measurement and detection process.

Therefore, it is proposed to introduce the principle of automatic decision-making, which determines how computers, software and electronic decision-making systems should be used in sports with the obligatory mentioned types of errors. In the mentioned mathematical discipline, probability and statistics, error dispersion is usually present as a standard deviation, exception. Following these principles, it can be assumed that in 5% of the predictions of the trajectory and results of the Hawk-Eye system, which is 1 in 20, the error in the calculation could be greater than 9 millimetres, while in 1% the error may be even greater than 11.7 millimetres.

A series of publicly available articles on the Internet have raised a number of doubts and controversies about the accuracy and reliability of the Hawk-Eye system, with numerous errors in measurement, detection and *3D* graphical display of calculation results. Some estimates say that the system is accurate in only 60% of cases measured and used in tennis (Thomas, 2019) (Pugh, 2019) (Braun, 2012).

Even the company Hawk-Eye in its technical paper (Hawk-Eye Innovations, 2016) explains and specifies the following details with reference to errors in detecting the position of objects in space: "As shown in 2005 during ITF testing, Hawk-Eye was the first system to pass a series of rigorous tests and conditions, which means it was the first electronic system to be officially accredited. Practical results showed that the system had an average error of 3.6 mm compared to the high-speed camera located on the playing surface."

It is further claimed that, with the advancement of technology and software and their application, together with a decade of experience at major sporting events, their electronic refereeing technology has an average error of 2.6 mm.

The factors most affecting the errors in measurements and calculations in the conditions when the terrain is outside are also listed (i.e. sun, shadows, wind).

The paper (Collins & Evans, 2008) also suggests that more information should be published on the uncertain reliability and accuracy of measurements and calculations, primarily for television audiences and viewers, in order to more honestly show variations in the possible correct trajectories of the ball. They suggest, for example, that the predicted location of the ball contact with the court and the con-

fidence intervals surrounding it be shown, both the location and the electronic referee's decision (if 95% it means there is only a 5% chance of error, i.e. the ball indeed fell outside this larger area of prediction).

In conclusion, the authors of this paper, without a subjective view, due to the potentially high probability of errors in tracking moving objects in existing systems in the world, can realistically agree with the need to show calculated graphical results and predicted paths together with the level of reliability, certainty and possible errors as seen in Figure 5. That would be quite fair to the public.

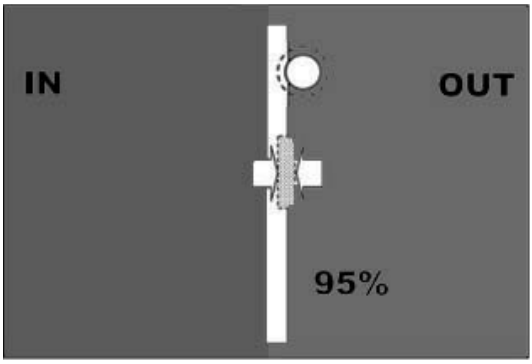


Figure 5. *Indicated level of trust in e-referee system*

This would not only more accurately reflect the limitations of this technology but could potentially teach complex mathematical concepts and principles of statistics and probability to a large number of people. Hawk-Eye could still provide a "good ball" or "out" response to a request from the in-game referees, but the likelihood is correct, the right answer would also be clear to everyone, especially TV viewers and viewers around the field as they watch live match, which also form public opinion.

As for the testing of the original system in real conditions, first of all it included the preparation of the tracking system, then the demanding installation of all parts of the system in the agreed areas, courts for playing tennis. Basic, prearranged tests were performed. After a lot of negotiations, two physical locations in Belgrade were agreed upon for testing the system in real conditions. These are the following two sports fields:

- Professional tennis courts in Jajinci, Đoković tennis school, and
- Gemaks tennis courts in Belgrade, Challenger tennis tournament.

Specific practical testing was performed on video-recordings from web cameras with a resolution of 1 megapixel and a speed of 30 frames per second (*fps*), using authors' original system.

In one experiment, X and Y positions (in pixels) were calculated, the ball movement detection and contact with the field line were detected on the video camera images in the plane of that line. In a certain frame, the ball made contact with the field, which was documented in the image from the video camera. It shows the importance of the correct selection of the ball movement detection algorithm suitable for real game conditions.

Based on the obtained results, it can be concluded that:

- A new algorithm for the ball detection gives better results in tracking moving objects in tennis and
- Potential error in electronic decisions of the older version of the algorithms is significantly higher than in the new one.

The possibility of malpractice and errors in position calculations is high if the appropriate technical detection algorithm is not selected/used.

FINDINGS

In the following section, we give two examples where potential malpractice has been done, or could easily be done, stating parts of the system very vulnerable to malpractice actions and tampering the results.

Figure 6. *Example 1: Incorrect 3D animation and graphics*

As shown in Figure 6, an evident, probably intentional *3D* graphical error leads to a wrong electronic referee decision. It happened in Australia Open tennis tournament 2011. The calculation of the trajectory of object in space in the older

Hawk-Eye system from 2011 was tampered. The vague and potentially incorrect trajectory of the ball in the surveillance area is clearly visible. The inaccurate *3D* shadow that is rendered in real time and the so-called flickering within the net as well as low-resolution and quality textures, poor texture mapping in *OpenGL* and especially insufficiently clear border areas, a line on the tennis court in the space monitored by this system. Simply, the shadow does not follow the exact ball trajectory in *3D* space. The detected position and graphically presented ball are not correct. Thus, in almost every use of the system in making electronic refereeing, it was additionally possible to make a mistake in the decisions.

Insufficient precision of the field lines, graphic areas that are on the border, lead to possible minimal mistakes when presenting the referee decisions. By the way, the lines that mark the area of the game in all sports are the most important areas that are monitored in space by these systems. Simulation of calculation results through visual *3D* graphic presentation potentially shows the public and the professional public incorrect results of referee decision-making because errors in the detection of position and movement of objects in space are possible, although all mathematical calculations are correct. In other words, a graphical simulation misrepresents accurate results. A ball in sports, for example, that was not in the out, i.e. it was not out of line in the observed predefined area at the time of contact with the terrain, as described in the Hawk-Eye system, *3D* animation reproduces graphically incorrect result, as if it was out, i.e. outside the observed line in the field.

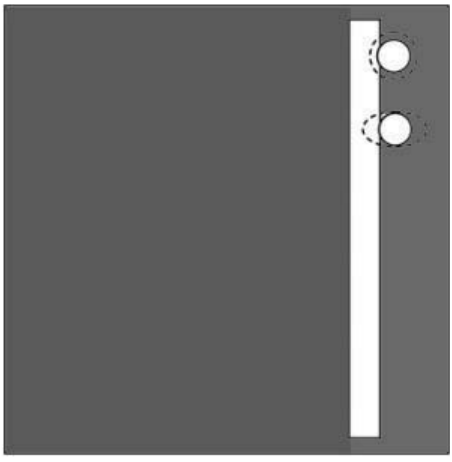


Figure 7. *Example 2: Measurement and detection error*

It is clear in Figure 7 that the uncertainty of detection is shown by dashed lines so that the potential contact of the ball with the ground, i.e. tennis terrain can be anywhere within a dashed-line circle. The upper, slower ball falls on the field of almost

90°. Trace detection can be with a big error in the case of the second lower ball in the picture due to fast movement and error in the direction of movement. The error can then be within a dashed ellipse, of arbitrary, highly dependent shape. Furthermore, the question is what the error limit in case of fast movement of the ball is.

Therefore, the database with the detected ball *3D* coordinates could be easily tampered and the results misused.

The scientific paper (Collins & Evans, 2008) stated that in direct contacts with the experts of the Hawk-Eye team and the *ITF* (International Tennis Federation) rather vague and incomplete tolerated error limits and percentage calculations of the possibility of measurement and calculation errors were obtained.

ORIGINALITY/VALUE

Numerous professional tests and research in modern sports are conducted every day (Bacvarevic Berjan et al., 2012) (Bozic, Pazin, Bacvarevic Berjan, 2019). Large number of collected data can be used to improve the game play, especially in tennis (Petkovic, Jonker, Zivkovic, 2001), and it is also subject to tampering, ending in false conclusions. Technical systems collect the information that can easily be changed intentionally or by a system error.

There are two vulnerable parts of the electronic tennis challenge system identified by the authors of this paper that can be used for intentional malpractice:

- *3D* animation, graphical display of a ball trajectory
- Database with calculated positions info (object x, y, z coordinates)

In the first case, the system operator, could easily change the graphical display of the calculated positions of the ball, therefore change the real trajectory to non-existent virtual path, causing the wrongful e-referee decision (in / out). This can be done in the *OpenGL* code.

The second part involves tampering with database, again by the system operator, changing the correct mathematically calculated positions. It also causes the wrongful e-referee decision. Both malpractice actions can be done unnoticeably.

If we speak about the management in the prevention of malpractice, the authors propose a management algorithm, a prevention model as shown in the following Figure 8, which can be applied to the electronic referee process.

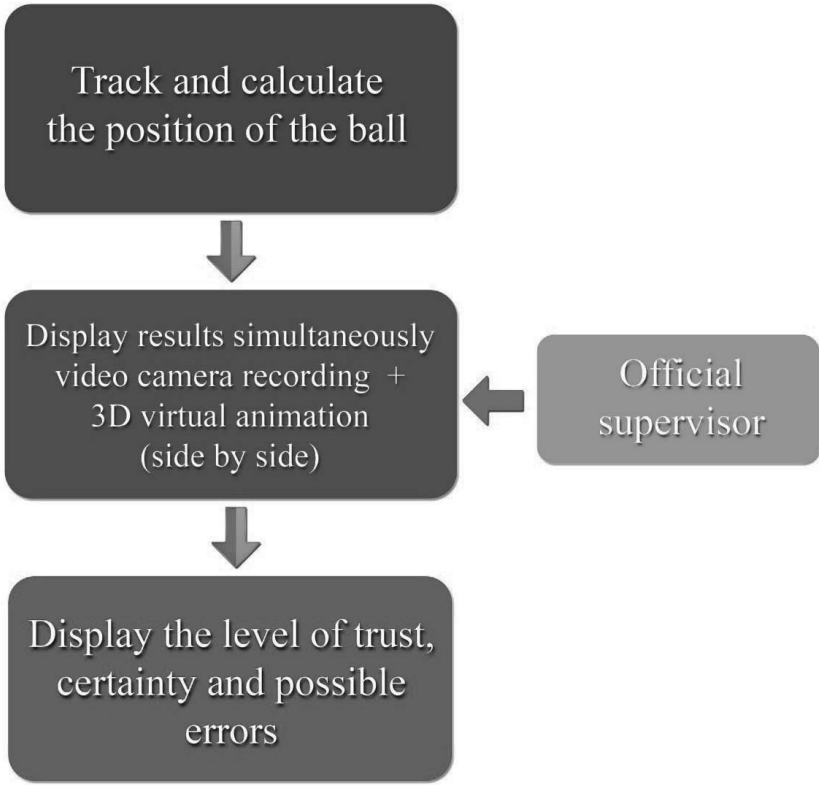


Figure 8. A malpractice-prevention management model

Following these steps, we can assure higher trust in the system results, public objectivity feeling and lower the possibility of intentional malpractice:

- Track the ball in space, detect, measure and mathematically calculate all positions, in the video-camera images, predict the flight path and contact with ground. All data are stored in the system database.
- Official supervisor restricts database access and monitors the use of *3D* virtual graphics system with animation showing the ball trajectory. In the same time, both *3D* animation and a video recording from the independent high-speed *UHD* video-cameras are shown to the spectators, TV audience and public. It shows the electronic system flight trajectory and ground contact.
- When the e-referee decision is shown, it must be accompanied with the adequate level of trust, certainty and possible error margin numbers and in each and every challenge call and use of the system.

By using the proposed model, we lower the possibility for intentional malpractice, especially with data tampering in the database ball positions with predictions and misusing the *3D* animation results display.

CONCLUSION AND RECOMMENDATION

Modern technology electronic refereeing systems are used in almost every sport all over the world. The possibility of malpractice is very high. Errors are made by the technology or by a human, sometimes intentionally.

The authors described in this paper the used technology in every step, made the systems overview, additionally describing an original new system. The weak spots of systems are given, public doubts on the objectivity of electronic decisions with stated possible malpractice areas, actions, examples and places in the technology that can easily be used to tamper the results, so the end decision might be wrong.

We proposed a new management model for malpractice-prevention and gave strong recommendations for a tamper-proof, a safer and more objective use of electronic refereeing systems in sports.

The overall authors' recommendation is - when the decision is shown, adding a real-time video-camera recording also include adequate level of trust, certainty and possible error margin numbers in public display.

It would be quite fair to the public.

REFERENCES

Bacvarevic Berjan, B. Pazin, N. Bozic, P. Mirkov, D. Kukolj, M. Jaric, S. (2012) Evaluation of a Composite Test of Kicking Performance,

Journal of Strength and Conditioning Research, 26(7), DOI: 10.1519/JSC.0b013e318237e79d 1945-1952.

BBC News (2011, March 7) Hawk-Eye ball-tracking firm bought by Sony, Accessed on July 7, 2022. https://www.bbc.com/news/business-12670063

Borović, V. (2021). *Advanced tracking system for moving objects in sports*. Doctoral dissertation. University of Niš: Faculty of Electronic Engineering

Borović, V. Spalević, P. Čisar, P. Rančić, D. Jović, S. (2019) Supervisory system for physical objects spatial location detection, *Physics A: Statistical Mechanics and its Applications, Elsevier,* 521, DOI: 10.1016/j.physa.2019.01.023. 781-795.

Borović, V. Spalević, P. Jović, S. Jerković, D. Drasute, D. Rančić, D. (2018) Hail suppression activities using TETRA-based sensor network, *Sensor Review, Emerald Publishing Limited*, 39(2), DOI: 10.1108/SR-02-2018-0029, 171-177.

Bozic, P. Pazin, N. Bacvarevic Berjan, B. (2019) Evaluation of the torque-angular velocity relationship across various joint positions,

The Journal of Sports Medicine and Physical Fitness, 59(10), DOI: 10.23736/S0022-4707.19.09615-4. 1691-1699.

Braun R. (2012, July 17) A Hawk-Eye for detail: how accurate is electronic judging in sport? Accessed on May 20, 2021. https://theconversation.com/a-hawk-eye-for-detail-how-accurate-is-electronic-judging-in-sport-8136.

Collins H, Evans R. (2008, July) You cannot be serious! Public understanding of technology with special reference to "Hawk-Eye". *SAGE PUBLICATIONS, Cardiff University, Public Understanding of Science,* 17(3), DOI: https://doi.org/10.1177/0963662508093370. 283–308.

Hawk-Eye at Wimbledon: it's not as infallible as you think (2013, July) The Guardian, England, UK, Accessed on May 20, 2021. https://www.theguardian.com/science/sifting-the-evidence/2013/jul/08/hawk-eye-wimbledon

Petkovic, M. Jonker, W. Zivkovic, Z. (2001). *Proceedings of the IASTED International Conference on Visualization, Imaging and Image Processing (VIIP 2001)* (page 5), Marbella, Spain, September 3-5, 2001

Hawk-Eye Innovations (2016, January 18) Hawk-Eye's Accuracy &Reliability Electronic Line Calling. Downloaded June 3, 2021.

Phys. Science X, (2008, June 12) We can be serious: Researchers dispute Hawk-eye's Wimbledon line call. Accessed on June 27, 2021. https://phys.org/news/2008-06-dispute-hawk-eye-wimbledon-line.html

Pscaife3. ELC - Understanding the tennis ball bounce (2016). Accessed on June 5, 2021. https://vimeo.com/135357489

Pugh W. (2019, July 14) HAWKEYES CLOSED England fans convinced Hawkeye is broken after Nicholls survives LBW review in Cricket World Cup final. The Sun, UK. Accessed on July 19, 2021. https://www.thesun.co.uk/sport/9503845/england-fans-hawkeye-broken-nicholls-lbw-cricket-world-cup-final/ Roke Manor Research Limited (2019, March). Accessed on July 5, 2021. https://en.wikipedia.org/wiki/Roke_Manor_Research

Thomas S. (2019, October 10) A-League invests A$150,000 in controversial Hawk-eye technology. Accessed on October 27, 2021. https://www.soccerscene.com.au/industry-4-0/a-league-invests-a150000-in-controversial-hawkeye-technology/

DEVELOPMENT OF LATENT FINGERMARKS ON DIFFERENT SUBSTRATES USING POLYANILINE-BASED POWDER OBTAINED BY SIMPLE PRECIPITATING METHOD

Nemanja Vučković, MSc[1]
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Nikola Glođović, MSc

Nikola Milašinović, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

PURPOSE

Forensic trace analysis implies the utilization of methods and techniques with the aim to identify and compare specific types of trace materials that could be transferred during the commission of a crime, and afterward the identification of a perpetrator and/or victim (Mozayani & Noziglia, 2006; Sonne, 2006). These trace materials include human and/or animal hair, textile fibers and fabric, rope, soil, glass, building materials and biological materials (Champod, Lennard, Margot, & Stoilovic, 2004; Sonne, 2006). However, fingermarks or fingerprints, as the common traces, represent about 10% of all material traces that could be recovered from a crime scene (Durose, Burch, Walsh, & Tiry, 2016), being one of the main tools used for identification of individuals in modern forensic science, due to their uniqueness, immutability, ease of classification and transferability (Mozayani & Noziglia, 2006). Fingermarks often remain as random marks, when the fingertip comes in contact with the surface of an object. The papillary line traces are transferred by the sweat (eccrine) glands, which secrete sweat and other components through the sweat pores. Additionally, the other compounds, such as blood, oil, dye, etc. can often be found and transferred from finger surface to the substrate along with the fingerprint (Datta, Lee, Ramotowski, & Gaensslen, 2001; Champod, Lennard, Margot, & Stoilovic, 2004; Lennard, 2007). Therefore, fingermarks

1 nemanjavuckovic95@gmail.com

could be divided in two main groups – the visible and latent (invisible) fingermarks. Visible fingermarks are easier for manipulation (e.g. photographing and lifting) when compared to the latent marks, requiring the visualization prior to processing and, for that purpose, different chemical, physical and optical methods are employed (Mozayani & Noziglia, 2006; Bumbrah, Sharma, & Jasuja, 2016; Milašinović & Koturević, 2016).

However, due to the aggressiveness and limitations of certain physical and chemical methods (Champod, Lennard, Margot, & Stoilovic, 2004), researchers are constantly attempting to develop new investigation approaches in forensic analysis of (latent) fingermarks. Polymeric materials are broadly used in different fields, such as vehicle and air industry, nanotechnology, medicine and pharmacy (Milašinović, Kalagasidis Krušić, Knežević-Jugović, & Filipović, 2010; Milašinović, et al., 2016), but scientific public is almost unaware and barely recognizes the potential of these materials in forensic applications (Lee, et al., 2014; Milašinović, 2016; Sen, Mohite, & Kayande, 2019). The goal of our previous researches was the utilization of biopolymeric materials (chitosan and dextran) in visualizing latent fingermarks, deposited on different (common) substrates and kept in different storage conditions. These so far promising achievements drove the us to the idea to extend our research to the utilization of synthetic polymeric materials (Vučković, Dimitrijević, & Milašinović, 2020; Vučković, Glođović, Radovanović, Janaćković, & Milašinović, 2020) that possess somewhat specific properties allowing the application of the prepared systems to various (illusive) surfaces. Polyaniline (PANI), one of the earliest known synthetic polymers, refers to a large class of conducting polymers. Synthetized from the cheap aniline, PANI can be found in one of three oxidation states: leucoemeraldine (white/clear & colorless), emeraldine (green or blue) and pernigraniline (blue/violet) (Heeger, 2001; Ćirić-Marjanović, 2010). On the other hand, unique properties (due to its inherent electrical activity), the ease of synthesis and low cost make PANI attractive to various industries and it is currently widely exploited in electronics (electrochromic glasses, solar cells, sensors, etc.), medicine (neural interfaces, scaffolds, delivery systems, etc.) and in anticorrosion materials (Ćirić-Marjanović, 2010; Beygisangchin, Abdul Rashid, Shafie, Sadrolhosseini, & Lim, 2021). However, there are not many studies regarding PANI application in forensic science (forensic trace analysis) (Beresford & Hillman, 2010; Beresford, Brown, Hillman, & Bond, 2012; Yuan, Li, Wang, Cao, & Lin, 2021).

In this paper, the polyaniline-based polymer powder, obtained by simple precipitating method, was synthetized and characterized with the aim to develop latent fingermarks deposited onto different surfaces, often found at the crime scene, i.e. plywood, glass and paper. The results demonstrated the potential of prepared PANI-based powder in developing latent fingermarks, as well as the ability to complement or replace some of the routinely applied physical methods.

DESIGN/METHODS/APPROACH

Materials

Aniline was purchased from Lach-Ner (Czech Republic), itaconic acid (IA) from Sigma-Aldrich (USA) and ammonium persulfate ($(NH_4)S_2O_8$) from Centrohem (Serbia). Distilled water was used for the preparation of all solutions, as well for the rinsing process. All materials were used without further treatment or purification.

Preparation of PANI-based powder

The PANI-based polymer powder was prepared by modifying the experimental procedures described by Yilmaz (2007). Briefly, 0.054 mole of ammonium persulfate was dissolved in 70 ml of 0.5 M IA in a 150 ml beaker and 0.054 mole of aniline was dissolved in 75 ml of 0.5 M IA in another 150 ml beaker, for one hour, at room temperature and low speed (~400 rpm). Afterward, the solution of $(NH_4)S_2O_8$ was added slowly to the aniline solution and then mixed for additional one hour, at the same conditions as already stated above. The obtained precipitate ("cake") in the form of emeraldine salt was collected on a Büchner funnel and flask using a water aspirator. The precipitate "cake" was washed with plenty (~1 l) of distilled water until the filtrate became colorless. After washing, the precipitate remained under suction for ~10 minutes until significant cracking of the moist "cake" occurred. Afterwards, the partially dried "cake" was transferred to a drying chamber at 37°C for additional few hours (until complete drying). Finally, the obtained dry formulation was ground with pestle and mortar to fine powder and kept in desiccator until further use.

CHARACTERIZATION OF THE PREPARED PANI-BASED POWDER

ATR FT-IR Analyses

The ATR-FTIR analyses were performed using Nicolet iS10 FTIR spectrometer (Thermo Scientific, USA), with a diamond attenuated total reflectance (ATR) smart accessory in the range of 4000-400 cm^{-1} at a resolution of 2 cm^{-1} and at 25°C.

SEM Analysis

SEM analysis was performed using electron microscope Tescan Mira3 XMU (Cranberry Township, USA). Prepared powder formulation was recorded in dry state. Before the analysis, dry powder formulation was coated using gold/platinum alloy (15/85) under vacuum using Polaron SC502 sputter coater.

Optical microscopy

The obtained PANI-based powder formulation and BVDA Magnetic black powder (control powder) (BVDA, The Netherlands) were recorded with optical microscope Leica FS C Comparison Macroscope, equipped with The Leica IM Matrox Meteor II Driver Software Module. Powders were recorded in dry state, with and without backlight. Prior to imaging under the microscope, latent fingerprints left on microscope glass slides were developed using prepared powder formulation and the control powder.

Development of latent fingermarks

In order to determine the performances of PANI-based powder formulation, three donors (two male and one female), using only a thumb of the right hand, deposited sebaceous/oily and dry fingermarks onto different non-porous, semi-porous and porous surfaces, i.e. plywood, glass and paper. The marks were then left under laboratory (humid) conditions for a short period of time. That period allowed the traces to dry and reduce the residues, until the latent fingerprints were developed with synthetized powder formulation and the control powder, using BVDA Squirrel hair brush and BVDA Magnetic brush (BVDA, The Netherlands), respectively (International Fingerprint Research Group, 2014).

Optical microscopy was used to determine performances of PANI-based polymer powder in visualizing latent fingermarks on glass surface, where the best results were obtained. Therefore, sebaceous fingerprints were randomly deposited onto the glass microscopic slides (properly labeled) and left for a few minutes. After this period, the fingermarks were separated into halves using a thin glass barrier and then the prepared powder formulation and BVDA Magnetic black powder were used for their visualization, according to the International Fingerprint Research Group (IFRG) (International Fingerprint Research Group, 2014).

FINDINGS

Prepared PANI-based polymer powder was used to develop latent fingermarks deposited onto three different substrates: plywood, glass and paper. Three different donors deposited fingermarks in accordance with the Guidelines proposed by the IFRG (International Fingerprint Research Group, 2014). Deposited sebaceous and dry fingermarks were halved with a thin slide barrier and two different powders were applied on the same fingermark – synthetized powder was applied to the left and BVDA Magnetic black powder (control powder) was applied to the right barrier side, using BVDA Squirrel hair brush and BVDA Magnetic brush, respectively. Both PANI-based powder and control powder were applied on mul-

tiple number of fingerprints on each substrate, to determine the performances and reproducibility of their application, i.e. to obtain satisfying results. The best results were obtained with the sebaceous fingerprints deposited onto the glass surface and developed with prepared PANI-based powder. On the other hand, development of dry fingerprints on each substrate with both powders was poor, without fingerprint basic form(s) and the papillary lines and therefore additional studies should be conducted, as it is already well known that visualization of dry marks is a challenging problem in forensic investigation of fingerprints (Cadd, Islam, Manson, & Bleay, 2015). The results obtained on plywood and paper substrate were satisfying, but with visible "overpowdering" of the fingerprints, since more powder particles retained in the porous (surface) structure of mentioned substrates. Additionally, disruption of papillary lines flow was observed on white paper surface, probably due to porous structure of the surface and the loss of fingerprint (sweat and lipid) residues.

a) b) c)

Figure 1. *Sebaceous fingerprints developed on: a) glass, b) paper and c) plywood surface, using PANI-based powder (left-half side of the images) and BVDA Magnetic black powder (right-half side of the images), recorded under visible light using white background surface for appropriate contrast (for glass and paper substrate)*

Figure 1 shows sebaceous fingerprints of one donor, developed with prepared powder (left-half side of the images) and the control powder (right-half side of the images) on three different substrates, i.e. glass, paper and plywood. The prints were then photographed under visible light with a 12 MP camera (aperture *ƒ*/2.2, pixel size 1.22 μm), using white background surface for appropriate contrast (for glass and paper substrate).

When comparing fingerprints developed with PANI-based powder and BVDA Magnetic black (control) powder on different surfaces, the best results were obtained on glass surface, with visible and clear fingerprint image, basic patterns, papillary lines and some minutiae points, as well (Figure 1, a)). PANI-based powder also showed satisfying results on paper and plywood surface, with obvious

fingerprint pattern and basic characteristics, but with noticeable disruption of papillary lines flow (on paper surface) and "overpowdering" of fingermarks (on plywood surface) (Figure 1, b) and c)). On the other hand, by comparing PANI-based powder with control powder in developing latent fingermarks, it is evident that equally good and comparable results were obtain on each surface, showing satisfying and very promising result.

ATR FT-IR Analyses

ATR FT-IR analyses were performed in order to determine interactions between components of synthetized formulation, i.e. interactions due to polymerization process. Figure 2 shows spectra of PANI-based polymer powder (emeraldine salt) and pure aniline. Both spectra contain some specific bands: very weak and broad band around 3400–3200 cm^{-1}, assigned to the N–H stretching vibrations (primary and secondary amines), and weak band near 3050–3030 cm^{-1} due to the C–H stretching (Habib & Maheswari, 1989; Kulkarni, Viswanath, & Khanna, 2006; Yilmaz, 2007). Peak shifting and decrease in intensity from 1599 cm^{-1} at spectrum of pure aniline to 1568 cm^{-1} at spectrum of prepared PANI-based powder can be related with mixed C=C and C–N stretching in a quinoid ring (Kulkarni, Viswanath, & Khanna, 2006; Yilmaz, 2007). Furthermore, the band around 1496 cm^{-1} at spectrum of pure aniline shifts to the band around 1488 cm^{-1} of a lower intensity at spectrum of PANI-based polymer powder and it is associated with C–C stretch in a benzenoid ring and C–H mixed vibrations (Quillard, Louarn, Lefrant, & Macdiarmid, 1994; Yilmaz, 2007). The peak around 1272 cm^{-1} at spectrum of pure aniline resulted in two new bands at spectrum of PANI-based powder, around 1294 and 1236 cm^{-1}, which can be assigned to C–N stretching (secondary aromatic amine) and C–H bending vibrations, due to bonding of aromatic rings in the polymerization process (Habib & Maheswari, 1989; Kulkarni, Viswanath, & Khanna, 2006; Yilmaz, 2007). Additionally, very weak peak around 1117 cm^{-1} at spectrum of pure aniline is slightly shifted to a broad band around 1120 cm^{-1} at spectrum of PANI-based powder, probably related with deformation of aromatic ring and C–H (in plane) bending (Quillard, Louarn, Lefrant, & Macdiarmid, 1994; Kulkarni, Viswanath, & Khanna, 2006; Yilmaz, 2007). Decrease in intensity of peak around 880 cm^{-1} at spectrum of prepared powder is associated with plane vibration in para-disubstituted aromatic rings, indicating polymer formation (Quillard, Louarn, Lefrant, & Macdiarmid, 1994; Kulkarni, Viswanath, & Khanna, 2006). Strong peak near 499 cm^{-1} at spectrum of pure aniline resulted in a formation of a weak peak around 505 cm^{-1} at spectrum of prepared powder, which can be ascribed to deformation of C–H (out of plane) of 1–4 disubstituted aromatic ring (Kulkarni, Viswanath, & Khanna, 2006; Yilmaz, 2007).

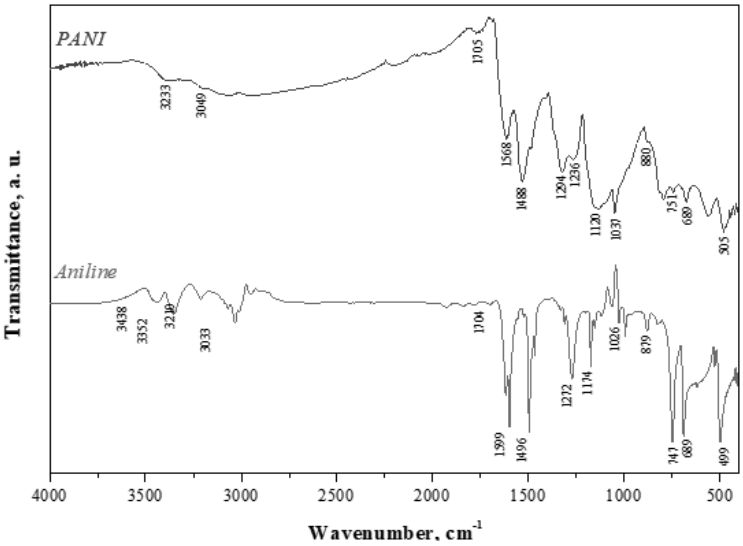


Figure 2. *ATR FT-IR spectra of prepared PANI-based powder (emeraldine salt) and pure aniline*

The shifting of peaks from spectrum of pure aniline to spectrum of prepared powder was also confirmed in studies of aniline polymerization by Trchova et al. (2005) and aniline doping by Ilic et al. (2000). A broad band around 1150-1100 cm^{-1} was assigned, as stated by Quillard et al. (1994), to the "electronic like band" and is considered to be a measure of the degree of delocalization of electrons and therefore denoted as a characteristic peak of PANI conductivity. Additionally, in the region around 1300 cm^{-1}, the peaks are associated with the presence of aromatic amines in polyaniline (Yilmaz, 2007).

SEM Analysis

SEM analysis was performed in order to determine microparticle morphology and surface fineness, their size and uniformity. Figure 3 shows SEM micrographs of prepared PANI based-powder, at different magnifications.

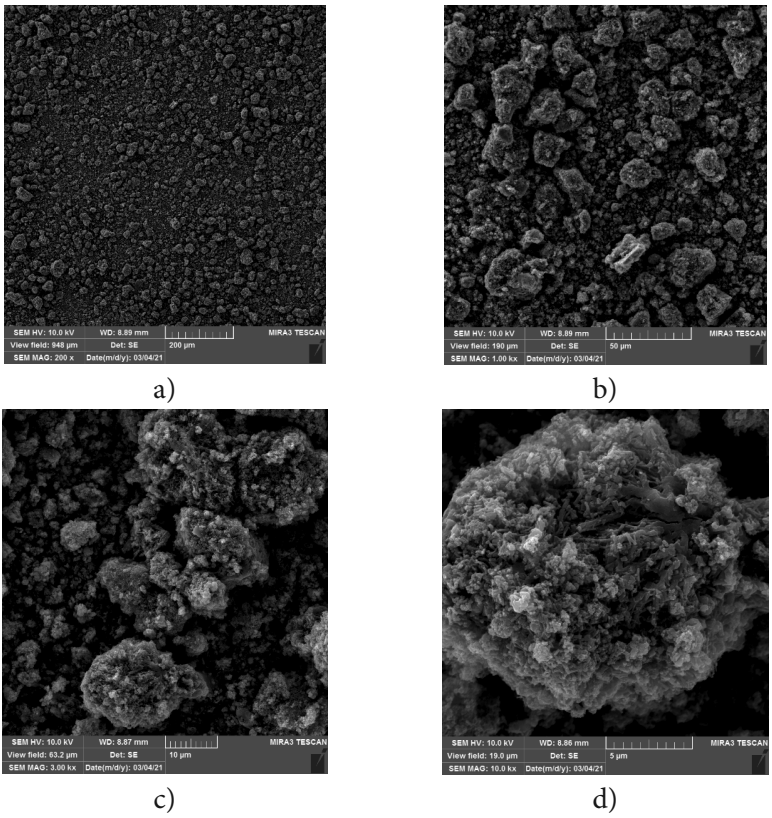


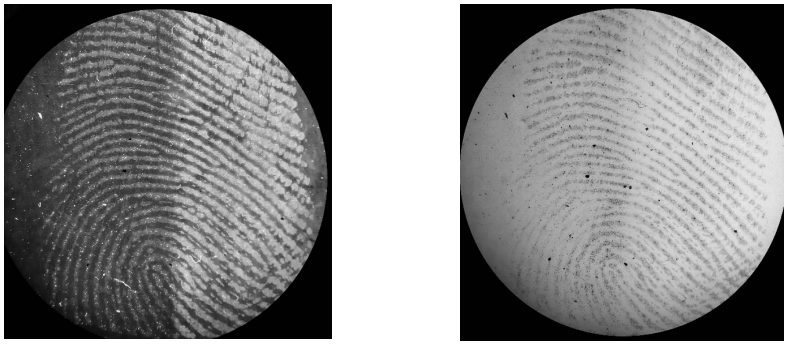
Figure 3. *SEM micrographs of PANI-based polymer powder, at different magnifications: a) ×200; b) ×1000; c) ×3000; d) ×10000*

SEM analysis showed that the particles of prepared powder were somewhat fine and uniform in size, which is additionally complemented by their small diameter size. The diameter of particles of prepared powder (~ 20 µm) was even smaller than some commercial magnetic powders, described in research of Gürbüz and associates (2015). Therefore, good binding of these particles to the fingerprint sweat and lipid residues was observed. We assume that small diameter particles managed to bind to and visualize papillary line traces with their continuous flow (on glass surface) and did not retain in the interpapillary space, which was very satisfying result.

Optical microscopy

In order to confirm results obtained from initial testing of powders, as well as hypothesis from SEM analysis, PANI-based powder and BVDA Magnetic black powder were used for visualization of latent fingermarks on glass surface. Therefore, three donors deposited sebaceous fingermarks onto labeled glass microscop-

ic slides using technical scale (force applied to accommodate 100–150 g, per fingermark) and the fingermarks were left for a few minutes, which allowed the traces to dry and reduce the residues. After this period, the fingermarks were separated into halves using a thin glass barrier, and then two different powder samples were used for their visualization – synthetized PANI-based powder was applied to the left and BVDA Magnetic black powder (control powder) was applied to the right barrier side, using BVDA Squirrel hair brush and BVDA Magnetic brush, respectively. Afterwards, the samples of enhanced fingermarks were recorded under the optical microscope (magnification ×15), using dark-field (Figure 4, a)) and bright-field (Figure 4, b)) contrast techniques.



a) b)

Figure 4. *Sebaceous fingerprint deposited onto glass microscopic slide, left for a few minutes and developed using PANI-based powder (left-half side of the images) and BVDA Magnetic black powder (right-half side of the images), recorded with optical microscope (magnification ×15), using: a) dark-field and b) bright-field contrast techniques*

When compared to the BVDA Magnetic black powder, PANI-based powder showed even better results in terms of visualizing latent fingerprints, by developing the papillary lines with their continuous flow and making perceptible some minutiae, as well. When observing the fingerprint developed with control powder, obtained fingerprint pattern was somewhat blurred and "overpowdered", but with visible papillary lines and some minutiae points. Additionally, when applied with a brush, prepared powder formulation bound with fingerprint residues and did not remain in the interpapillary spaces. Based on the obtained results, very promising visualization of sebaceous fingerprints was achieved using glass surface as a substrate, and with cheap PANI-based powder system.

ORIGINALITY/VALUE

In this research, PANI-based polymer powder, obtained by simple precipitating method, was prepared and characterized with the aim of evaluating its performance as a fingerprint powder. PANI-based powder was used due to low price and availability of aniline, as well as for easy synthesis process. Based on the obtained results, prepared powder formulation showed the best properties when developing sebaceous fingermarks deposited onto glass substrate, with good binding capacity to the fingermark residues and their clear development. Additionally, satisfying results were obtained on white paper and plywood substrate, with obvious fingerprint image, basic patterns and some minutiae points, as well. However, there were some drawbacks: disruption of papillary lines flow was observed on white paper substrate; the "overpowdering" of the fingermarks was present when developing marks on plywood substrate; dry fingermarks were not visualized on any substrate, with neither powder, so additional studies need to be performed to overcome these problems. On the other hand, as many commercial fingerprint powders, this formulation requires no prior knowledge, the method itself is non-destructive and prepared powder is easily applicable with standard/commercial fingerprint brushes. Finally, additional researches could include doping of prepared formulation, with the aim of expanding utilization of this PANI-based powder system on other (conductive) substrates and potentially supplementing or replacing some of the routinely used physical methods (fingerprint powders) in visualizing latent fingermarks.

REFERENCES

Beresford, A. L., & Hillman, A. R. (2010). Electrochromic Enhancement of Latent Fingerprints on Stainless Steel Surfaces. *Analytical Chemistry, 82*(2), 483–486.

Beresford, A. L., Brown, R. M., Hillman, A. R., & Bond, J. W. (2012). Comparative Study of Electrochromic Enhancement of Latent Fingerprints with Existing Development Techniques. *Journal of Forensic Sciences, 57*(1), 93–102.

Beygisangchin, M., Abdul Rashid, S., Shafie, S., Sadrolhosseini, A. R., & Lim, H. N. (2021). Preparations, Properties, and Applications of Polyaniline and Polyaniline Thin Films – A Review. *Polymers, 13*(12), 1–46.

Bumbrah, G. S., Sharma, R., & Jasuja, O. (2016). Emerging latent fingerprint technologies: a review. *Research and Reports in Forensic Medical Science, 6*, 39–50.

Cadd, S., Islam, M., Manson, P., & Bleay, S. (2015). Fingerprint composition and aging: A literature review. *Science & Justice, 55*(4), 219–238.

Champod, C., Lennard, C. J., Margot, P., & Stoilovic, M. (2004). *Fingerprints and Other Ridge Skin Impressions* (2nd ed.). Boca Raton, Florida: CRC Press, Taylor & Francis.

Ćirić-Marjanović, G. (2010). Polyaniline Nanostructures. In A. Eftekhari, *Nanostructured Conductive Polymers* (pp. 19–74). Chippenham, UK: John Wiley & Sons.

Datta, A. K., Lee, H. C., Ramotowski, R., & Gaensslen, R. E. (2001). *Advances in Fingerprint Technology* (2nd ed.). CRC Press, Taylor & Francis.

Durose, M. R., Burch, A. M., Walsh, K., & Tiry, E. (2016). *Publicly Funded Forensic Crime Laboratories: Resources and Services, 2014.* Bureau of Justice Statistics.

Gürbüz, S., Özmen Monkul, B., İpeksaç, T., Gürtekin Seden, M., & Erol, M. (2015). A systematic study to understand the effects of particle size distribution of magnetic fingerprint powders on surfaces with various porosities. *Journal of Forensic Sciences, 60*(3), 727–736.

Habib, M. A., & Maheswari, S. P. (1989). Electrochromism of Polyaniline: An In Situ FTIR Study. *Journal of The Electrochemical Society, 136*(4), 1050–1053.

Heeger, A. J. (2001). Nobel Lecture: Semiconducting and metallic polymers: The fourth. *Reviews of Modern Physics, 73*, 1–20.

Ilic, M., Koglin, E., Pohlmeier, A., Narres, H. D., & Schwuger, M. J. (2000). Adsorption and Polymerization of Aniline on Cu(II)-Montmorillonite: Vibrational Spectroscopy and ab Initio Calculation. *Langmuir, 16*(23), 8946–8951

International Fingerprint Research Group (IFRG). (2014). Guidelines for the Assessment of Fingermark Detection Techniques. Downloaded June 1, 2022. https://ifrg.unil.ch/wp-content/uploads/2014/06/IFRG-Research-Guidelines-v1-Jan-2014.pdf.

Kulkarni, M. V., Viswanath, A. K., & Khanna, P. K. (2006). Synthesis and Characterization of Conducting Polyaniline Doped with Polymeric Acids. *Journal of Macromolecular Science, Part A: Pure and Applied Chemistry, 43*(4–5), 759–771.

Lee, J., Pyo, M., Lee, S., Kim, J., Ra, M., Kim, W.-Y., Park, B. J., Lee, C. W., & Kim, J.-M. (2014). Hydrochromic conjugated polymers for human sweat pore mapping. *Nature Communications, 5*, 10.

Lennard, C. (2007). Fingerprint detection: current capabilities. *Australian Journal of Forensic Sciences, 39*(2), 55–71.

Milašinović, N. (2016). Polymers in Criminalistics: Latent Fingerprint Detection and Enhancement – From Idea to Practical Application. *NBP – Journal of Criminalistics and Law*, 133–148.

Milašinović, N., Čalija, B., Vidović, B., Crevar Sakač, M., Vujić, Z., & Knežević-Jugović, Z. (2016). Sustained release of *α*-lipoic acid from chitosan microbeads synthetized by inverse emulsion method. *Journal of the Taiwan Institute of Chemical Engineers*, *60*, 106–112.

Milašinović, N., Kalagasidis Krušić, M., Knežević-Jugović, Z., Filipović, J. (2010). Hydrogels of *N*-isopropylacrylamide copolymers with controlled release of a model protein. *International Journal of Pharmaceutics*, *383*, 53–61.

Milašinović, N., & Koturević, B. (2016). *Uvod u hemiju: praktikum za laboratorijske vežbe.* Belgrade: Academy of Criminalistic and Police Studies.

Mozayani, A., & Noziglia, C. (2006). *The Forensic Laboratory Handbook Procedures and Practice.* Totowa, New Jersey: Humana press.

Quillard, S., Louarn, G., Lefrant, S., & Macdiarmid, A. G. (1994). Vibrational analysis of polyaniline: A comparative study of leucoemeraldine, emeraldine, and pernigraniline bases. *Physical Review B, 50*(17), 12496–12508.

Sen, D., Mohite, B., & Kayande, N. (2019). Review on Polymer. *International Journal of Pharmaceutical Sciences and Medicine, 4*(10), 1–15.

Sonne, W. J. (2006). *Criminal Investigation for the Professional Investigator* (1st ed.). Boca Raton: Taylor & Francis.

Trchová, M., Šeděnková, I., & Stejskal, J. (2005). In-situ polymerized polyaniline films 6. FTIR spectroscopic study of aniline polymerisation. *Synthetic Metals, 154*(1–3), 1–4.

Vučković, N., Dimitrijević, S., & Milašinović, N. (2020). Visualization of Latent Fingerprints Using Dextran-based Micropowders Obtained From Anthocyanin in Solution. *Turkish Journal of Forensic Sciences and Crime Studies, 2*(2), 3–53.

Vučković, N., Glođović, N., Radovanović, Ž., Janaćković, Đ., & Milašinović, N. (2020). A novel chitosan/tripolyphosphate/*L*-lysine conjugates for latent fingerprints detection and enhancement. *Journal of Forensic Sciences, 66*(1), 149–160. doi:DOI: 10.1111/1556-4029.14569

Yilmaz, F. (2007). Synthesis of Polyaniline (Emeraldine Base) at 25°C. *Polyaniline: Synthesis, Characterization, Solution Properties and Composites.* Doctoral dissertation, 64–66. Ankara, Turkey: The Graduate School of Natural and Applied Sciences of Middle East Technical University.

Yuan, C., Li, M., Wang, M., Cao, H., & Lin, T. (2021). A critical review of fundamentals and applications of electrochemical development and imaging of latent fingerprints. *Electrochimica Acta, 390*, 1–15.

THE ONLINE DRUG MARKET AS A CURRENT LAW ENFORCEMENT CHALLENGE

Vince Vári, PhD[1]
Faculty of Law Enforcement, University of Public Service, Budapest, Hungary

INTRODUCTION

The COVID-19 pandemic has not only targeted our biological immune systems; it has also penetrated our social fabric, transforming traditional methods and affecting how we work, travel, and even spend our leisure time. As a result, it has also significantly impacted our everyday lives in terms of social relationships, contact, and communication. Because traditional social spaces for face-to-face interaction and connection, such as the workplace, education, and offline platforms for leisure activities, have been restricted by public policies, social life and activity have shifted to digital online spaces (URL1). What was previously a complementary and occasional substitute or auxiliary tool for the lack of opportunities for face-to-face interaction has now taken on a prominent and exclusive position. And public policies have made their use routine and everyday, making them part of everyday life and opening up a way of improving the quality of activities in online spaces. This has led to a massive demand for online communication software, educational and work platforms, and improving the quality of development activities to meet the growing number of needs. As life has increasingly conditioned our daily activities in the online space, criminal activities that typically involve face-to-face contact, such as traditional drug trafficking (URL2), have been eroded. Of course, no epidemic can or has ever been able to eliminate and eradicate the demand for drugs, and this pandemic situation is no different. However, there is one significant difference: when a social crisis has arisen for whatever reason – economic, political, or health-related – criminal activities related to drugs have been at most temporarily reduced and sometimes even temporarily suspended. They would

1 vari.vince@uni-nke.hu

then continue in the traditional drug market system and distribution pattern once the crisis had disappeared and social peace had been consolidated.

In contrast, during this period, an alternative way of life became a reality, which, with its many positive and beneficial features, brought about a significant transformation in social life. On the other hand, these changes have brought about additional social, economic, and political scenarios (URL3). These changes have significantly impacted the areas that frame their daily lives and have had a decisive influence, no longer allowing the return to the same conditions that were previously so characteristic. Consider, for example, that multinational companies employing large numbers of people have realized how much more economical it is to work from home (URL4). There is also a trend for younger generations to prefer more convenient ways of accessing services online, alongside older generations (URL5). The COVID-19 epidemic has therefore set in motion a process that has significantly reshaped our habits. This has affected the global drug trade, a highly profitable business that has started to use the online world as an alternative to, and perhaps instead of, the traditional distribution network to avoid a significant reduction in revenues compared to the previous period. The issue of the "delocalization" of drug trafficking has also been reflected in the "reach" of law enforcement. The main reason is that law enforcement organizations are geared toward crime in the physical space. In other words, the legal framework, the tools, the organizational structure, and the possibilities of action are primarily designed to prosecute drug-related crimes in a conventional setting (Tihanyi et al., 2020/a). While criminality is more flexible in its transformation, bound by informal constructs at most, law enforcement cannot show the same flexibility within highly rigid and entrenched legal and organizational structures. Of course, over time, the legal system and organizations can keep pace with changes in crime, as they always have, but we are now faced with a more complex problem than before (Tihanyi et al., 2020/b). A new type of behavior has emerged, such as bank card fraud or even illegal acts in information systems, but drug trafficking crime has moved into a decisively different space. This, by its very nature, requires a very different response and attitude from law enforcement authorities.

IMPACT OF THE COVID-19 PANDEMIC ON THE DRUG MARKET

2020 will see the introduction of varying degrees of restrictive measures across Europe, unprecedented in peacetime, including the shutdown of all non-essential services, border closures, restrictions on the right of assembly, and freedom of movement. This situation has directly impacted a wide range of behaviors related to drug use and supply and has disrupted health care and some law enforcement activities.

In 2018, nearly 269 million people used drugs, a 30 percent increase from 2009. The majority of drug users are adolescents and young adults. While the increase reflects population growth and other factors, the data also show that illicit drugs are now more diverse, potent, and available (URL6). The relaxation or elimination of some public health measures has reestablished the conditions for the drug market to return to and even exceed pre-COVID-19 levels. The coronavirus pandemic also caused enormous damage to the economy, fundamentally affecting our daily lives, all of which, as touched on in the introduction, had less impact on the profitability of the drug market. There were even countries where the market recovered due to closures, although this required dealers (URL7) to be flexible in responding to the changed circumstances. The EU law enforcement agency Europol has published a report summarizing its key findings, comparing data and processes in the first months of 2020. The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) contributed to its preparation (URL8). It is shown that the epidemic has significantly overridden the previous rules for a drug crime. For example, the raw chemicals that form the basis of synthetic opiates such as methamphetamine and fentanyl come primarily from China, including the epidemic's source in the Hubei province (URL9). Difficulties resulting from disrupting supply chains have severely hampered the supply chain, causing a short-term price hike. It is particularly true for drugs such as heroin or crystal, which are physically addictive (URL10). Theoretically, the price increase anticipates a contraction of the drug market in most segments, but this is not what the Europol report suggests. Europeans spend at least €30 billion a year on drugs at the retail level, making the drug market the primary source of income for organized crime groups in the European Union. Around two-fifths (39%) of this amount is spent on cannabis, 31% on cocaine, 25% on heroin, and 5% on amphetamines and MDMA. The most recent data show that overall drug availability in Europe remains "very high" and that consumers have access to a wide range of high purity and high potency products at varied but decreasing prices. An essential overarching theme of the report is the environmental impact of drug production, including deforestation and the dumping of chemical waste, which leads to ecological damage, safety risks, and high clean-up costs. Organized crime groups are rapidly seizing new opportunities for financial gain and exploiting technological and logistical innovations to expand their activities beyond international borders. Nevertheless, drugs are now more accessible to European consumers, often through social media and the Internet. The 2019 report only hints at the potential impact, which was translated into a comprehensive analysis in 2021. According to the UN Office on Drugs and Crime's World Drug Report 2020, only one in eight people will receive the drug dependence treatment they need. There are nearly 35.6 million drug addicts in the world (URL11). As a result, the drug market has been able to withstand the disruptive effects of the pandemic extraordinarily. Drug traffickers have adapted to travel restrictions and border closures.

As a result, the drug market has been remarkably resilient to the disruptive effects of the pandemic. Drug traffickers have adapted to travel restrictions and border closures. At the wholesale level, this is reflected in some changes in routes and methods, with greater reliance on container smuggling and commercial supply chains and less reliance on human couriers. Although early government restrictions disrupted street-based retail drug markets and localized supply shortages, dealers and buyers appear to have adapted by using encrypted messaging services, social media apps, online resources, and postal and door-to-door delivery services. It raises concerns that one of the possible long-term consequences of the pandemic could be that drug markets become even more digitalized. Several new distribution strategies for the drug market have emerged. The demand for so-called party drugs has fallen due to the lack of festivals, and the retail price of cocaine and opiates has increased somewhat in most European Member States, as has the prevalence of new psychoactive substances. Violence between groups involved in the retail and wholesale trade has grown in some European countries.

As demand declined, severe struggles for customers, territory, and distribution channels began (Ritter, 2020). Following difficulties in the initial supply chain due to the disruption of the Crown's supply chain, organized criminal groups involved in drug crime recognized the advantages of the digital space for drug distribution. In most countries affected by the lockdown, there has been a significant decline in street drug distribution-related crime, but it has increasingly shifted to the online space, where there is also the dark web (Dornfeld, 2020: 200). Traditional criminal groups have thus opened up to cyberspace, becoming more closely intertwined with cybercriminals engaged in other illegal activities there (URL12). The system and functioning of cybercriminal groups have been examined by Michael Mcguire, who points out that traditional criminal organizations are increasingly expanding their activities on the Internet, while newer and less closely linked criminal groups are forming. Criminal groups show different levels of organization depending on whether they operate online only, use online tools to enable them to commit crimes in the "real" world, or use a combination of both online and offline (Mcguire, 2012).

THE DIFFICULTIES OF THE ONLINE DRUG MARKET FOR LAW ENFORCEMENT

Hungary remains both a transit and a destination country for drug trafficking. Most types of drugs enter the country from abroad, with domestic production playing an increasingly important role only in the case of marijuana (Mátyás, 2020). Drug prices have remained unchanged compared to 2009, with heroin

prices decreasing slightly as its active ingredient content has decreased. The most significant development in the drug market in the last two years has been the transformation of the synthetic drug market, with the disappearance of ecstasy tablets and the emergence and unusually rapid spread of new powders and tablets, many of which contain legal psychoactive substances. In police seizures, the Institute of Criminal Experts and Research identified five new compounds in 2009, sixteen in 2010, and thirty-three in 2011 (URL13). As a result of the coronavirus, drugs are sold online, in chat rooms, on the darknet, or on other online platforms (URL14). It is combined with encrypted telecommunication tools that give consumers access to order drugs and medicines to meet their needs directly and without the risk of being caught, bypassing the traditional "dealer" distribution chain, both physical and in person. In darknet markets, there is no physical encounter. In addition, the drug trade in the digital space provides criminal organizations with a significantly higher profit margin than the traditional distribution system, which is recycled back into the "legal" economy through various assets through money laundering activities (URL15). The trade conducted on online platforms and the formally legal entities and companies linked to "legalizing" money laundering make asset tracing extremely difficult (Kármán et al., 2016). A similar feature of the online drug market is that drugs are mostly posted abroad, delivered by parcel services, mostly foreign-registered, and have a massive turnover at doorstep or parcel delivery points (Mezei, 2019). The organizational and IT capacities of the police alone are not sufficient to conduct a meaningful investigation of every online drug order and delivery once the goods arrive at the airport and are realized by the National Tax and Customs Administration (NAV), following the reports made. With the proliferation of the Internet and the potential of net marketing, a significant part of the downstream distribution market activity in the drug market takes place through this sales channel. In many cases, the buyer and seller are only virtual actors (Ritter, 2020).

THE EX OFFICIO APPROACH AS THE "ACHILLES' HEEL" OF EFFICIENCY

The countries and societies determine the functioning and values of organized crime groups and the cultures in which they operate and are thus influenced by the geography, politics, criminal tradition – such as illegal demands – and structure and effectiveness of law enforcement (Tóth, Kőhalmi, 2016, 608). In law enforcement, when criminal groups are strengthening and increasing their presence and realizing increasing profits from their illegal activities, it becomes a critical issue that a restrictive legal environment is in place that does not weaken the performance of the authorities. An examination of Hungary's criminal procedural

system reveals that the main obstacle is the principle of ex officio prosecution, based on the strict principle of legality that is characteristic of continental legal systems. In those legal systems where the principle of legality applies, the police cannot exercise the power of diversion. Diversion is most effective at the beginning of the procedure, which is why it is essential that each legal system allows prosecutors and investigating authorities to use it. Diversion is derived from the Latin word *divertere*, which means to deviate (URL16). The term entered the public domain in 1967, when the President of the United States put it into practice by referencing the final report of the Committee on Law Enforcement and the Judiciary (Nejelski, 1982: 434). Diversion is a summary term for deviating from the usual "stages" of criminal proceedings (Barabás, 2004:60). If they become aware of a crime from any source, they must initiate proceedings ex officio. However, the police can use a solution when they talk down the complainant in cases of trivial actions, do not take up the complaint, and do not act on reports. It is called "hidden diversion". It also results in minor offenses not being prosecuted (Blau, 1987, 29). So we are faced with the problem that, although the system tacitly accepts hidden divergence, and because of capacity limits, it actually "does not take up" cases, especially for those offenses where latency is high and considerable investigative work is required to detect them. The main problem is that in the case of online drug trafficking, there is no way for the investigating authority to operate covert diversion because the knowledge of the crime is documented by the fact that the drug appears in physical space during the delivery of the parcel services. The authorities detect these; they are obliged to initiate procedures that result in a massive increase in cases, thus increasing the case processing workload. Much of the traditional drug trafficking has been "invisibly" conducted based on a secret. With open-source information from various sources, the authorities have operated with the "hidden" diversion tool. They have been able to decide which cases and offenders to target with what amount of time and investigative capacity. The physical availability of the police is not relevant for online drug trafficking. Responsiveness is the more relevant factor (Mátyás, et al., 2019).

The 1998 Act XIX of 1998 on Criminal Procedure (referred to as the former Be.) – as a form of diversion – recognized the institution of partial disregard of the investigation, which was hardly used in practice. It is because it requires a detected and investigated offense. According to the former Be. § 187 (1), after questioning the suspect, the prosecutor may, by decision, dispense with a further investigation into an offense which is of no relevance for the prosecution, due to the more severe offense committed. However, it was impossible to refrain from investigating if there was no possibility of successful detection or if investigations into minor offenses jeopardized the success of proceedings for more severe offenses. The current Act XC of 2017 on Criminal Procedure (hereinafter referred to as: Be.) only offers the prosecutor the option of discontinuing the investigation as an alterna-

tive to the decision. Under Section 398 (2) of the Be., the prosecutor's office shall terminate the proceedings if e) they are pending for an offense which, apart from the more severe offense committed, is of no relevance for the prosecution of the perpetrator. Even though this no longer requires a case to be detected and investigated, prosecutors still do not use it more often. Thus, the legislator's assumption that the work already invested by law enforcement would not result in a shift away from the traditional method of prosecution has not been proven correct.

CRIMINAL PROCEDURAL AND ORGANIZATIONAL SOLUTIONS TO IMPROVE LAW ENFORCEMENT EFFECTIVENESS AGAINST ONLINE DRUG CRIME

In agreement with the theory of Lévai, who, in terms of criminology, divides drug crime into the supply side associated with organized crime and the demand side associated with traditional crime (Lévai, 1992: 61), increasing the effectiveness of drug law enforcement is essential on the supply side because the results achieved there have a significant impact on the cost of sales and consequently, as a price-increasing factor, reduce availability on the demand side. Reduced access is especially severe for poorer groups who are actively involved in the lower end of the drug supply chain (Reuter, 2006). It is clear that urgent and more effective action against drug trafficking than is currently the case requires more effective law enforcement, better technical equipment, training of the relevant bodies, and practical information exchange and cooperation with the relevant international bodies. To this end, the effectiveness of countermeasures must be increased, the bodies responsible for combating criminal organizations must be strengthened, and the human, material, and technical basis for criminal expertise must be reinforced. In addition to the above, a national-level service for the fight against drug-related crime should be set up (URL17). As stated in the National Security Strategy, closer cooperation between law enforcement agencies (police and national security services) and the judiciary at the national and international level, particularly within the European Union, and the efficient use of existing resources, are essential to fight organized crime (URL18). In drug supply reduction/safety, the new EU Drugs Strategy 2021–25 also recognized the increased threats of the online drug market, thus targeting all aspects of illicit drug markets (URL19).

As discussed in the previous chapter, the main obstacle is the principle of strict legality, which operates without exception and without relaxing it. The police are forced to conduct all drug-related cases, which prevents them from strategically focusing their substantive investigative capacities on more effective action against drug-related criminal organizations. The principle of legality is the consequence of

the criminal code, while officiality is the requirement to initiate and conduct proceedings ex officio (Király, 2000: 115). Thus, first of all, the possibilities to amend the Be. should be reviewed and the possibility of not investigating should be introduced in the interest of law enforcement. It would be applied where there is no natural or legal person as a victim of the offense; there is no cumulative offense, or the danger of the offense to society is negligible (in the case of offenses punishable by imprisonment up to 3 years), so that the investigating authority could refrain from opening an investigation if there is a more significant law enforcement interest. Otherwise, there may be many reasons for not prosecuting, such as cooperation with the prosecution or the institution of undercover investigators (Mészáros, 2019). The above arguments are supported by the fact that in 2019, according to Act C of 2012 on the Criminal Code (hereinafter referred to as: Criminal Code), 4972 persons were convicted, of which 1620 persons were convicted for drug trafficking (§ 176–177), which is a supply-side conduct, and 3322 persons were convicted for possession of drugs (§ 178–180), which is typically a demand-side conduct. This illustrates the investigating authority's focus, which it cannot influence in its own power due to the aforementioned principle of officialism. It would be advisable for the Prosecutor General's Office to establish an internal protocol of regulation and cooperation between the prosecution and the investigating authority, which would not allow for divergent practices between the different bodies with different competencies and jurisdictions. It would be necessary for efficiency to standardize procedures so that it would not be necessary to arrest, seize and carry out other covert investigative measures for any minor drug trafficking. It is based on the principle of strict legality for any factual, ergo illegal, albeit minor conduct that is of little danger to society if brought to the attention of the authorities (Belovics, 2007). Therefore, the discretion of the police authority should be more comprehensive, based on the strategic decisions generated by the analytical evaluation work. For orders not exceeding "low volume" by consumers, records and OSINT analysis should be conducted (Szabó, 2019) to map and analyze the relationship networks between customers, thus revealing the existing "consumer nodes". In addition, the sale of drugs takes place on social media platforms, mainly on the darknet (Serbakov, 2020). Consumers who place orders and request delivery in "small" quantities for individual use should preferably not be investigated, as they tie up law enforcement capacity (Vári, 2014). Moreover, trends in recent years show that the gap between female and male offenders in drug-related crime is narrowing in favor of female offenders (Tihanyi et al., 2020/c).

On the other hand, clandestine investigative activities should be carried out, and data should be collected to establish the links, connections, and networks between bulk orders (§§ 261–266 of the Criminal Code). For those not fitting into a more extensive system, a more complex criminal structure (distribution network, criminal organization, money laundering) should be subject to preliminary pro-

ceedings without opening investigations. However, where it can be established that drugs are being ordered in large quantities and in an organized manner, the blocking of electronic channels to remove and secure the necessary electronic data should be used as an urgent measure, especially in the case of foreign suppliers (Art. 337 (1) of the Criminal Code). An essential investigative measure is requesting data from companies providing commercial mail-order services for mapping order volumes for persons or addresses who have ordered several times. In particular, it is necessary to establish who has requested the delivery of what weight of the parcel and when, and how and when the parcel's sender paid for the goods to be forwarded. The legislation must be amended to tighten the rules on parcel delivery so that only payment by credit card or bank transfer is possible for orders of this type of material. Furthermore, a clearly defined minimum set of data on the sender should be made available to parcel delivery companies. It can ensure traceability and the identification of persons.

CONCLUSION

The pandemic has had a significant impact on the drug market. In the early stages of the pandemic, disruptions in the drug supply chain were a significant price driver. There appeared to be a decline in sales, which could be permanent. In contrast, and in addition, the epidemic triggered changes that affected people's daily lives and acted as a catalyst for the digital revolution. As a consequence, people's online presence has increased in general. During the pandemic, more and more people spent their working and leisure time online. Organized crime offered a significant proportion of its drugs online, giving drug distributors easier and cheaper access to a now increased customer base. The process was also aided by the fact that it was easier to conceal identities and set up front companies online than offline. The drug market, open to cybercrime, has used its potential to serve its ends by shifting part of its distribution system to delivery by mail-order services, which are less regulated. Another pandemic consequence, which reinforced the untraceability of orders, was the proliferation of online shopping and non-cash means of payment. In the online drug market, bulk drug orders are placed in unencrypted chat rooms on the darknet and other online platforms. Delivery services do not record customer data, and payment methods are not documented by the supplier due to the use of cryptocurrencies or cash payments. They thus cannot be traced (Baráth, 2021: 27). However, the discovery of parcels containing drugs entering the country from abroad, mostly in small quantities, does happen due to air and international transport. It places the NAV under an obligation to report to the police authorities with jurisdiction and competence. It also means a massive increase in the number of cases on the investigation side. In addition, many parcels

are arriving within the EU which do not even come to the attention of any of the authorities. Moreover, the investigations launched into suspicious parcels naturally reduce investigative efficiency, which is particularly damaging on the supply side, because not enough attention is paid to these high-profile crimes. Some legal and organizational solutions could be offered to the investigating authorities to avoid investigating drug offenses that would otherwise be on the demand side, the Achilles'heel of which would be to relax the strict principles of legality and officialism. The legislative change could also improve the effectiveness of detection and evidence if parcel services were to record significantly more data when taking orders. It would also greatly improve the effectiveness of law enforcement if a separate unit were set up to deal with illegal activities in the online drug market and explore the links between the drug dimension of organized crime and cybercrime. The online drug trade is a significant challenge for law enforcement. There is no time for delay in working out legal and professional solutions to curb the online drug supply as quickly as possible.

REFERENCES

Barabás, A. T. (2004). *Börtön helyett egyezség? Mediáció és más alternatív szankciók Európában.* Budapest: KJK-KERSZÖV Jogi és Üzleti Kiadó Kft.

Baráth, N. E. (2021). Kábítószer-kereskedelem és droghasználat alakulása a COVID-19 pandémiás időszakban. *Interdiszciplináris Drogszemle,* 2, 25–32.

Belovics, E. (2007). A jogellenesség és a társadalomra veszélyesség konfliktusa. *Iustum Aequum Salutare* 3(3).

Blau, E. (1987). *Diversion und Strafrecht.* Berlin: Jura

Dornfeld, L (2020). A koronavírus-járvány hatása a kiberbűnözésre. *In Medias Res*, 2, 193–204.

Kármán G, & Mészáros, Á. &Tilki, K. (2016). Pénzmosás a gyakorlatban. *Ügyészségi Szemle,* (23)3, 82–98.

Király, T. (2000). *Büntetőeljárási jog.* Budapest: Osiris

Lévai, M. (1992) *Kábítószerek és a bűnözés.* Budapest: Közgazdasági és Jogi Kiadó.

Mcguire, M. (2012). *Organised Crime in the Digital Age.* London: John Grieve Centre for Policing and Security.

Mátyás Sz. & Sallai, J. & Tihanyi, M. &Vári, V. (2019). A rendőri elérhetőség és a bűnözés közötti összefüggések térbeli elemzése. *Területi Statisztika,* (59) 2, 152–163.

Mátyás, Sz. (2020). *A kábítószer-bűnözés elleni küzdelem mint stratégiai kihívás a magyar bűnüldözésben.* Budapest: NKE

Mészáros, B. (2019). A fedett nyomozó bűncselekményeinek jogi megítélése az új büntetőeljárási törvény alapján. *Miskolci Jogi Szemle: A Miskolci Egyetem Állam- és Jogtudományi Karának folyóirata,* 2(2). Különszám, 141–149.

Mezei, K. (2019). A szervezett bűnözés az interneten. In: *A bűnügyi tudományok és az informatika.* Pécsi Tudományegyetem Állam- és Jogtudományi Kar; MTA Társadalomtudományi Kutatóközpont, Budapest – Pécs, 125–147.

Nejelski, P. (1982) Diversion the Promies and the Danger. In: *Juvenile Delinquency.* New York: A Book of Readings, Giallombardo, R.

Reuter, P. (2006). What drug policies cost. Estimating government drug policy expenditures. *Addiction*, 101(3), 315–322.

Ritter, I. (2020) Karanténban a drogpiac? A COVID 19 pandémia hatásai a globális drogpiacra. *Ügyészek Lapja,* (27) 4–5, 35–49.

Serbakov, M. T. (2020). Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. *Büntetőjogi Szemle.* 1, 91–107.

Szabó, K. (2019). Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről. *Nemzetbiztonsági Szemle*. 7(2), 68–82.

Tihanyi M., & Mátyás, Sz.& Vári, V.& Krasnova, K. (2020/a). A Drug Policy in Hungary: Current Trends and Future Prospects, *Сибирское юридическое обозрение* 17(4), 485–494.

Tihanyi M. & Mátyás, Sz.& Vári, V. (2020/b). Drug policy in Hungary: genesis of legal regulation. In: Д. В., Рыбин (пред.); Е. В., Трофимов (edt.) *Актуальные проблемы развития государственности и публичного права: материалы IV международной научно-практической конференции,* Sankt-Peterburg, Oroszország: Санкт-Петербургский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста) 192, pp. 18–22.

Tihanyi, M. & Mátyás, Sz.& Vári, V.& Krasnova, K.& Volkova, M. (2020/c).. Correlation between Female Identity in Civil Society and Criminal Repression in Hungary and Russia, *Russian Law Journal*, (8)4, 92–108.

Tóth, M. & Kőhalmi, L. (2016). A szervezett bűnözés. In: Borbíró, A. & Gönczöl K. & Kerezsi, K. & Lévay, M.: *Kriminológia.* Wolters Kluwer Kft. Budapest.

Vári, V. (2014). Hatékony vagy eredményes a bűnüldözés. *Magyar Rendészet.* (14)1, 87–97.

INTERNET SOURCES

(URL1) Digital technology is changing our lives. The EU's Digital Agenda aims to make this transformation work for citizens and businesses while helping to achieve the goal of Europe becoming a climate-neutral continent by 2050.

The Commission is determined to make 2020–2030 Europe's "Digital Decade". Europe must strengthen its digital sovereignty and set its own standards rather than follow those of others. It must accomplish this by prioritizing data, technology, and infrastructure. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_hu

(URL2) Europol: Catching the virus. Cybercybercrime, disinformation and the COVID-19 pandemic, 3 April 2020, https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf.

(URL3) Milyen jövő vár Európára a koronavírus járvány után? (What future awaits Europe after the coronavirus epidemic?) http://library.fes.de/pdf-files/bueros/budapest/16375.pdf

(URL4) Technology companies have long since made the concept of remote working fashionable. Citing a previous study, the World Economic Forum points out that 98 percent of the workforce wants the opportunity to work remotely. https://www.allianz.hu/hu_HU/lakossagi/sajtoszoba/sajtokozlemenyek/munkavegzes-a-covid-utan.html

(URL5) https://www.nak.hu/tajekoztatasi-szolgaltatas/koronavirus/102582-a-koronavirus-atalakitotta-a-vasarlasi-szokasokat-is

(URL6) https://unis.unvienna.org/pdf/2020/Op-Eds/WDR_ED_Waly_HU.pdf

(URL7) The Hungarian language clearly associates the word "dealer" with drug trafficking. On the one hand, the "dealer" "drugs" his prospective victims, i.e. he acts as an agent for the drugs, and on the other hand, he serves the customer. https://www.szomagyarito.hu/szocikk.php?id=42

(URL8) The EU Drugs Market Report (including the executive summary) is available in English and is accompanied by flagship policy and practice publications and 13 background documents that address the gaps identified in 2016. The report is part of a series published every three years (since 2013). https://www.europol.europa.eu/newsroom/news/2019-eu-drug-markets-report-emcdda-and-europol

(URL9) https://www.vice.com/en/article/bvgazz/sinaloa-cartel-drug-traffickers-explain-why-coronavirus-is-very-bad-for-their-business?utm_source=dmfb&fbclid=IwAR3ZWrpRjwB-nwWsnF9oBEWTXLnttg7V6oAyqOxNri6t8GMKa_HF6jqeKcA

(URL10) https://index.hu/gazdasag/2020/03/24/kabitoszer_drogkereskedelem_sinaloa_metamfetamin_fentanil_heroin_mexiko_kartel_drog_dragul_a_koronavirus_miatt/

(URL11) https://unis.unvienna.org/pdf/2020/Op-Eds/WDR_ED_Waly_HU.pdf

(URL12) http://drogfokuszpont.hu/wp-content/uploads/EMCDDA_EDR_2021_HU.pdf

(URL14) H/11798. számú országgyűlési határozati javaslat a Nemzeti Drogellenes Stratégiáról 2013-2020 Tiszta tudat, józanság, küzdelem a kábítószer-bűnözés ellen. (H/11798. proposal for a parliamentary resolution on the National Anti-Drugs Strategy 2013–2020. Clear conscience, sobriety, fight against drug-related crime) https://www.parlament.hu/irom39/11798/11798.pdf

(URL15) http://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/chatszobaban-adtak-vettek-a-kabitoszert

(URL16) https://idegen-szavak.hu/diverzi%C3%B3

(URL27) H/11798. számú országgyűlési határozati javaslat a Nemzeti Drogellenes Stratégiáról 2013-2020 Tiszta tudat, józanság, küzdelem a kábítószer-bűnözés ellen. (H/11798. Proposal for a parliamentary resolution on the National Anti-Drugs Strategy 2013–2020. Clear conscience, sobriety, fight against drug-related crime) https://www.parlament.hu/irom39/11798/11798.pdf

(URL18) 1163/2020. (IV. 21) Kormány Határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 151. pont (1163/2020.(IV. 21) Government Decision on the National Security Strategy of Hungary, 151).

(URL19) https://data.consilium.europa.eu/doc/document/ST-14178-2020-REV-1/hu/pdf

LEGAL SOURCES

Act CX of 2017 on Criminal Procedure (Be.), "Hungarian Gazette", No. 99/2017.

Act C of 2012 on Criminal Code, (Btk.) "Hungarian Gazette", No. 92/2012.

Act XIX of 1998 on Criminal Procedure (former Be.), "Hungarian Gazette", No. 37/2002.

H/11798. Proposal for a parliamentary resolution on the National Anti-Drug Strategy 2013–2020. Clear conscience, sobriety, fight against drug crime. https://www.parlament.hu/irom39/11798/11798.pdf (Date of download: 14/06/2022).

Government Decision 1163/2020 (21.IV.) on the National Security Strategy of Hungary, point 151. https://data.consilium.europa.eu/doc/document/ST-14178-2020-REV-1/hu/pdf (downloaded on 17/06/2022).

THE POSSIBILITIES OF USING UNMANNED AERIAL VEHICLES – DRONES IN CRIME SCENE INVESTIGATION[1]

Ivana Bjelovuk, PhD[2]
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Tanja Kesić, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Milan Žarković, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

INTRODUCTION

In order to ensure the quality of an investigation and crime scene processing as its segment, it is first necessary for authorized officials to establish the perimeter of the crime scene properly, and then to secure and protect it until the arrival of the crime scene investigation team. Only an unchanged appearance of the crime scene allows for a high quality and thorough collection of relevant information, objects and traces, in order to elucidate a criminal offence or event. The perimeter of the crime scene should encompass all traces that are found (Bjelovuk, 2022: 107). At the very beginning of crime scene investigation, it is recommendable to make a few photographs of the crime scene as it was found. The gathering of data at the crime scene is usually done in practice as part of the criminalistic-tactical tasks, while the crime-investigation experts and forensics specialists deal with the

1 This paper is the result of the realization of scientific research project titled *Development of Institutional Capacity, Standards and Procedures for Countering Organized Crime and Terrorism in Terms of International Integrations*. The project is funded by the Ministry of Science and Technological Development of the Republic of Serbia, No. 179045.
2 ivana.bjelovuk@kpu.edu.rs

forensic investigation of the crime scene, which involves inspecting the scene, finding and then marking and preserving relevant objects and traces. In order to be able to make a decision about which objects and traces are relevant to the solving of a crime case, the specialist must understand the mechanisms of using the objects and the origins of traces, and be able to create a mental reconstruction of the event. Because of this, it is necessary for them to possess some specific professional knowledge and the skills for carrying out investigation and the forensic analysis of the physical evidence they found on site. They should also be familiar with the further procedure of the analysis of found objects and traces in the forensic lab, in order to observe/respect/ensure the chain of custody and its continuity, given that they take part in its formation. There are multiple methods which allow the specialists to document the crime scene properly, or to prove what happened at it: the verbal method, the photographic method, the video method, the measuring and graphic method, and the method of lifting (Žarković, et al., 2012: 117). Securing the scene of an event, whether it is a crime scene or the scene of a traffic accident etc., involves permanently preserving the important features of the scene for further analysis (Lipovac, et al., 2019: 280). The end result of a completed crime scene investigation is the investigation documentation, whose main components include the documents created after the found state of the scene of the event was preserved. Elements of the documentation are the investigation report, the report of the forensic inspection of the scene, photo documentation, sketches and the situational plan. Court practice has shown that the most important element of the investigation documentation is the investigation report (there were cases in practice where documentation was accepted as adequate despite not having any other elements aside from the investigation report, while in cases where there was no investigation report the documentation was deemed to be inadequate). Because of this, the documentation is organized in such a way as to attach all other elements of the investigation documentation to the investigation report.

Because the purpose of an investigation is to establish material facts about a certain event which is the subject of the investigation, the contents of a quality investigation documentation must fully match the factual state at the scene of the event. There are three basic principles that must be observed while making the investigation documentation and these are the principles of objectivity, comprehensiveness, and compliance (Lipovac et al., 2018: 39). Respecting these principles while producing investigation documentation ensures that the documentation contains only such facts as an authorized official has established by observation or on the basis of personal expert knowledge. The investigation documentation should contain everything that the authority in charge of the proceedings and all other users thereof may find important. All of its elements should be mutually synchronized, in terms of their contents, terminology, but also their substance. Regardless of who

is in charge of an investigation, its success rate is closely related to the applied professional knowledge and the used equipment (Žarković et al., 2012: 98).

Using the verbal method for describing the factual state at the scene implies the use of words. In order to be more efficient, it is suggested to use a dictation recorder, and then later to enter the facts into a textual document (the investigation documentation, the forensic report on the crime scene investigation and other written documents). The use of measuring and graphic method for documenting the state of the crime scene requires specific knowledge and equipment, as well as measuring instruments (measuring tapes, laser rangefinder, angle measuring devices, etc.) and the creation of a sketch and a situational plan of the scene (drawing kit, a computer with drawing software such as AutoCAD or ScenePD, etc.).

When it comes to photographing and video recording as the methods of documenting the situation and details of the crime scene, it is a fact that analogue devices have been phased out, and that digital cameras and camcorders whose technical characteristics allow for the level of quality required for investigation photography are used instead. Although rarely, certain countries use photogrammetry devices and equipment (Lipovac et al., 2010). Analytic photogrammetry involves the use of cameras and computers in order to establish all the measurements needed for the analysis, the creation of a situational plan or even a 3D model of the crime scene, or some specific objects. In the criminalistic-technical field, that is forensic analysis of the crime scene, spheric photography is also used, and it includes panoramic photographing using a camera from a few determined points of view, and then a software matching of the photos, so that the software such as *Easypano* or a similar one should allow for a virtual "walk around" the scene (Bjelovuk, 2022: 120). Another modern device that finds its use in the forensic analysis of the crime scene is the thermal vision camera (Kesić & Bjelovuk, 2021). Unmanned aerial vehicles could also find their place in the forensic investigation of crime scenes.

UNMANNED AERIAL VEHICLES

Drones are unmanned aerial vehicles, or aircraft, which are controlled using a unit located on land, or on an object on land, on a ship, on a different aircraft, or other vehicle by a navigator. They are remotely controlled. They receive controls from a station that is on land, in the water, in the air, at a nearby or a distant location. Unmanned vehicles also include the ones that autonomously travel along a predetermined trajectory, using an auto pilot. These flying devices are constructed in a way that allows them to function without a human crew or a pilot, and they can be reused many times, with the exception of cruise missiles, which are loaded

with an explosive charge and intended for destroying their targets. Unmanned aircraft can also be combined, meaning that they are partially controlled by a unit on land, and partially fly on their own, using previously memorized navigational data. Over the last couple of years, the definition of an unmanned aircraft has changed, so that "the U.S. Department of Defense (DoD), followed by the FAA and the European Aviation Safety Agency (EASA), adopted the term UAS or Unmanned Aircraft System" (Valavanis & Vachtevanos, 2015: 44).

They found the most widespread use for military purposes,[3] where they first started being used for scouting, target marking, combat and other goals, but were later adapted for civil use. Thus, unmanned aircraft find their place in agriculture, traffic, photography and other fields. They are manufactured from different materials that possess certain characteristics; they should be light, but durable at the same time. The materials that are most often used include plastic and composite materials. The technical specifications of the aircraft (dimensions, weight, load capacity, power, cruise speed, maximum speed on optimal altitude, tactical radius, range, flight ceiling, lift-off speed, etc.) differ from model to model. They might even possess multiple engines depending on their construction. While constructing an aircraft like this, just as when creating a manned aircraft, it is very important to pay attention to its aerodynamics. The basic elements of an unmanned aircraft construction are the body/housing, the control unit, the signal receiver, the battery, and a mobile device. The kind of sensor used on an unmanned aircraft depends on the type and purpose of the aircraft. Controlling an aircraft requires a specially trained user. On the controlling unit, there is a screen which allows for real time tracking of the aircraft's position in the air, and also the footage from the onboard camera.

The use of unmanned aerial vehicles for photographing crime scenes presents a real revolution in capturing the situation at the crime scene. In order for this technology to transition into being routinely used by the forensic crews that investigate crime scenes, a comparative analysis should be made of conventional methods of crime scene investigation and the use of unmanned aircraft or drones, as they are also referred to. Photos made from above, from the so-called birds' eye view, allow for a better overview of the objects, items and traces found at the crime scene, especially in the case when there are both wide and narrow angle shots of the crime scene. This can even be applied in the cases involving an aircraft falling from a great height, especially in the case of a prior explosion on the aircraft in the air, when the spread area of objects and traces (wreckage pieces, bodies and possessions of the casualties) can encompass up to a few square kilometres of geographically varied, and poorly connected and accessible terrain (Žarković et al.,

3 Predator MQ-1 drones were used as espionage tools during the wars in the Balkans. The operators of the unmanned aerial vehicles flew them from hangars in Albania. See more on this in: М. Мазети, *Хируршки прецизно* [M. Mazeti *Surgical Precision*], Лагуна, 2014, стр. 108.

2009:195) In addition, the use of unmanned aircraft is much more practical, when compared to the frequently necessary recording from a helicopter (for instance, for getting a wider picture of the event scene) because of the size and mass of the vehicle, as well as the cost of operating it. The weight/mass of unmanned aircraft in civil use does not exceed 150 kg. It is easier to manoeuvre/steer an unmanned aircraft than a massive machine such as a helicopter. These vehicles also require a smaller surface to take off and land. Depending on the manufacturer and the model of the aircraft, the range varies from 200 m to 2000 m from the control unit.

When an unmanned aerial vehicle is used to photograph something, the quality of the photograph is very important. It depends on a lot of factors, such as the following, for example: the relative position of the camera and the object being captured; whether the camera is moving or standing still in relation to the object, and vice versa. With that in mind, it is very important to properly set up the parameters for recording, the shutter aperture and exposure length which regulate the amount of light that is allowed through the objective. When the object and the camera are in a state of relative movement, that is, when they are moving in relation to one another, it is important for the exposure to be as short as possible, in order to avoid capturing a series of consecutive positions, thus rendering the recording unclear. Also, the quality of the recording is affected by the resolution, which is directly related to the price of the aircraft. Because of this, the camera that the aircraft uses to capture footage must be stable (any motion and movement of the vehicle must be stabilized) for the recording to be clear. Logically, the camera should have the highest resolution possible, as the resolution will directly influence the quality of the recording.

External conditions under which the recording is made may also affect the quality of the footage. Drones can be used both indoors and outdoors. The wind is known to have a significant effect on the recording quality. The effect of the wind can partially be predicted by using a software solution, but unexpected wind surges must always be taken into consideration. The cameras which are built into these aerial vehicles are of various DSLR[4] technologies.

Considering that these vehicles are operated by a software and remote control, they can be vulnerable, so a lot of attention must be given to their cyber security (Yağdereli, et al., 2015). Another issue that comes into focus is battery life. Bearing this in mind, it is vital for the operator in the field to be supplied with spare batteries with a long-life span and a precise indicator of their charge level.

Drones can be equipped with high resolution photo and video cameras, thermal imaging cameras, heat sensors, radars and other devices which allow them to scan the terrain according to different parameters, so they can be used with the aim

4 Digital Single-Lens Reflex camera

of finding human remains (Dukowitz, 2020), and can also be equipped with face recognition software. So, it should not come as a surprise that the use of drones, as well as processing the data collected by them, requires specialized training. It is worth noting, that there are experts specializing in the analysis and interpretation of drone-collected data (https://digitpol.com/drone-forensics/).

LEGAL FRAMEWORK FOR USE OF UNMANNED AIRCRAFT

The advent of unmanned aircraft, the ever-increasing potentials for their use and their availability to a large number of users, has naturally given rise to the question of legal regulations for this kind of aircraft. Because of this, a lot of countries have codified some of the most important questions regarding the use and the necessary conditions for safe usage of unmanned aircraft. Especially important in this area is the legal regulation of police usage of unmanned aircraft, considering that they are being used more and more frequently in daily police activities, including for detecting and solving criminal cases. Certain authors point out that the possibilities of the usage of drones, or as they sometimes call them "planes with brains", are almost unlimited (Dwyer-Moss, 2017/2018: 1049). The necessity of the existence of precise and clear rules about the usage of this kind of aircraft stems from the needs of air space safety and national security, as well as from the fact that with their usage may involve violation of the basic rights and freedoms of the citizens, primarily the right to privacy.

The first state in the world to solve legally the question of the use of unmanned aircraft was Australia by creating the Civil Aviation Safety Regulations in 1998. Some subsequent changes regulated the safe usage of drones, which were then described as Remotely Piloted Aircraft (RPA). These amendments contained a general prohibition against operation of an RPA in a way that created a hazard to another aircraft or personal property, which was supported by more specific provisions concerning the operation of Remotely Piloted Aircraft Systems (RPAs) (Butler, 2014: 437-439). These regulations were subsequently amended in 2016 to clarify requirements and limitations governing safe operation of RPAs. This new scheme categorizes RPA by size and weight. The concept of 'standard RPA operating conditions', which is defined in regulation, implies that the RPA is operated within the visual line of sight of the person operating it and the RPA is operated at or below 400 ft above ground level, by day. Also, it is stipulated in what circumstances the RPA is not operated: in a prohibited area; in a restricted area; within 3 nautical miles of the movement area of a controlled aerodrome; over an area where a fire, police or other public safety or emergency operation is being conducted without the approval of the person in charge of the operation, etc.

(Butler, 2019: 1043-1044). In the beginning, the registration of these vehicles was not required, but it was later requested for any aircraft heavier than 250 g. Also, unmanned aerial vehicle operators should be educated about the basic rules of air traffic safety. Despite all this, Australian legislation still contains no provisions on the usage of cameras, and recording from drones (Butler, 2019: 1044).

In the United States, the usage of drones is regulated on both the federal and state levels. The federal legislation makes a distinction between the usage of drones for recreational and commercial purposes. Special rules apply for the aircraft used by certain agencies, including the police. The Code of Federal Regulation (Title 14, 2016) introduced mandatory registration of all drones, the terms for their safe usage and the conditions that must be met by the people operating them. The Federal Aviation Administration (FAA) is responsible for introducing, supervising, and implementing the federal rules that apply to the usage of drones. A part 107 license "allows operations of drones or unmanned aircraft system (UAS) under 55 pounds at or below 400 feet above ground level for visual line-of-sight operations only". Also, this rule has a number of other restrictions, including not being allowed to fly a drone at night. Some flight restrictions associated with a part 107 license can be overcome by applying for waivers (Drones – A Report on the Use of Drones by Public Safety Agencies and a Wake-Up Call about the Threat of Malicious Drone Attacks, 2020: 7). In order to become part 107 certified, each drone pilot for the agency needs to pass the FAA's Aeronautical Knowledge Test to obtain a Remote Pilot Certificate (Drones – A Report on the Use of Drones by Public Safety Agencies and a Wake-Up Call about the Threat of Malicious Drone Attacks, 2020: 7). As regards the use of drones by the police, the part 91 COA (Certificate of Authorization) applies. Operating under the part 91 COA allows the police agency to set standards for determining whether someone is ready to be a pilot, because they do not need to take the FAA's Aeronautical Knowledge Test (Drones – A Report on the Use of Drones by Public Safety Agencies and a Wake-Up Call about the Threat of Malicious Drone Attacks, 2020: 7). A COA provides authorization for activities that are prohibited by part 107, such as flying at night, flying beyond the visual line of sight, flying over people, flying at altitudes above 400 feet above ground level, and flying in controlled airspace (Drones – A Report on the Use of Drones by Public Safety Agencies and a Wake-Up Call about the Threat of Malicious Drone Attacks, 2020: 7-8). Under a part 107 license, the drone is considered a civil aircraft for commercial operations, whereas under a COA, the drone is considered a public aircraft that is only used for governmental purposes (Drones – A Report on the Use of Drones by Public Safety Agencies and a Wake-Up Call about the Threat of Malicious Drone Attacks, 2020: 7-8).

When talking about the usage of drones by the police, it is interesting to note the Freedom from Unwarranted Surveillance Act was enacted in 2015 in Florida.

This law prescribes that law enforcement agency may not use a drone to gather evidence or other information, except:

1. to counter a high risk of a terrorist attack by a specific individual or organization if the United States Secretary of Homeland Security determines that credible intelligence indicates that there is such a risk;

2. if the law enforcement agency first obtains a search warrant signed by a judge authorizing the use of a drone;

3. if the law enforcement agency possesses reasonable suspicion that, under particular circumstances, swift action is needed to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect or the destruction of evidence, or to achieve purposes including, but not limited to, facilitating the search for a missing person;

4. to provide a law enforcement agency with an aerial perspective of a crowd of 50 people or more, provided that: the law enforcement agency must have policies and procedures that include guidelines: for the agency's use of a drone; or the proper storage, retention, and release of any images or video captured by the drone; that address the personal safety and constitutional protections of the people being observed.

A drone may be used to assist a law enforcement agency with traffic management and to facilitate a law enforcement agency's collection of evidence at a crime scene or traffic crash scene. Otherwise, evidence obtained or collected in violation of this act is not admissible as evidence in a criminal prosecution in any court of law in Florida.

In the Republic of Serbia, the question of unmanned flying vehicles is only partially legally solved. Namely, the Air Traffic Act defines an unmanned aircraft as an aircraft whose crew is not located on board, and that is either controlled remotely or uses autonomous flight (Article 3, paragraph 1, item 4). According to these regulations, unmanned aircraft can be used for commercial, scientific, educational, sporting and other purposes as long as they do not interfere with air traffic safety (Article 10, paragraph 1). The Directorate for Civil Aviation was tasked with determining more precise conditions for the safe usage of unmanned flying vehicles, their categorization, equipment, registration and maintenance, along with the requirements that the parties that operate unmanned aircraft must meet. The law also provides for responsibility of persons using an unmanned aircraft for any potential damage caused through its use (Article 10, paragraphs 2 and 3). Along with the responsibility for the caused damage, a legal entity could be liable for breaking the law if they used an unmanned aircraft in such a way as to endanger air traffic safety or that is contrary to conditions prescribed by the law. Natural persons can also be held responsible for these offences. The same law also mentions that the act of flying a foreign unmanned aircraft in the airspace of the Republic of Serbia

without permission of the Directorate for Civil Aviation is considered a violation of the state's airspace (Article 23, paragraph 2). In order to get approval to fly from the Directorate for Civil Aviation, one must first obtain the consent from the ministry in charge of defence (Article 23, paragraph 3). In the case of any breach of this legal obligation, legal and natural subjects shall answer for their infraction (Article 258, paragraph 1, item 15 and Article 260, paragraph 1, item 13).

Some more detailed regulations concerning unmanned aircraft can be found in the Regulation on Unmanned Aircraft (hereinafter: the Regulation), which was adopted by the Civil Aviation Directorate in 2020. The Regulation determines the conditions for the safe use of unmanned aircraft, their classification, categorization, maintenance and the conditions which the parties that operate them must meet. However, the provisions of the Regulation only apply to: unmanned aircraft, whose maximal take off mass (MTOM) is less than 0.25 kg, whose maximum speed does not exceed 19 m/s and which cannot achieve more than 80 J of kinetic energy; unmanned aircraft whose maximal take off mass (MTOM) is greater than 150 kg; unmanned aircraft that are used for operational needs of the authorities responsible for defence, internal affairs and customs, and for flying unmanned aircraft in enclosed spaces. The Regulation requires the registration of unmanned aircraft in the Aircraft Registry, and allows for the maximum flight altitude of 100 meters above the ground, unless the Directorate has previously approved the flight to go ahead at a greater altitude and allocated the required air space. It is important to note, that the Regulation generally stipulates that an operator of an unmanned aircraft (whether a national or a foreign citizen) must be a of age, a person in good health who has passed an aptitude test that proves that they have the knowledge necessary for safely operating an unmanned aircraft (Article 20).

As in the presented comparative laws of other countries, the legislation of the Republic of Serbia also defines unmanned aircraft, their types, and the conditions for their safe usage. We especially point out the importance of regulating the competencies of unmanned aircraft operators, because expertise and competence, just as in all other professions, guarantee proper and lawful action (Bjelovuk et al., 2021: 233). However, unlike the legislation in the United States, Serbian law does not specifically regulate the use of unmanned aircraft by the police. This omission can also be noticed in the cases where the police use some other technical means such as, for example, thermal vision cameras, because using them endangers the right to privacy and makes room for their illegal use (Kesić & Bjelovuk, 2019: 999). With this in mind, it is important for the lawmakers to resolve these issues as soon as possible.

DISCUSSION

Because investigations take place in order to establish facts about some event, which may have taken place at various, sometimes inaccessible locations, the use of these devices can prove very useful. It could reduce the risk of injury of the investigation team members, it would allow for much faster access and insight into the situation at the event scene, and then a much more adequate choice of necessary measures, manpower and equipment, in line with the circumstances of the case at hand. Also, the use of unmanned aircraft could be very useful for situations where an investigation must be conducted following an explosion. Namely, in these locations, where forensic investigation is very peculiar, there is a risk of new explosions. Here, the use of these flying vehicles can be very important, because recording the scene can help notice and neutralize the danger of new explosions.

Conventional methods for crime scene investigation start with gathering information about the event (what crime or event took place, who perpetrated them, what are the consequences, the time when it occurred etc.) that took place, and about the location (micro and macro location), and then inspecting the crime scene using senses and equipment (different kinds of lighting devices and detectors). In order for the original state at the crime scene to remain unchanged, it is necessary for a forensic investigator to enter the very scene and start making photographs according to the methodology of crime scene photography. Generally, he/she must wear protective equipment and have predetermined guidelines that are to be followed while at the crime scene, in line with the international standard operational procedures from the ISO 17020 standard. The main flaw of this approach to the crime scene is the factor of human error because inattention and unprofessional behaviour might contaminate or alter the crime scene. Also, even with the necessary caution and controlled movement of the investigation team members, the risk of contamination is practically impossible to avoid when it comes to latent or hardly visible footsteps of the perpetrator (Žarković, et al., 2010: 735). This risk could be avoided by using an unmanned aircraft, considering the fact that it does not have any physical contact with the crime scene. (Sharma, et al., 2019) Using an onboard camera, it is possible to gain an insight into the situation at the scene, and to record during the static phase of the investigation. Recording from an unmanned aircraft is much less time consuming when compared to the conventional method of doing it at the crime scene. However, this gives rise to new issues regarding the quality of the footage received from an unmanned aircraft, and the possibility of a cyber security breach in respect of the collected data. Also, it would require special training of the operational forensic experts that are charged with investigating the scene. Another issue is recording during the so-called dynamic phase of the investigation, where it is necessary to make certain movements at the crime scene. It goes without saying that the use of unmanned aircraft by forensic teams, and also the use of the

footage collected from them further in the legal process for specific legal issues, must be properly regulated by the law.

When a trace is found at a crime scene, it calls for scale photography, which allows proper reading of the trace dimensions from a photograph. When using an unmanned aircraft, this activity becomes more complicated.

Forensic crime scene investigation also requires the use of the measuring-graphic method (sketching of the scene) with the goal of determining the coordinates of the positions of various objects and traces at the crime scene, which requires further footage analysis using special software in order to map the recorded terrain. The traces are found by the forensic investigators. Certain traces require being taken from the crime scene for further analysis in forensic laboratories. This involves physically removing the trace and sampling the crime scene, packing and marking the packaging, in order to ensure the chain of custody. When using an unmanned aircraft, this activity becomes more complicated.

The use of unmanned aircraft requires additional education of the crime scene investigation team members, both for controlling the aircraft, and for the processing of the collected data. Also, using the necessary software requires licensing, which increases the cost of use of this equipment.

CONCLUSION

Modern technology makes a lot of jobs considerably easier to do, including the ones in the field of forensic investigation of crime scenes. But, the application of this technology involves new risks, and the possibility of misuse. It could be useful to combine the conventional means of forensic crime scene investigation with recording from unmanned aircraft in the situations where it is necessary for the safety of the investigation team members (for example, an investigation of the crime scene under a risk of explosion).

The currently existing operational procedures that are applied in the forensic practice during crime scene investigation do not recognize the use of unmanned aircraft. Their use in everyday and routine forensic crime scene investigation should be delayed. Even though the use of unmanned aircraft makes human activities in certain areas easier, it also carries the risk of misuse, starting with using the aircraft as a weapon to destroy various targets, illegal collection of personal data, or other unethical behaviours. This claim is supported by the fact that the legal regulations of the Republic of Serbia for the use of unmanned aircraft for forensic crime scene investigation are not complete.

REFERENCES

Bjelovuk, I. (2022). Kriminalistička tehnika. Beograd: Kriminalističko-policijski univerzitet.

Bjelovuk Ivana, Kesić Tanja, Žarković, M. Comparative Analysis of Competences in the Fields of Fire and Explosion, Revija za kriminalistiko in kriminologijo, (2021), vol.72(3), 233-244.

Butler, D. (2014). The Dawn of the Age of the Drones: An Australian Privacy Law Perspective. University of New South Wales Law Journal, Vol. 37(2), 434-470.

Butler, D. (2019). Drones and Invasions of Privacy: An International Comparison of Legal Responses. University of New South Wales Law Journal, Vol. 42(3), 1039-1074.

Code of Federal Regulations, www.law.cornell.edu, available 1st Sept.2022.

Drones – A Report on the Use of Drones by Public Safety Agencies and a Wake-Up Call about the Threat of Malicious Drone Attacks (2020), www.cops.usdoj.gov > RIC > cops-w0894-pub, accessed on 1st Aug.2022

Dukowitz, Z. Drones for CSI—How Drones Can Help Criminal Forensic Scientists Find Human Remains. 2020. Available at https://uavcoach.com/drones-criminal-forensics/#:~:text=Using%20drones%20equipped%20with%20infrared,parties%20should%20concentrate%20their%20efforts.

Dwyer-Moss, J. (2017/2018). The Sky Police: Drones and the Fourth Amendment, Albany Law Review, Vol. 81(3), 1047-1070.

Freedom from Unwarranted Surveillance Act, www.leg.state.fl.us/, available 1st Aug.2022

Žarković, M., Bjelovuk, I., Kesić, T. (2010). Kriminalistički i dokazni aspekti postupanja sa tragovima stopala, *Pravni život, časopis za pravnu teoriju i praksu*. God. 59, knjiga 539, (9), 729-742 (glavni i odgovorni urednik prof. dr Slobodan Perović).

Žarković M., Mlađan, D., Bjelovuk, I. (2009). Criminal investigation procedure on the scenes and within the conditions of massive accidents, *NBP Žurnal za kriminalistiku i pravo,* Beograd, Kriminalističko-policijska akademija, vol. 14 (2), 185-202.

Žarković, M., Bjelovuk, I., Kesić, T. (2012). Kriminalističko postupanje na mestu događaja i kredibilitet naučnih dokaza. Beograd: Kriminalističko-policijska akademija.

Lipovac, K., Vujanić, M., Obradović, D., Nešić, M. (2018). Uviđaj saobraćajnih nezgoda za javne tužioce i saobraćajnu policiju. Beograd: Pravosdna akademija. Beograd: Glosarijum.

Lipovac, K., Bjelovuk, I., Nešić, M. Primena savremenih uređaja i opreme u forenzičkoj obradi mesta događaja, *Pravo i forenzika u kriminalistici* (Zbornik radova sa istoimenog Prvog naučnog skupa sa međunarodnim učešćem, Kragujevac, 15–17. Septembar 2010.), Beograd: Kriminalističko-policijska akademija, 2010, str. 27-38, (urednik: prof. Dr Željko Nikač).

Lipovac, K., Jovanović, D., Nešić, M. (2019). *Osnove bezbednosti saobraćaja.* Beograd: Kriminalističko-policijski univerzitet.

Kesić, T., Bjelovuk, I. Application of thermal imaging cameras in crime detection, Teme – casopis za drustvene nauke – Journal for social sciences, Vol. 48(4), 2019, 997-1011.

Mazeti, M. (2014). *Hirurški precizno*. Beograd: Laguna.

Pravilnik o bespilotnim vazduhoplovima, "Službeni glasnik RS", br. 1/2020.

Sharma, Bhoopesh & Chandra, Geetanjali & Mishra, Ved P. (2019). Comparitive Analysis and Implication of UAV and AI in Forensic Investigations. 824-827. 10.1109/AICAI.2019.8701407.

Yağdereli, E., Gemci, C., Aktaş, A. Z. A study on cyber-security of autonomous and unmanned vehicles. The Journal of Defence Modeling and Simulation: Application, Methodology and Technology Special Issue: Modeling & Simulation for Cyber Security of Autonomous Vehicle Systems.Vol. 12, (4), 2015, 369-381.

Zakon o vazdušnom saobraćaju, "Službeni glasnik RS", br. 73/2010, 57/2011, 93/2012, 45/2015, 66/2015 – drugi zakon, 83/2018 i 9/2020.

Valavanis K.P., Vachtevanos, G.J. Editors (2015). Handbook of Unmanned Aerial Vehicles. Springer Reference Available at https://dh8.kr/workshop/sejong_control/Handbook_of_Unmanned_Aerial_Vehicles.pdf 7th July 2022.

SECRET AS AN OBJECT OF CRIMINAL LAW PROTECTION IN THE REPUBLIC OF SERBIA[1]

Ivana P. Bodrožić, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia[2]

Mladen Milošević, PhD
Faculty of Security Studies, University of Belgrade, Serbia

INTRODUCTION

Taking into account that criminal offences in the national criminal legislation are governed by the provisions of the special part of Criminal Code (CC) and partly by the secondary criminal legislation, as well as that they are classified in various categories based on a group protection object, the authors attempt to determine systematization criteria used for providing criminal law protection of a secret as a defusing defined category, thus indicating potential options for a different theoretical classification. The authors' aim is to analyse the adequacy of the existing positive legal solutions and to suggest potential amendments to the legal frame in this complex but important field.

A secret in the paper is considered both as an object of protection and an object of action, i.e. as a material object upon which a criminal offence is committed. It is not perceived as an object in an ordinary meaning but as the value, i.e. a set of individual rights or as a secret which the legislator defined as a trade, state, official or military secret.

1 This paper has been published as a part of the project that is financed by the Science Fund of the Republic of Serbia, within its program "IDEAS" - Management of New Security Risks - Research and Simulation Development, NEWSIMR&D, #7749151.
2 ivana.bodrozic@kpu.edu.rs

The five types of secrets specified by the legislator of the Republic of Serbia are provided the strongest legal and criminal law protection. However, certain types of secrets are explicitly defined in a different way and their protection is prescribed in various chapters defining criminal offences within the Special part of the Criminal Code.

The basic research question and the purpose of the paper is to establish, define and determine criteria used as the basis for different definitions of secrets presenting a substantive criterion for specifying conducts which should be regarded as criminal acts and their categorization in various groups of criminal offences which are mutually heterogeneous.

DESIGN/METHODS/APPROACH

Beside the introduction and conclusion, the paper has four separate chapters. The first chapter deals with the questions of the general theoretical determination of a secret and its normative definition in the Serbian legislation. The second one reviews a secret as a specific object of protection within various types of criminal offences and a secret as an object of action in five incriminating manifestations. The third chapter offers a standard analysis of the characteristics of the substance of the criminal offence of illegal disclosure of a secret, Art. 141 of the CC from the category of criminal offences against the rights and freedoms of man and citizen, while the fourth one surveys a normative analysis of the criminal offences which are provided protection by other manifestations of a secret, such as: disclosure of a trade secret, Art. 240 of the CC from the group of criminal offences against the economy; disclosure of a state secret, Art. 316 of the CC from the group of criminal offences against the constitutional order and security of Serbia; disclosure of an official secret, Art. 369 of the CC from the group of criminal offences against official duty and disclosure of a military secret, Art. 415 of the CC from the group of criminal offences against the Army of Serbia. Special attention has been paid to a criminal offence provided for by Art. 98 of the Data Secrecy Law and its relation with the incriminations from Art. 316, 369 and 415 of the CC.

The authors start their analysis from the standard normative method since the subject of the research is a legal text, i.e. five separate norms providing criminal law protection of the individual secret and the secrets protecting economic or public interest (trade, state, official and military, i.e. secret data).

In addition to the normative method, standard methods of formal logic, induction and deduction, as well as analysis and synthesis have been used in the paper.

THEORETICAL AND NORMATIVE DETERMINATION OF A SECRET IN SERBIAN LEGISLATION

"He who keeps his secrets to himself remains his own master forever" the words of Omar Ibn Al- Khattab (Mislilo – knjiga misli hiljadu mudraca, 1993:787) unequivocally contains the motive of the source and secret keeping. A fundamental requirement for keeping a secret arises from everyone's right to freedom – freedom that the data and information somebody possesses may be obtained freely, without any restraints and that they are employed solely for the purpose they are meant for, meaning that the user, holder of the secret, may use everything that secret contains. On the other hand, La Bruyère's quote "When a secret is revealed, it is the fault of the man who confided it" (Mislilo – knjiga misli hiljadu mudraca, 1993:787) indicates its other dimension – disclosure. If a secret, comprehended solely in its linguistic sense of the word, is determined as "a fact known to a tight circle of people who have justified general or individual interest not to spread it" (Bodrožić, 2019:228), is not kept adequately, it loses its fundamental meaning and becomes its opposite; it becomes a datum, just a piece of information which may be misused against persons and the society who were its legal and legitimate "holders".

The issue of determination of a secret and the system of its keeping in a modern democratic society depends on the method of its basic categorization and determines implications of its disclosure.

According to the literature, a secret may be either private or public. A private secret is the result of a close relation and the relation of confidentiality among people (Peran et al., 2015:127), while a public secret has a broader sense involving data which state bodies or legal authorized persons, as well as natural persons who have access to the mentioned data are obliged to keep secret under certain circumstances and it may be classified as a trade, state, official or military secret (Bodrožić, 2019:228).

We are of the opinion that secrets should be classified according to two important criteria: a) interest which is protected by keeping a secret and b) individual, group or collective values which are the subject of protection. Taking these two criteria into consideration, secrets may be divided into: 1. secrets protecting interests in the field of national security (secret data); 2. secrets protecting interests in the field of corporative security (a trade secret), and 3. secrets protecting interests in the field of individual security (an official or personal secret).

Strictly legally speaking, secret has its material and normative dimension. The material dimension implies that a datum or a piece of information comprising a secret is known only to a certain person or a group of people, while the normative dimension of a secret concurrently denotes the fact that the secret is known only

to a certain group of persons, as well as the existence of norms protecting it and proscribing its disclosure.

The normative determination of a secret represents both a foundation and limit line for prescribing mechanisms for its protection. The categorization and definition of secrets in the Republic of Serbia are regulated by the Data Secrecy Law, the Law on Personal Data Protection, the Law on Protection of Trade Secret and the Criminal Code.

The Law on Protection of Trade Secret and the CC explicitly define the concept of a trade secret, while the CC also defines the concept of a state, official and military secret. The Data Secrecy Law has particular importance because it systematically regulates the field of information protection which is of interest to the Republic of Serbia and it revokes the former classification of secrets as official, military and state, introducing as a substitute the concept of secret data which is further ranked with adequate secrecy levels (internal, confidential, strictly confidential and a state secret). Although the concept of a personal secret is not explicitly defined by the CC, it relies on other normative by-laws which regulate the labour of certain professions (primarily the work of lawyers and medical staff) and therefore they are labelled as official secrets. Here, the criminal offence of unlawful secret disclosure regulated by Art. 141 of the CC stands out. Furthermore, we may refer to the incriminations protecting constitutional right to privacy since they both directly and indirectly protect a personal secret as well. The following criminal offences may be classified here (adequate articles of the CC are cited in the brackets): unauthorized disclosure of a secret (Art. 141); stalking (Art. 138a, paragraph 1, item 3); violation of privacy of a letter and other mail (Art. 142); unauthorized wiretapping and recording (Art. 143); unauthorized photographing (Art. 144) and unauthorized publication and presentation of another's texts, portraits and recordings (Art. 145); unauthorized collection of personal data (Art. 146); as well as dissemination of information on personal and family life (Art. 172) (Milošević, 2021a:115). Nevertheless, taking into account that the criminal law protection of the right to privacy may justifiably be studied separately from the subject of our paper, we shall not deal with it in detail here. Excluding all of the above mentioned, we shall focus only on the incrimination determining a secret as an indirect object of protection (Art. 141 of the CC).

According to Art. 2 of the Data Secrecy Law "classified information shall mean any information of interest to the Republic of Serbia, which has been classified and for which a level of secrecy has been determined by law, other regulations or decisions of a competent authority passed under law" (Data Secrecy Law, Official Gazette of the Republic of Serbia, no. 104/09).

The purpose of this regulation as stated by Art. 2 of the Data Secrecy Law is to protect fundamental rights and freedoms of natural persons, especially their right

to the personal data protection, while its application is connected to processing of personal data entirely or partially, both as automated and non-automated processing of personal data, which are part of a data collection or are intended for the data collection. The syntagma "personal data" as to Art. 4 of this law is defined as any information regarding a natural person whose identity is determined or determinable directly or indirectly, especially on the basis of the identification labels (e.g. the name and unique personal identification number), information on location, identifier in electronic communications networks either of one or more features of his/her physical, physiological, genetic, mental, economic, cultural and social identity, while the concept of "personal information processing" implies any operation or set of operations which are performed in an automated or non-automated way in connection with the personal data or their collection, such as collecting, recording, classifying, organizing i.e. structuring, storing, adapting or modifying, disclosing, granting access, using, disclosing through transmission, i.e. delivering, copying, disseminating or rendering the data accessible in any other way, comparison, restriction, deletion or destruction (Law on Personal Data Protection, Official Gazette of the Republic of Serbia, no. 87/2018).

The Law on Protection of Trade Secret governs the legal protection of a trade secret against unlawful acquisition, use and disclosure. The law entered into force in 2021 - superseding the law with the same name, which had been in effect for ten years but which had regulated the protection of trade secret in a different way - and as such it represents the legal foundation directly regulating the concept, civil-law, corporate offence and misdemeanour protection of a trade secret, while criminal-law protection of such a secret is regulated by the CC provisions. As to Art. 2 of the Law on Protection of Trade Secret, information considered a trade secret 1) represents a secret because it is not in whole or in terms of the structure and set of its components generally known or easily accessible to persons who in their activities usually come into contact with this type of information, 2) has commercial value because it represents a secret, 3) a person legally controlling it has undertaken reasonable measures in order to preserve its confidentiality (Law on Protection of Trade Secret, Official Gazette of the Republic of Serbia, no. 53/2021).

SECRET AS A SPECIFIC OBJECT OF PROTECTION WITHIN VARIOUS GROUPS OF CRIMINAL OFFENCES AND SECRET AS AN OBJECT OF ACTION

The concept of a secret is comprehended in a defusing way and as such it is protected, and its protection as a direct object of protection is regulated in five incriminations in the CC. They are all grouped in different criminal offences according

to the prevalence of interests which are to be realized by their protection. Protection of a personal secret is typically associated with concurrent protection of a trade secret which has been unlawfully disclosed by a person, thus committing a criminal offence against fundamental rights and freedoms of man or citizen. The subject of our analysis is the criminal offence regulated by Art. 141 - unlawful disclosure of a secret. Other criminal offences protecting the right to privacy and thus indirectly a personal secret as well, should not be overlooked either. However, as we have already mentioned, we have chosen to focus on this incrimination because of terminological reasons as the only one among others directly regulating a personal secret as an object of action.

Secrets protecting the interests of the state, i.e. national security, are governed by different chapters of the CC dedicated to the following objects of protection: constitutional order and security, official duty and army.

Secrets protecting corporative security, i.e. interests of business entities (legal entities and natural persons dealing with economic activities) are termed as trade secrets. Socially dangerous conducts in the field of protection of trade secrets are incriminated by the criminal offence in Art. 240 of the CC headed as Disclosing of a Business Secret. This criminal offence is to be found in chapter 22 of the CC dedicated to criminal offences against economic interests.

All mentioned manifestations of a secret in the sense of a criminal offence also represent an object of protection differentiated within a group object of protection as a specific value whose endangerment or violation indirectly compromise and infringe its abstract value. They simultaneously have the function of an object of action, i.e. of the value upon which a criminal offence is committed and which are defined as disclosure and revelation.

CRIMINAL LAW PROTECTION OF A PERSONAL SECRET – UNAUTHORIZED DISCLOSURE OF SECRET, ART. 141 OF CC

The criminal offence of unauthorized disclosure of a secret is stipulated by Art. 141 of the CC under a group of criminal offences against the rights and freedoms of man and citizen. It consists of a basic form provided for in the first paragraph and a special paragraph stipulating a specific basis for exclusion of illegality.

The article deals with a specific criminal offence *delicta propria* since a perpetrator may be a person practicing precisely defined professions. He/she may be a lawyer, physician or any other person who in an unauthorized way discloses a secret learned while performing his/her professional duty. The article specifies two professions that offenders may practice, while other perpetrators may also be persons

who because of the nature of their job have opportunity to find out personal secrets of other people and disclose them. These professions include clerics, pharmacists, midwives, nurses and trainee lawyers since personal secrets of people with whom they deal with during performance of their duties may come to their knowledge.

A good example is the Opinion of the Ministry of Labour, Employment, Veteran and Social Affairs stating that "it is unethical and unprofessional practice of the employees in the social welfare centers to pass on information about children and their parents so as to avoid professional procedure, thus giving priority to certain persons who want to adopt children in accordance with their expectations. Furthermore, disclosure of the data from official records is the violation of legal obligation of keeping official secret (Art. 323 and Art. 331 of the Family Law) resulting in criminal liability as to Art. 369 of the CC. All other people, as well as lawyers and physicians, who disclose information about a child for whom there is assumption that it may be adopted and which they have learned during the performance of their professional duty shall be held accountable (Art. 141 of the CC). (Opinion of the Ministry of Labour, Employment, Veteran and Social Affairs 110-00-00681/2007-14, 17th July 2007).

This offence is defined as the disclosure of a personal secret of an individual. The concept of disclosure implies revealing or granting access to a secret, i.e. the data unknown to him/her which are "an official secret the perpetrator was obliged to keep confidential on the basis of regulations and a professional code" (Stojanović, 2020: 528).

As a personal secret is not explicitly defined under Art. 141, it should be comprehended as the data on a person, his/her features, medical status, family and other relations with regard to his/her personality and private life (Đorđević, Kolarić, 2020: 52).

An illustrative example of the obligation of keeping an official secret is a lawyer-client privilege specified under Art. 14 of the Code of Professional Ethics implying "everything that a client, or a person given a power of attorney by a client, has confided to his lawyer representing him/her in the case, has learned or obtained in any other way during the preparation, in the course of or after the legal representation in court" (Code of Professional Ethics of Lawyers, Official Gazette of the Republic of Serbia, no. 27/2012 and 159/2020 – decision by the Constitutional Court). Similarly, a medical secret is defined under Art. 23 of the Code of Medical Ethics of the Medical Chamber of Serbia as professional medical secrecy denoting "all information a physician possesses about his/her patient, his/her personal, family and social environment, as well as all information about determining disease, treatment and disease monitoring obtained during performance of professional duty (Code of Medical Ethics of the Medical Chamber of Serbia, Official Gazette of the Republic of Serbia, no. 104/2016).

An offence may be perpetrated by commission, or occasionally by failing to act. Constitutional feature of the body of criminal offence specifies that the disclosure of a secret must be unauthorized. Consequently, there are situations in which the disclosure of secrets is not only admissible but also the obligation of a person who knows such a secret. In case of the medical profession, such situations refer to disclosing information about contagious diseases, mental disorders of a person applying for a job, the birthdate of a child or en exact hour of death. In all the mentioned situations a doctor is obliged to report the information he/she has come into possession.

Beside these cases, paragraph two of the same article stipulates a specific basis for exclusion of illegality implying that the person committing the offence of disclosure of a secret of general interest or the interest of other person defined in paragraph 1 shall not be punished since the disclosure in such cases is more important than keeping information confidential. It involves two cumulatively defined conditions whose simultaneous realization brings about the exclusion of illegality and accordingly of a criminal offence.

Premeditation as a subjective element of an entity results in the sentence of either a fine or imprisonment lasting up to one year. On an abstract level, the principle of proportionality and justice, as well as the utilitarian character of criminal law are the basis of the relatively lenient sentencing policy of the legislator establishing adequate balance between the protection of fundamental rights and freedoms and necessary and justifiable repression (Bodrožić, 2020: 384).

Taking into consideration sentences provided for by the law, these offences are classified as petty crimes for which courts may opt for sentence substitution as a standard in modern European criminal law sentencing policy and consider imposing community sentence instead of short-term imprisonment depending on a particular case and actual circumstances.

Pointing out minor importance of this offence, Art. 153, paragraph 2 cumulatively provides for a number of criminal offences for which a civil suit may be filed.

CRIMINAL LAW PROTECTION OF A SECRET IN NATIONAL AND CORPORATIVE SECURITY – DISCLOSURE OF A STATE, OFFICIAL AND MILITARY SECRET, SECRET INFORMATION AND TRADE SECRET

Criminal law protection of a secret in national and corporative security (secrets protecting state, i.e. national or business interests) is specified in four criminal offences in the CC and one incrimination in the Data Secrecy Law. These include

disclosure of a trade secret, Art. 240 of the CC referring to a group of criminal offences against economy, disclosure of a state secret, Art. 316 of the CC relating to a group of criminal offences against constitutional order and security of Serbia, disclosure of an official secret, Art. 369 of the CC regarding a group of criminal offences against legal duty, disclosure of a military secret, Art. 415 of the CC pertaining to a group of criminal offences against the Army of Serbia and criminal offence stipulated by Art. 98 of the Data Secrecy Law.

The CC provides for a number of criminal offences with a multiple object of protection. There is a great number of incriminations which concurrently include the protection of numerous values. When considering these offences, the legislator must take into account the concept of legitimacy while opting for dominant abstract value as a systemizing criterion. The situation as regards criminal law protection of a secret is less complicated since the legislator in advance prescribes the group in which this offence will be categorized by explicitly defining a particular secret.

The concept of a **trade** secret as to **Art. 240**, paragraph 4 of the CC includes all the data and documents which are declared a trade secret by the law, other regulations or the ruling of a competent authority provided for by the law and whose disclosure would or could result in damaging consequences for the subject of a business (CC, Official Gazette of the Republic of Serbia, no. 85/2005, 88/2005 – amendment, 107/2005 – amendment, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019). Undoubtedly, an object of protection in this criminal offence refers to the right of competition, while a group object of protection relates to businesses, i.e. economy.

The concept of **a state secret** as defined by **Art. 316**, paragraph 5 of the CC includes all the data and documents which are declared a state secret by the law, other regulations or the ruling of a competent authority provided for by the law and whose disclosure would or could result in damaging consequences for the security, defence or political, military and economic interests of Serbia (CC, Official Gazette of the Republic of Serbia, no. 85/2005, 88/2005 – amendment, 107/2005 – amendment, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019). The last part of the definition specifies that the object of protection in this criminal offence refers to the security of Serbia, while a group object of protection relates to the constitutional order (political, military or economic interests) and security of the Republic of Serbia.

The concept of **an official secret** as specified by Art. **369**, paragraph 4 of the CC also includes all the data and documents which are declared an official secret by the law, other regulations or the ruling of a competent authority provided for by the law and whose disclosure would or could result in damaging consequences for the service (CC, Official Gazette of the Republic of Serbia, no. 85/2005, 88/2005

– amendment, 107/2005 – amendment, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019). By putting an emphasis on the service, i.e. official duty as the value that may be endangered by disclosure of a secret, this criminal offence is classified as a classic wrongful act against official duty.

A military secret as to Art. **415**, paragraph 4 of the CC includes all the data and documents which are declared a military secret by the law, other regulations or the ruling of a competent authority provided for by the law and whose disclosure would or could result in damaging consequences for the Army of Serbia or defence and security of the state (CC, Official Gazette of the Republic of Serbia, no. 85/2005, 88/2005 – amendment, 107/2005 – amendment, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019). As already defined in the previous three paragraphs of this paper, since the disclosure of a military secret may pose a detriment or endanger the object of protection, this criminal offence is classified in the group of criminal offences against the Army of Serbia.

The interpretation of the terms used in the CC is mostly in connection with Art. 112 which defines the terms in the Code. Since the mentioned article includes the terms of general character that may be found in a number of provisions of the CC, this article specifies their uniform meaning regardless of the provision in which they are used. As for the definition of the term *a secret* in the provisions of the CC, it must be pointed out that these are only interpretative provisions, characteristic for the use of just one norm. Therefore, bearing in mind the necessity for an easier and more systematic review of the method by which the CC provides for the protection of a secret, their interpretation is given successively, both for easier use and the ensuing comparison.

The chosen nomotechnics used by the legislator to define subtypes of a secret is generally consequent. It represents the extension of the definition "the data and documents stipulated by the law, other regulations or the ruling of a competent authority provided for by the law" declaring a particular subtype of secret whose disclosure would or could cause detrimental consequences for one of the selected objects of protection. Although a uniform definition facilitates the use of this norm in practice and provides technical precision, it should be accompanied by a consequent definition of the other part of the norm which will be discussed in the part of the paper dealing with the analysis of the elements of the entity of four criminal offences protecting secret.[3]

3 Various legislative techniques, i.e. styles characterizing them may be in connection with the comprehension of the norm or its technical precision. Legal reasoning is mostly expressed through linguistics, i.e. used nomotechnical style, which after it has been chosen must (should! A/N) be consequently used throughout the whole text of regulations. Otherwise, it may lead to confusion and diversion from the fundamental nomotechnical and legal-political foundations of the legal text (Bodrožić, 2022:124-125).

DISCLOSURE OF A TRADE SECRET, ART. 240 OF THE CC

Disclosure of a trade secret is incriminated by provisions of Art. 240 of the CC. This criminal offence has one fundamental and two supplement forms (qualified and privileged) and it is, as already mentioned, classified in the chapter dealing with criminal offences against economy. The fundamental form (Art. 240, paragraph 1) consists of two alternative perpetrations. The offence shall be committed if a perpetrator discloses, hands over or in any other manner makes available information declared a business secret or otherwise obtains such information with the intention of handing it over to an unauthorized person. Premeditation represents a subjective element, while the other alternative perpetration requires the determination of a specific norm. The maximum penalty for this form of disclosure of a trade secret is imprisonment of six months to five years.

Paragraph 5 of this article offers a criminal law definition of a trade secret. Taking into account that its content has instructing character, it should be interpreted in accordance with the provisions of the special code which deals with the subject of secret protection in the Law on Protection of Trade Secret (Milošević, 2021: 57; Mandić et al., 2017: 302).

The literature emphasizes that the scope of criminal law provision is not sufficiently comprehensive (Milošević, 2021: 60). The Law on Protection of Trade Secret, whose content is inspired by the EU Directives on the Protection of Trade Secrets (Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Official Journal of the European Union, no. 157/1) introduces civil law and criminal law (corporate crime and misdemeanour) liability for unauthorized disclosure, acquisition and use of confidential trade secrets. However, the analysed provision of the CC incriminates only unauthorized disclosure of secrets and excludes acquisition and use by an unauthorized person. The court practice, which is otherwise rather lacking with regard to this criminal offence, supports this position as in the Ruling of the Basic Court in Niš, K 65/14 of 23 April 2014 (Milošević, 2022: 134).

Additionally, the fact that the Law on Protection of Trade Secret introduces criminal law sanctions for unauthorized disclosure, use and acquisition of trade secrets may cause problems regarding the enforcement of the law, i.e. a conflict between criminal law and misdemeanour (i.e. corporate crime) provisions in the light of criminal procedural principle *ne bis in idem* (Milošević, 2021: 63). In fact, unauthorized disclosure is sanctioned by criminal law, misdemeanour and corporate crime provisions, while unauthorized acquisition and use are exclusively the subject of misdemeanour and corporate crime law, which is not logic and sustainable legal solution. Evidently, all three forms of unauthorized acts are the basis for civil

law liability (as well as labour law liability if all conditions are fulfilled); nonetheless, these forms of liability are neither mutually competitive nor they exclude the enforcement of penal sanctions.

The qualified form of the offence, for which the maximum penalty is imprisonment of two to ten years including a fine, is committed if it was perpetrated with an intent – if it is motivated by greed or if the disclosed data were exceptionally confidential. Greed represents the motive for unlawful material benefit (Delić, 2021; Vuković, 2021), while exceptionally confidential data are defined as "those whose disclosure could inflict considerable damage to the holder of a trade secret" (Milošević, 2022: 134). "Nevertheless, with the purpose of reaching conclusion that a certain datum of a trade secret was particularly confidential when compared to others, it is necessary for the holder of that secret to declare it as the secret of higher confidentiality and to take stricter measures than the ones used for the protection of other data of that trade secret" (Milošević, 2022: 134; Mandić et al., 2017: 303).

A less serious form of the disclosure of a trade secret is committed when the objective elements of the basic form are perpetrated negligently. The prescribed penalty is up to three years of imprisonment. "A negligent form is committed when e.g. an employee does not keep to the recommended company procedures and protection standards, taking it for granted that the data will not fall into the hands of an unauthorized person or that he will be able to prevent the disclosure to an unauthorized person. The same thing will happen in the case when the perpetrator does not expect or is not aware that his conduct may cause the violation of a trade secret although he/she is obliged or could foresee it on the basis of his/her personal features and circumstances. An illustrative example is the situation in which the perpetrator leaves recorded parameters for electronic access to the data on his/her office desk (unprotected from unauthorized persons) without considering that someone could take advantage of them" (Milošević, 2022: 135).

DISCLOSURE OF A STATE SECRET, ART. 316 OF THE CC

The criminal offence of disclosing a state secret is provided for by Art. 316 of the CC of the chapter 28: "Criminal offences against the constitutional order and security of the Republic of Serbia" (Milošević, 2010). Confidential data, which are defined and ranked in accordance with the existing regulations, are protected by this incrimination. As already emphasized, the basic law regulating the confidentiality of data is the Data Secrecy Law. However, the fact that this law comprises a criminal law provision arises questions and dilemmas in practice (Kovačević, Milošević, 2022). "Consequently, both the criminal offence of disclosure of secret data provided for by the Data Secrecy Law and "old" criminal offences (disclosure

of a state secret, disclosure of an official secret and disclosure of a military secret) stipulated by the CC are contemporarily in force. The criminal offence defined by Art. 98 of the CC refers to the disclosure of secret data which are ranked through the provisions of that law (chiefly, all confidential data originating upon its enactment in 2009), while the criminal offences from the CC refer to the disclosure of the data defined by previous provisions, i.e. provided for before the Data Secrecy Law came into effect" (Milošević, 2022: 215). Hence, we shall firstly present three criminal offences from the CC, then discuss their relation with the incrimination from Art. 98 of the Data Secrecy Law.

The basic form of the offence defined by Art. 316 of the CC is committed when the perpetrator discloses, hands over or in any other way makes available to an unauthorized person information or documents that are entrusted to him/her or that he/she acquired otherwise. In this case premeditation is the subjective element.

The disclosure of a state secret, as opposed to espionage, does not include a foreign element (Stojanović, 2018; Đorđević, 2014; Delić, 2021; Milošević, 2022). Espionage therefore presents incrimination protecting secrecy of data, but it requires additional elements that make it sufficiently specific for not being a separate subject of this paper. Prescribed penalty for the basic form of the disclosure of a state secret is from one to ten years of imprisonment. The legal definition of a state secret is specified by paragraph 5, while paragraph 6 defines which data and documents cannot be declared a state secret.

Art. 316 comprises paragraph 2 defining one of the privileged forms of the criminal offence for which the prescribed penalty is from six months to five years of imprisonment. This form of the offence is committed when a perpetrator reveals the data that he/she unlawfully obtained to an unauthorized person. It incriminates the perpetration of a person who is not a lawful holder of a secret but who obtains it unlawfully and then hands it over, discloses or makes available to another unauthorized person. The same penalty is prescribed for the form from paragraph 4 (which is also lenient). This form is committed when a state secret is disclosed negligently (Kovačević, Milošević, 2022: 100).

Nonetheless, it should be mentioned that "it is still not clear why the legislator fails to incriminate unlawful acquisition of the ranked documents by an unauthorized person regardless of the fact whether the secret has been handed over or not" (Kovačević, Milošević, 2022: 101).

Art. 316, paragraph 3 defines the qualified form for which the penalty of three to fifteen years of imprisonment is provided for. The legislator specifies two alternative qualifying circumstances: the first referring to the offence committed during the state of war or emergency state, the second one in case the security, economy or armed forces of the state are endangered.

DISCLOSURE OF AN OFFICIAL SECRET, ART. 369 OF THE CC

The offence under Art. 369 of the CC is formulated similarly to the offence under Art. 240, although with some differences arising from the nature of these incriminations. The basic form may be committed solely by officials who unlawfully disclose, hand over or in any other way make available the data representing an official secret, or gather such information in order to hand it over to an unauthorized person. The prescribed penalty is from six months to five years of imprisonment - the same as for the basic form of the disclosure of a trade secret. Oddly, the legislator evaluates the level of abstract social jeopardy of these two offences as equal although the offence under Art. 240 protects the interests of business entities, while the incrimination under Art. 369 protects official, i.e. public interests.

Analogously to the adequate provisions in Art. 316, the legislator defines the concept of an official secret and the so called unlawful official secret in paragraphs 5 and 6. As these provisions are also of indicating character, other regulations should be consulted for their comprehension, primarily the Data Secrecy Law and other laws that had been in force before it came into effect.

Even the basic form of disclosing an official secret, more precisely its other alternative commission, the act which is by its nature a preparatory action, is equalled to a completed action indicating in that way the importance of early criminal justice response and prevention of these acts by which the confidentiality of the data in national security is breached. It is interesting that paragraph 6 of Art. 369 specifies explicitly that an offence may be committed by an official after his position of an official has ceased. This solution is logical because an official is still acquainted with the secret data after his official position has ceased. Therefore, it is of vital importance to secure criminal justice protection in such a case.

The legislator provides for a serious form of this offence: "If the offence specified in paragraph 1 of this Article is committed for gain or in respect of particularly confidential information or for publishing or use abroad, the offender shall be punished by imprisonment of one to eight years" (Art. 369, paragraph 2 of the CC). This offence differs from the serious form of the disclosure of a trade secret by one qualifying circumstance - the foreign element. It seems that this circumstance is not classified as a feature of the qualifying form of the offence of the disclosure of a trade secret due to the omission by the legislator (Milošević, 2021; Milošević, 2022). The legislator stipulates the punishment of one to eight years of imprisonment for this form of offence, while a more severe sentence is prescribed for a serious form of the disclosure of a trade secret. It is difficult to find the excuse for such a solution provided for by the legislator since it is neither logic nor legitimate from the criminal law policy point of view.

Eventually, the specified sentence for negligent disclosure is up to three years of imprisonment, the same as for the adequate form of the disclosure of a trade secret. It is interesting that unlike the offence of disclosing a state secret, the law does not provide for a form of the offence relating to unauthorized use of secret. We consider this to be the omission by the legislator (Kovačević, Milošević, 2022: 103).

DISCLOSURE OF A MILITARY SECRET, ART. 415 OF THE CC

Article 415 of the CC incriminates the disclosure of a military secret. The basic form is characterized by almost the same features as for the criminal offence specified in Art. 369 although the perpetrator is not defined as "an official" but as "a person who unlawfully communicates…". The prescribed sentence is from six months to five years of imprisonment (once again exactly the same as for the disclosure of a trade secret, which we consider to be a rather unusual solution).

Although it is not explicitly specified that the perpetrator may be solely an army officer or an official employed in the Army of Serbia, i.e. the competent Ministry of Defence, it is clear that a military secret may be disclosed only by a person in lawful possession of such a document or information. Beside an army officer or official (e.g. a civilian dealing with official duties in the Ministry of Defence), this offence may be committed by any other person who is entrusted with such a document or information (e.g. an employee dealing with technical and other professional duties, a courier, an official of another body of public authority, an authorized person in a legal entity discharging public authorities functions or a person employed with a company dealing with legal obligations in the field of defence, i.e. developing a defence plan, etc.).

Paragraphs 2 and 3 of this article are formulated in exactly the same way as the criminal offences of the disclosure of a state secret although there are certain differences relating to the object of action (a military instead of an official secret). Even the range of prescribed sanctions is the same. Here the attention should be paid to the fact that if judged by the prescribed sentences, the legislator estimates the abstract social value of the disclosure of a trade secret in a qualified form as greater value compared to a serious form of the disclosure of a military secret (?!). Additionally, we want to emphasize that the punishment for unlawful use of a military secret is not provided for in this criminal offence (Kovačević, Milošević, 2022: 103).

As in the case of disclosing an official secret, paragraphs 5 and 6 define the concept of a military secret specifying data and documents which are not to be deemed a military secret.

THE RELATION BETWEEN THE OFFENCES PROVIDED FOR BY ART. 98 OF THE DATA SECRECY LAW AND CORRESPONDING INCRIMINATIONS IN THE CC

The provision of Art. 98 of the Data Secrecy Law provides for the criminal offence of the disclosure of secret data, as we shall term it freely, considering the fact that it does not have a legal name (Kovačević, Milošević, 2022:98). This offence has its basic, qualified and privileged forms. Objective and subjective elements are essentially identical as in the already analysed criminal offences except for an important difference with regard to the object of action. The basic form occurs if the object of action (secret data) is labelled with levels of confidentiality "internal" and "classified"; a serious form involves the data categorized as "strictly confidential", while a more serious form is labelled as "a state secret". The most serious form exists when one of the following qualifying circumstances occurs: the offence is committed during either the state of war or emergency, for obtaining unlawful gain or for the use abroad. The stipulated sentence depends on the fact whether the perpetrator has committed the offence defined in paragraphs 1, 2 and 3 involving adequate qualifying circumstance. The legislator provides for the criminal offence of disclosing secret data committed from negligence.

The fundamental question arising here is how to determine when to implement Art. 98 of the Data Secrecy Law and when the articles 369 or 415 of the CC. The answer is clear: "[…] Art. 105, paragraph 1 of the Data Secrecy Law explicitly defines that the data and documents assigned a classification level based on earlier regulations shall keep the type and level of classification assigned under such regulations (Art. 105, paragraph 2 of the Data Secrecy Law). The intention of the legislator to reconsider all former secrecy labels (Art. 105, paragraph 2 of the Data Secrecy Law) could not easily be implemented in practice because of the expected extent and number of labelled data and documents" (Kovačević, Milošević, 2022: 102). Therefore, the data labelled according to the formerly existing regulations that have not been revised, i.e. revoked or otherwise labelled according to the regulations of the Data Secrecy Law will be treated compliant with the corresponding provisions of the CC, while the secret data labelled in accordance with the provisions of the Data Secrecy Law shall be sanctioned by its prescribed sentences.

However, the attention should be paid to another important legal inconsistency. Namely, the qualifying circumstance - the commission of the offence during the state of war or emergency is provided for by Art. 316, paragraph 3. However, the same circumstance is stipulated by Art. 321, paragraph 3 of the CC, as well as Art. 98, paragraph 4 of the Data Secrecy Law. Yet, different sanctions are prescribed in all three cases (Art. 316, paragraph 3 of the CC stipulates from three to fifteen years of imprisonment; Art. 321, paragraph 3 of the CC prescribes a specified

minimum of ten years or life imprisonment; Art. 98, paragraph 4 of the Data Secrecy Law prescribes the punishment of five to fifteen years of imprisonment). This discrepancy and contradiction should be eliminated by legal intervention (Milošević, 2010; Milošević, 2021; Kovačević, Milošević, 2022).

CONCLUSION

As the subject of this paper belongs to the field of the special part of criminal law and consists of a classic analysis of the entity elements of the selected criminal offences, its significance is viewed in the systematization of the knowledge about criminal law protection of secret and offering suggestions for introducing new theoretical classification criteria. The authors have not dealt with all criminal offences which are ensured secrecy protection but only with those considering secret as a separate object of protection or direct object of action. This implies the authenticity of the subject, as well as contribution of the research question which served as a starting point. The incriminations providing for a secret as an object of protection both in the CC and the Data Secrecy Law have been singled out; the distinction among the types of secrets has been noticed; new criteria for their classification as per which secrets should be categorized into three types depending on the context they originate from and the interests protected by keeping data confidential has been suggested. Accordingly, secrets have been classified as: 1. secrets introduced for the protection of personal interests, i.e. privacy of individuals (a secret protecting personal security); 2. secrets introduced for the protection of the interests of business entities (a secret protecting corporative security), and 3. secrets introduced for the protection of national, i.e. state interests (a secret protecting national security). This type of a selected legislative technique is considered useful, although the legal interpretation is not overvalued since the field of the norm enforcement facilitates its comprehension and provides a broader protection range.

The paper emphasizes the peculiarities of the nomotechnical approach which makes difference between the protection of a personal secret and the secrets protecting business or national interests. Next, the paper draws attention to the subsidiarity of criminal law regulations in the cases of their relation with *lex posterior* and *lex specialis* norms of the Law on Personal Data Protection, the Data Secrecy Law and the Law on Protection of Trade Secret within the definition of the concept of public secret.

Scientific contribution is manifested through the originality of the systemizing criterion used for the selection of incriminations, systematization of the knowledge about criminal offences involving a secret as a direct object of protection and an object of action, then the analysis of the peculiarities of distinguished interpretative norms, as well as their partial inconsistencies. The authors have definitely estab-

lished that the provisions of the criminal law of the Republic of Serbia provide for a relatively adequate level of legal protection characterized by *ultima ratio societetis*, and that efficient protection system, which should primarily serve as prevention and only in rare cases as repression in the fields analysed in this paper, can be realized by consecutive use and enforcement of other regulations from this field.

However, the noted inconsistencies, discrepancies and non-compliance of certain legal solutions should be corrected by legislative intervention. The authors emphasize the need for different regulation of certain issues and offer clear, theoretically credible and practical suggestions as regards the solutions for the matter in question.

REFERENCES

Bodrožić, A. (2019). Secret as an assumption of political power. *Teme* 1, 225-241.

Bodrožić, I. (2022). *Terorizam kao kategorija nacionalnog i međunarodnog krivičnog prava.* Beograd. Kriminalističko-policijski univerzitet.

Bodrožić, I. (2020). Kontinuirani krivičnopravni ekspanzionizam - na raskršću politike i prava. *Srpska politička misao*, 2, 381/396.

Delić, N. (2021). *Krivično pravo – posebni deo.* Beograd. Pravni fakultet Univerziteta u Beogradu.

Đorđević, Đ, Kolarić, D. (2020). *Krivično pravo-posebni deo.* Beograd. Kriminalističko-policijski univerzitet.

Đorđević, Đ. (2014). *Krivično pravo – posebni deo,* 3. izdanje. Beograd. Kriminalističko-policijska akademija.

Kodeks medicinske etike Lekarske komore Srbije, Sl. glasnik RS, br. 104/2016.

Kodeks profesionlane etike advokata, Sl. glasnik RS, br. 27/2012 i 159/2020 - odluka US.

Kovačević, N., Milošević, M. (2022). Zaštita tajnih podataka u digitalnoj formi – bezbednosni i krivičnopravni aspekti. Bezbednost, 1, 93 – 108. doi: 10.5937/bezbednost2201093K

Mislilo-knjiga misli hiljadu mudraca. (1993). Beograd. Alfa. Sezam.

Mandić, G., Putnik, N., Milošević, M. (2017). *Zaštita podataka i socijalni inženjering - pravni, organizacioni i bezbednosni aspekti.* Beograd. Univerzitet u Beogradu-Fakultet bezbednosti. ISBN 978-86-80144-14-6, COBISS.SR-ID 247160076.

Milošević, M. (2010). Krivična dela protiv ustavnog uređenja i bezbednosti Republike Srbije-istorijski i pozitivnopravni prikaz, u: Cvetković, V. (urednik),

Rizik, moć i zaštita-uvođenje u nauke bezbednosti. Beograd, Službeni glasnik i Univerzitet u Beogradu-Fakultet bezbednosti. 414-452.

Milošević, M. (2021). The Role of Criminal Law in Trade Secret Protection. "*Archibald Reiss Days", 11th Thematic Conference Proceedings of International Significance*, Belgrade. University of Criminal Investigation and Police Studies, 53-63.

Milošević, M. (2021a). Krivičnopravna zaštita podataka o ličnosti. Revija za kriminologiju i krivično pravo, 2, 113-130.

Milošević, M. (2022). *Krivično pravo – posebni deo: izabrane inkriminacije za studije nauka bezbednosti.* Beograd. Univerzitet u Beogradu - Fakultet bezbednosti.

Mišljenje Ministarstva rada i socijalne politike, broj 110-00-00681/2007-14, od 17.07.2007. godine.

Peran, B., Goreta, M., Vukošić, K. (2015). Pojam i vrste tajni. *Zbornik radova Veleučilišta u Šibeniku,* 3-4, 127-135.

Presuda Osnovnog suda u Nišu K 65/14, od 23.04.2014. godine.

Stojanović, Z. (2020). Komentar Krivičnog zakonika. Beograd. Službeni glasnik.

Vuković, I. (2021). Krivično pravo – opšti deo. Beograd. Pravni fakultet Univerziteta u Beogradu.

Zakon o zaštiti podataka o ličnosti, Sl. glasnik RS, br. 87/2018.

Zakon o tajnosti podataka, Sl. glasnik RS, br 104/2009.

Zakon o zaštiti poslovne tajne, Sl. glasnik RS, br. 53/2021.

CHARACTERISTICS OF ENVIRONMENTAL CRIMES AS CHALLENGES FOR THEIR DETECTION AND PROVING

Ivana Marković, PhD[1]
Faculty of Law, University of Belgrade, Serbia

INTRODUCTION

The recognition of the environment as an object of protection by criminal law happened simultaneously with the development of the environmental consciousness and the new concept of sustainability, as an answer to the consequences of unsustainable practices that have led to serious pollution of the nature (Banić 2021: 65, 66). It should be undisputable by now that the nature and its media - water, air and soil, as well as her emanations in the form of flora and fauna are part of the elementary conditions of life of humankind and as such clearly fall into the circle of legal goods that are to be protected by means of criminal law (Schall 2014: 819).

Furthermore, it is also a highly lucrative activity, where the risks are low and the profits are high (Bachmaier 2016: 195). Environmental crime is the third most lucrative category of crime globally, with costs of up to 246 billion EUR annually.[2] The drivers of environmental crimes are obviously economic, and so are the financial and human costs of this type of crimes enormous, if indeterminable (Shover & Routher 2005: 322).

Already in 1989 - still the initial phase of the emerging environmental law, the importance of environmental crimes has been recognized: „The cumulative effects of pollution are more dangerous and their repercussions more long-lasting and pro-

1 ivana.markovic@ius.bg.ac.rs
2 WWF, Position Paper, March 1, 2022, 1. https://www.wwf.eu/?6109916/A-new-EU-Environmental-Crime-Directive, last accessed on July 5, 2022.

found than any crime yet cared by a judicial system" (Milne 1989: 333). They can victimize entire nations or populations (Shover & Routhe 2005: 324); and they do not stop at national borders, having an organized (Bugarski 2015: 1100 – 1102) and transnational dimension of the crime (Elliott 2012: 89 – 95; Pisarić 2011: 425 - 439).

However, judicial statistics show that environmental crimes are not prosecuted as often as traditional crimes (Uhlmann 2009: 1243; Burns & Lynch 2004: 105), despite the importance of the protected legal good, its ubiquity and long-term consequences that can victimize more people than the majority of the other offences.

STATISTICAL OVERVIEW

To gain an overview of the practical situation regarding environmental crimes, Serbia[3] has been chosen as an example. The following parametres have been selected: 1) reported adult perpetrators by criminal offences[4] in the ten-year-period (2011 – 2020);[5] 2) reported adult perpetrators by criminal offence and type of decision for 2020 (newest available data); 3) accused adult perpetrators, by criminal offence and type of decision for 2020; and 4) convicted adult perpetrators, differentiation within the group of crimes against the environment, for 2020. The aim is to shed light on the statistical path of environmental crimes in the stages report – accusation – conviction. Regarding the types of decisions that are shown in the second and third table, their selection was based on their link to the detection and proving of these crimes.

In this statistical display, crimes that are in relative connection to environmental crimes have been selected; either because they are committed in similar ways, or because the consequences of the crimes are close. Here, we can observe a low number of reported environmental crimes, despite their high frequency of occurrence in practice. Only criminal offences against the public safety or persons and property have been reported less. For other groups of crimes that have been left outside of this display (offences against the security of computer data; offences against constitutional order and security; offences against humanity and other assets protected by international humanitarian law; offences against the Army of Serbia), their even lesser percentage is attributed to their extraordinary character or also to lack of criminal enforcement (for computer crimes).

3 For an overview of Substantial Criminal Law in Serbia see Marković (2017: 885 – 908).

4 Chapter XXIV of criminal offences against the environment from the Serbian Criminal Code.

5 This time frame has been chosen due to the fact that it is the newest period for which complete data is available. Incomplete, outdated information and data that is not harmonized (Faure 2006: 17, 18) are further obstacles for combatting environmental crimes.

Table 1. Reported adult perpetrators, by criminal offences, 2011-2020

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
In total	**88.207**	**92.879**	**91.411**	**92.600**	**108.759**	**96.237**	**90.348**	**92.874**	**92.797**	**74.394**
Criminal offences against life and limb	3.908	3.923	3.734	3.268	3.818	3.451	3.278	3.084	3.064	2.481
Criminal offences against civil freedom and rights	2.470	2.676	2.850	2.975	3.874	4.046	4.052	4.264	4.390	3.643
Criminal offences against property	39.742	45.291	45.899	50.303	58.741	44.000	40.443	40.595	38.713	29.788
Criminal offences against the economy	2.957	3.221	3.397	3.347	3.526	3.333	2.939	2.767	2.461	1.814
Criminal offences against human health	3.409	3.603	3.464	3.161	3.731	3.687	4.574	5.546	6.693	7.329
Criminal offences against the environment	1.789	1.841	1.996	2.148	2.205	2.507	2.187	2.550	2.425	2.153
Criminal offences against the public safety of persons and property	1.128	1.305	1.210	1.264	1.284	1.220	1.135	1.285	1.291	1.010

Source: Statistical Office of the Republic of Serbia

Compared to the total numbers of all crimes reported in the 10 year period, crimes against the environment circle around 2% (in 2011: 2, 07%, 2015: 2, 03%), with a slight increase in the last two years observed (2019: 2, 61%, 2020: 2, 89%). However, the percentage remains low.

Table 2. Reported adult perpetrators, by criminal offence and type of decision, 2020

	Total	Perpetrators known					Perpetrators unknown
		Perpetrators known, total	Crime report rejected		Investigation suspended		
			The act is not a criminal offence	No reasonable ground for suspicion, prosecutorial inopportuneness	The act is not a criminal offence	No proofs	
Republic of Serbia	74.394	51.863	10.945	1.231	31	198	22.531
Criminal offences against the environment	2.153	1.072	213	15	-	-	1.081

Source: Statistical Office of the Republic of Serbia

In this table of reported adult perpetrators for the year 2020, listed by the type of decision that is relevant in the context of detection and further investigation of the crimes, we can firstly observe a very high number (50.21%) of perpetrators that remain unknown. The average for these types of crimes is higher than for the average of all crimes in Serbia (30.29%). Regarding the rejection of the crime reports, the vast majority is because of the conclusion that the act is not a criminal offence.

Table 3. Accused adult perpetrators, by criminal offence and type of decision, 2020

	Accused persons - total	Proceedings discontinued	Exoneration judgment		
			All	The act is not a criminal offence	No evidence
Republic of Serbia	29.389	1.150	1.330	147	1.183
Criminal offences against the environment	382	18	31	-	31

Source: Statistical Office of the Republic of Serbia

Looking at the next stage, a remarkable difference becomes obvious. While out of the reported overall crimes 39.50% of the cases resulted in accusations, for environmental crimes this number is more than halved (17.74%). It confirms the hypothesis that environmental crimes are not prosecuted as often as traditional crimes (Uhlmann 2009: 1243).

Table 4. Convicted adult perpetrators, differentiation within the group of crimes against the environment, 2020

	Total
Republic of Serbia	**25.487**
Criminal Offences against the environment	**291**
Damaging the environment	3
Destroying, damaging and taking abroad or into Serbia a protected natural asset	3
Bringing dangerous substances into Serbia and unlawful processing, depositing and stockpiling of dangerous substances	3
Killing and abuse of animals	14
Contamination of drinking water and food for animals	1
Devastation of forests	12
Forest theft	240
Illegal poaching	13
Illegal fish poaching	2

Source: Statistical Office of the Republic of Serbia

Even when the enforcement authorities have formally established that a violation has taken place, the case is very often not prosecuted and simply ends with a dismissal (Faure 2016: 17, 18). 8.12% of the accusations resulted in exoneration judgments; compared to 4.53% for the overall crimes – nearly a double value. All 31 exoneration judgments were made because evidence could not be found. This is the first stage where the absence of evidence is seen in the statistics for 2020. In the previous stage (reported crimes), no investigation was suspended because of the absence of proofs.

In the final stage, the number of convictions shows again a flattening. While the ratio of the reports for environmental crimes and overall crime reports was 2.89% in 2020, this ratio decreased to 1.14% for convictions. In other words, only a bit more than 1% of the overall convictions in Serbia in 2020 were convictions for environmental crimes.

Furthermore, if we look at the distribution of convictions within the group of environmental crimes, an even greater imbalance can be seen. Out of the 291 convictions for eco-crimes, 240 of them are for forest theft. This means that 82.47% of the convictions are basically for only one offence. Beside the concrete monetary damage and hence interest for prosecution of the concrete owners of the felled trees, another reason might be the easier detection and proving of the cutting off the trunk and its roots (see Delić 2022: 293, 294).

LEGISLATIVE FORMULATIONS OF ENVIRONMENTAL CRIMES

Apart from the fact that there are many definitions of environmental crimes in general - particularly their complexity,[6] variety[7] and heterogeneity represent challenges for criminal law enforcement. Lazarus has even questioned whether

6 Bachmeier has identified additional, non-normative factors that contribute to rare prosecutions of environmental crimes: their transnational (organized) character; profitability as a corporate crime („and even as a normalized part of manufacturing corporations everyday activities" and the connection to corruption in public institutions, especially in developing countries (Bachmaier, pp. 195, 196). She mentions the study of Brian Wolf, in which empirical data show that the larger the firm the more likely it is to commit environmental violations, although this factor alone is not decisive (Wolf 2009: 127 – 131). For the criminal liability of legal entities and their employees in general see Delić (2011): 289 – 301) and Vuković (2011): 302 – 317.

7 The US Sentencing Guidelines, for example, divide environmental violations into four categories of seriousness: knowing endangerment of human life, violations involving hazardous or toxic substances, those involving other pollutants, and conservation and wildlife offense (Shover & Rote 2005: 351). However, not even this relatively modest number of categories manages to object all the critiques on behalf of the nature of environmental crimes and the arising difficulties for detecting and proving crime.

environmental law[8] and criminal law are sufficiently integrated at all (Uhlmann 2009: 1232). He pointed out the environmental law's complexity as a distinguishing feature that makes it a difficult fit for criminal enforcement and identified the following characteristics: focus on technicality (the scientific underpinnings of environmental law require expertise to master), indeterminacy (the uncertain jurisdictional lines that define what conduct is covered by the environmental laws, and the fact that much of environmental law does not involve prohibitions against pollution, but limits on how much one can lawfully pollute),[9] and obscurity (the volume and density of the various regulatory definitions and concepts) (Lazarus 1995: 2429 – 2438, according to Uhlmann 2009: 1231, 1232).[10]

These features can be found in the Chapter XXIV of criminal offences against the environment from the Serbian Criminal Code (hereinafter: CC)[11] as well. Out of the 18 crimes regulated in the Chapter, for at least 16 of them, either directly from their wording or from practice, the above-mentioned characteristics are valid. Let´s take as an example the first and basic environmental crime from the Chapter – environmental pollution from Article 260 CC. By imprisonment of six months to five years and a fine should be punished „whoever by violating the regulations on protection, preservation and improvement of the environment pollutes air, water or soil to a larger extent or over a wider area" (para. 1). Firstly, regulations on protection, preservation and improvement of the environment have to be identified, known and understood, in order to then be able to recognize their violation. Law enforcers are instructed to search both in administrative or other legal acts (instructive part of the wording) and also to continue to do so in the technical and subject-specific context when it comes to recognizing pollution of air, water or soil. This search continues in the next paragraph, where the negligent form is criminalized (para. 2), so the level of the duty of care has to be established. Ambiguity continues in paragraph 3, where a stricter sentence is stipulated if the offence „results in destruction or damage to animal and plant life to large extent or environmental pollution in such an extent that clean-up requires a longer period of time or a great expense." The elements „large extent", „longer period of time" and „great expense" have to be specified, which cannot be done without the interpretational help of the (with regard to eco-crimes underdeveloped) judicial practice and other legal sources. These elements have to be specified enough to enable criminal investigations. Other examples of notions whose meaning has to be searched for outside criminal legislation are „protected natural asset" or „protected or rigorously protected plant or animal species", or even international

8 On Environmental Law in Serbia see Drenovak-Ivanović (2021).

9 In this regard also Kuhlen (1993: 726).

10 Uhlmann remarks that it is therefore not surprising that environmental crime is cited as an example of overcriminalization (2009: 1229).

11 Criminal Code, *Official Gazette of RS*, nos. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.

treaties and documents, which additionally broaden the scope of legal sources that have to be taken into account (all examples are from Article 265 – Destruction, Transfer into a Foreign Country or into Serbia of Protected Natural Asset) (see Author 2021: 99, 100).

Even seemingly common notions, like waste, can open up space for vague interpretations. The offender could claim that the substance is not waste, but a by-product, and as such not criminally relevant. This vagueness may affect the detection, investigation and proving of the respective case, at the same time using (wasting) already scarce resources (Vagliasindi 2016: 162). Dogmatically speaking, this is problematic with regard to the *lex certa* segment of the principle of legality, and consequently, to the principle of guilt and the possibility to know the criminal provision.[12]

In criminal cases where the meaning of law has to be determined, where detection has to be supported by strong evidence, in the light of the concomitant burden of proof (see Ilić, Majić, Beljanski & Trešnjev 2022), the tendency is to avoid prosecution. The defendant´s guilt must be proved beyond reasonable doubt, which is cumbersome to accomplish when the underlying regulations and definitions are unclear or confusing (Uhlmann 2009: 1234). The process of proving the claims is complex in non-environmental cases as well (see Škulić 2015); yet the highly technical nature, combined with intertwined and overlapping regulations and consequences of the crime that are often in the somewhat blurry form of endangerment[13] seem to be particularly deterring with regard to eco-crimes. In addition, the environment and its various manifestations as the protected legal goods seem to have the same reputation as victimless crimes, where the illegal act typically either involves only the perpetrator or occurs between consenting adults. Prosecutors have limited resources and will not tend to pursue cases that seem unwinnable (Uhlmann 2009: 1234), especially if no person and, some may add, media attention is involved.

DEPENDENCE ON ADMINISTRATIVE LAW PROVISIONS

Another overarching issue is the dependence of ecological crimes on administrative law provisions. Like criminal and ecological law, administrative law is a form

12 The WWF lists and defines specifically those two terms in their position paper on a new EU Environmental Crime Directive. So is substantial damage additionally defined by the criteria of monetary value of the damage, the conservation status of the species affected, and the habitat affected. The scale of financial benefits gained by committing the offence, and whether the act is committed by an organized criminal group or not are mentioned with regard to what constitutes negligible quantity. WWF (2022: 3).

13 See section „Technical Expertise and Models of Liability".

of public law. It deals with the establishment, duties, and powers of and available remedies against authorized agencies in the executive branch of the government.[14] The previously mentioned blanket formulations from criminal law provisions have to be specified by the respective regulations from administrative law; they rely and depend directly upon them.

This dependence existed already since the emergence of environmental laws in the 1970s. They were usually of administrative nature and imposed, for example, an obligation for the operator to apply for permission and to conduct the operations in accordance to the conditions set out in the permit (Faure 2016: 12). The criminal law provisions would be located only at the end of the respective environmental statute, to assure that disobedience of the law would be followed by criminal sanctions (Faure 2016: 12). It was mostly pollution without a permit or the violation of permit conditions or other obligations that were criminalized (Faure 2016: 12). Although today the issue of environmental crime has gained momentum and received a more prominent place within the (core) criminal legislation, this simple formula – absence of or violation of permit leading to criminal liability, remained an integral part of criminal law provisions in formulations from the Criminal Code like „by violating the regulations" (i.e. in Article 260, Article 264), „contrary to regulations" (i.e. in Article 262, Article 267, Article 268), „in breach of regulations" (Article 269) or even literally „without a special permit when such permit is required" (Article 276) - meaning in the broader sense „unlawful", „illegal" or „illicit" (see also Marković 2015), and by this, maintained the administrative dependence as well. Also, secondary criminal legislation still contains ecologic crimes at the end of the respective laws like in the early period and by this also the absolute administrative dependence. This highly dispersed nature of environmental criminal law (spread throughout primary and secondary law, and then again within numerous secondary laws) makes it obviously difficult for the law enforcer to find out to what extent the respective behaviour would be prohibited (Faure 2016: 15). The law enforcers may consider environmental issues to be of higher significance if they are a part of the criminal codifications and criminal laws. The implementation of these provisions into the penal code could affect general prevention and could facilitate prosecution of these crimes. However, the walk through the administrative jungle remains. As we have seen, the provisions from the central criminal codes also refer to administrative notions; hence dependence on them cannot be avoided even there.

One consequence of this dependence[15] is that ecological values are not directly protected by criminal law (Faure 2017: 328), not even if they are part of the primary legal acts. A huge pollution of a river, for instance, will not necessarily be

14 https://www.merriam-webster.com/dictionary/administrative%20law, last accessed July 10, 2022.
15 For a comparison of models of the administrative dependency see Andrea Rocco Di Landro 2022, SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4029962, last accessed July 5, 2022.

a crime or will be punishable at all.[16] Before criminal liability can be investigated and confirmed, the act committed has to constitute an administrative violation first. In other words, administrative acts do not only establish criminal liability; they are the forerunners and set the direct boundaries to criminalize pollution. By defining the conditions for obtaining permits and licences, and by setting the reference values for pollution, they directly determine the requirements for penal liability and relativize the autonomy of criminal law.[17]

The structure of environmental crimes, involving the element of „(administrative) unlawfulness" in many different expressions, differs from the structure of traditional crimes that protect individual values, such as property, life or health (Faure 2017: 328); although all of them constitute an intrinsic part of eco-crimes. Unlawfulness in this context is a violation of regulatory rules promulgated and enforced by environmental protection (Shover & Routher 2005: 324) or other, less specified agencies. By introducing an intermediary (the administrative authority), the legislator does not deem the environment as such to be the foundational legal interest of eco crimes; the central point is the violation of administrative requirements (Faure 2017: 329). This is further differentiated depending on the form of endangerment/harm that is required according to the respective criminal law provision.[18]

The detection and proving of environmental crimes will therefore have to overcome the „administrative jungle" of numerous regulations that concern threshold values and that are spread throughout various acts that regulate a multitude of different issues and that are not necessarily connected and easy to find.

On the other hand, these manifold provisions can also intersect and create another challenge, namely the untangling and identification of the right provision that has been breached. So, the steps in establishing the element of unlawfulness will have to include the identification of the correct provision and the eventual delimitation from similar regulations. This often also involves cross-referencing from act to act, including international agreements that have been implemented in the national legal systems. For example, for wildlife protection in Serbia, not only are the Criminal Code and the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) relevant, but also the – almost identical-sounding - Law on Environmental Protection and the Law on Nature Pro-

16 Pollution in Belgium, caused by the German pharmaceutical company Bayer, could not be assesed by the Antwerp Court of Appeal, because there was no valid license, due to an administrative error and hence the company could not be blamed. This administrative dependence of environmental criminal law (here the non-existence of a license due to failure of administration) disallowed the Court to verify if the emissions from Bayer were illegal pollution. Faure 2017: 328.

17 This lack of autonomy was critized at the AIDP (Association Internationale De Droit Pénal – International Association of Penal Law) Conference in 1994, where it was stated that „where offences against the environment are subject to criminal sanctions, their key elements should be specified in legislation and not left to be determined by subordinate delegate authorities." Faure 2016: 13, 14.

18 See next section.

tection (Marković 2021: 94, 95). Also, the demarcation line has to be established between criminal offences, misdemeanors and economic crimes.

Those administrative rules, however, do not necessarily entail specifications that go beyond quantitative values. This means that in addition, the nature of the offence has to be determined whether it is an instantaneous or continuous crime. It has to be done for various reasons - for the sake of the criminal classification (what crime?), for later sentencing (mitigating or aggravating circumstances), for the application of the law over time and for the potential for initiating new proceedings (Billiet 2018: 15). A continuous behaviour carries on as long as the perpetrator does not terminate his criminal behaviour (i.e. pursuing a polluting activity without authorization) (Billiet 2018: 15). An instantaneous crime happens in one single moment and is completed with the termination of the act (i.e. the killing of an animal that belongs to a protected species) (Billiet 2018:15). This is an additional effort, inseparably connected to precise technical knowledge about the eco-medium and the possible pollution.

TECHNICAL EXPERTISE AND MODELS OF LIABILITY

From the aforementioned administrative dependence, further challenges arise. The most practical and straining in terms of time and finances is the proving of breaches of administrative obligations, which can be done by the use of technical knowledge and skills. The expertise is necessary to establish the extent of contamination, to determine the remedial requirements and the costs of restoration and to allocate, at least technically, the liability for the immediate consequences and for injuries due to the exposure to toxics ((Murphy 2016: 1-20, according to Bachmaier 2016: 200).[19] This is insofar important as damages to the environment are often caused by the mere accumulation, addition or synergetic effects of hazardous actions, raising problems regarding the proof of causality (Cho 2000: 22).

This knowledge and evaluation is provided by an (appointed and sworn) technical expert or by administrative agency, and the judge can rely heavily on that exper-

19 These can be broken down into the following questions: What is the subject of pollution? / In what form has the pollution manifested itself? / Are there other harmful consequences? / Where and when did the consequences occur? / Where is the origin of the pollution? / What is the source of pollution? / What circumstances have facilitated the commission of the offence? / What were the technical preconditions for the pollution to occur? / What regulations on the protection of the environment have been breached and have the rules of operation and the company policy been breached? / Who is responsible for the pollution? / Were the regulations violated by action or ommission? / What is the causal link? / What are the motives, goals? / What are the mitigating and aggravating factors? / What is the form and level of guilt? / What type of eco-delict (criminal offence, misdemeanor, economic offence) has been committed? Pisarić 2015: 790, 791.

tise (Faure & Visser 1995: 327). These specialists derive from various technical fields, traffic, medicine and other vocations, and have to fulfill the triad of technical knowledge, experience, and knowledge of the applicable provisions.

Here we see not only is the administrative dependence an interim step; the interpretation of the actual consequences in the respective case is a further intermediate point. In addition, the admissibility, reliability and the high costs of scientific expert evidence represent further obstacles in the prosecution of environmental crimes (Bachmaier 2016: 193). The gathering and assessment of evidence gets even more complicated when the expertise has to be conducted in a foreign country, due to the transnational dimension of environmental crimes, having to apply the already complex cross-border judicial cooperation procedures (Bachmaier 2016: 193).

These consequences are, together with the required form of guilt, basically establishing the model of liability that is attributed to the offence; they represent the relationship between the way the crime is legally defined and the conditions of proof that have to be met to provide evidence for this crime (Faure & Visser 1995: 316).

The first possible consequence is abstract endangerment – not the creation of risk, but the potential creation of risk. As it is only a potential, it is not specifically required in legal wordings of crime and has not to be proven. An example would be the offence from Article 272 CC – Producing Harmful Prodcuts for Treating Animals. The crime committs whoever produces for sale or puts into circulation by trade products for treatment or prevention of animals that are dangerous to life or health of animals (para. 1). It is not necessary that life or health of animals are endangered; it is only necessary that the possibility for concrete danger occurs, not the occurrence itself is required (Stojanović 2018: 851). In other words, since the potential risk suffices for establishing criminal liability, it is not needed for the danger or even damage to arise. The problem of proof is therefore small here (Cho 2000: 26). In this case, all the public prosecutor has to do is to show that the products are dangerous to life or health of animals; there is no need to prove that this was done illegally or that it actually has constrained the life or health of animals. What constitutes the danger is standardized in general legislation, or, as in this case, it is specified in by-laws (Faure & Visser 1995: 319). The downside to this kind of regulation is its conflict with the legality principle (*lex certa*) when the legislator defines the conditions of criminal liability very broadly and leaves all the power to determine the more specified conditions to the executive and its administrative agencies (Cho 2000: 25). The focus of protection is then more on the administrative provisions than on the environmental legal good, bringing us back to the issue of administrative dependence.[20]

20 See previous section.

The next model is that of concrete endangerment – a threat that has occurred and is not anymore only a possibility. Unlike abstract endangerment from the previous case, the concrete risk is part of the wording of the criminal offence and therefore needs to be proved. Contamination of drinking water and food for animals from Article 273 CC is an example for a criminal act with concrete danger, committed by „whoever contaminates livestock food or water by a harmful substance and thereby endangers the life or health of the animals (Stojanović 2018: 852). This kind of provision aims more directly at the protection of the environment, the administrative component is less in focus. However, contrary to the previous example, additional operations of proving the actual danger have to be conducted when we speak about concrete endangerment.

The last option is that of harm. Physical alterations in the form of damage or destruction, as part of the legal wording, have to be substantiated. Example for that is Damaging the Environment from Article 264 CC. Demarcation issues with regard to pollution of the environment may arise, though (Stojanović 2018: 838, 839). The causality link to this kind offences should be established easier than in the previous case due to its materialization in the environment.

CONCLUSION

The importance of water, air and soil, flora and fauna is indisputable by now. However, the statistics on reported crime, accusations and convictions, a high number of unreported and unprosecuted cases is in strong disproportion to the importance and frequency of violations of those goods. The combination of huge profits, low risk of detention and ineffective penalties has made environmental crime extremely profitable (Bachmeier 2016: 195).

Certain characteristics of those crimes can be seen as contributing factors. The legislative provisions try to regulate intrinsically complex facts in a vague way that is often contrary to the legality principle of criminal law. In fact, their immanent administrative dependence raises the need to reconcile the logic of administrative law with that of criminal law. On the other hand, a universal definition of environmental crimes is not necessary, especially as it would not satisfy the requirements of the main criminal law principle of legality. However, the existing national provisions do need to be more specific or at least backed by a developed judicial practice that will give orientation in detecting, proving and prosecuting these types of crime.

A connected issue to low detection and persecution rates is the lack of understanding of the respective, rather scattered provisions – their content, their limits, and their scope of harm. The lack of resources for costly investigative operations and the involvement of experts in various fields adds up to this. Expert evidence

is crucial; depending also on the formulation of the consequences of the crime (harm/endangerment). Naturally, the high technical and factual complexity of this expertise is raising its costs (de la Cuesta 2016: 346). The judicial system as such lacks the required technical knowledge to fully grasp, understand and classify polluting and otherwise damaging actions. As a result, prosecutors will have the tendency to use their discretion to bring only the most egregious cases to court (Faure 2017: 328). A vicious circle is formed: one the one hand, criminal prosecution tends to be avoided because of the lack of specialization; and on the other hand, judges do not acquire the needed experience in environmental crimes as there are only few cases (Bachmaier 2016: 197). Together with the dismissal rates in environmental cases and in absence of alternative penalties, environmental crimes are likely to suffer from under-deterrence (Faure 2017: 328).

This is the reason why some countries (i.e. Australia, New Zealand) have established specialized environmental courts (Bachmaier 2016: 197).[21]

In order to achieve a more developed judicial practice that would provide orientation for the ambiguous provisions, training for prosecutors and judges would be beneficial. They would gain enhanced and specified knowledge of environmental offences and harm it causes or potentially can cause. To paraphrase Billiet: by getting a full insight into the scope of the illicit benefits eco-crimes generate, law enforcers would understand what a „big business" environmental crime can be (Billiet 2018: 45).

REFERENCES

Administrative Law. https://www.merriam-webster.com/dictionary/administrative%20law, last accessed on July 10, 2022.

Bachmaier, L. (2016). Obstacles to prosecution of environmental crime and the role of expert evidence. A comparative approach. *Revue Internationale de Droit Pénal*, 191 – 219.

Banić, M. (2021). Krivičnopravna zaštita ugroženih i divljih biljnih i životinjskih vrsta i izazovi pravne prakse. *Strani pravni život*, 1, 63 – 78.

Billiet, C.M. (ed). (2018). *Sanctioning Environmental Crime: Prosecution and Judicial Practice*, available at https://biblio.ugent.be/publication/8611216.

Bugarski, T. (2015). Izazovi organizovanog ekoloükog kriminaliteta. *Zbornik radova Pravnog fakulteta, Novi Sad*, 4, 1097 – 1107.

Burns, R. & Lynch, M. (2004). *Environmental Crime. A sourcebook*. El Paso: LFB Scholarly Publishing.

21 For a differentiated view see Lukić & Pisarić 2012: 219 – 239.

Byung-Sun, Ch. (2000). Emergence of an International Environmental Criminal Law? *UCLA Journal of Environmental Law and Policy*, 1, 11 – 47.

Criminal Code, *Official Gazette of RS*, nos. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.

De la Cuesta, J. L. (2016). Protection of the Environment through Criminal Law. Final Reccomendations. *Revue Internationale de Droit Pénal*. 343 – 348.

Delić, N. (2011). Nekoliko napomena u vezi uslova odgovornosti pravnog lica za krivično delo. *Pravo i privreda*, 7-9, 289 – 301.

Delić, N. (2022). *Krivično pravo Posebni deo*, 2. izdanje. Beograd: Pravni fakultet Univerziteta u Beogradu.

Di Landro, A. R. (2022). *Environmental Criminal Law´s dependence on Administrative Law, in the Purely Accessory and Partially Accessory Models: Pluses and Minuses. Assessing the Opportunity for a Limited Number of Offences Being Autonomous from Administrative Law*, February 8, 2022, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4029962.

Drenovak-Ivanović, M. (2021). *Ekološko pravo*. Beograd: Pravni fakultet Univeziteta u Beogradu.

Elliott, L. (2012). Fighting Transnational Environmental Crime. *Journal of International Affairs*, 1, 87 – 104.

Faure, M. (2016). Limits and Challenges of Criminal Justice Systems in Addressing Environmental Crime. *Revue Internationale de Droit Pénale*. 11 – 36.

Faure, M. (2017). The Revolution in Environmental Criminal Law in Europe. *Virginia Environmental Law Journal*, 2, 321 – 356.

Faure, M., & Visser, M. (1995). How to Punish Environmental Pollution? Some Reflections on Various Models of Criminalization of Environmental Harm. *European Journal of Crime, Criminal Law and Criminal Justice*, *3*(4), 316-368.

Ilić, G. P., Majić, M., Beljanski, S., Trešnjev, A. (2022). *Komentar Zakonika o krivičnom postupku*. 11. izdanje. Beograd: Službeni glasnik.

Kuhlen, L. (1993). Umweltstrafrecht – auf der Suche nach einer neuen Dogmatik. *Zeitschrift für die gesamte Strafrechtswissenschaft*, 4, 697 – 726.

Lazarus, R. (1995). Meeting the Demand of Integration in the Evolution of Environmental Law: Reforming Environmental Criminal Law. *Georgetown Law Journal.* 2407 – 2438. Quoted according to Uhlmann 2009.

Lukić, T. & Pisarić, M. (2012). Specijalizacija pravosudnih i drgih organa u borbi protiv ekološkog , kriminaliteta. *Zbornik radova Pravnog fakulteta, Novi Sad*, 4, 219 – 239.

Marković, I. (2015). Neka osnovna pitanja u vezi sa objektivnom stranom protivpravnosti. In: Dj. Ignjatović (ed), *Kaznena reakcija u Srbiji* (V deo, 285 – 300). Pravni fakultet Univerziteta u Beogradu: Beograd.

Marković, I. (2017). Kernaspekte der aktuellen Reform des Allgemeinen Teils in Serbien. *Zeitschrift für die gesamte Strafrechtswissenschaft,* 3, 885 – 908

Marković, I. (2021). Wildlife Trafficking as Catalyst of (COVID19) Pandemic. *Archibald Reiss Days – Thematic Conference Proceedings of International Significance*. Belgrade: University of Criminal Investigation and Police Studies, 91 – 103.

Milne, R. A. (1989). The Means Rea Requirements of the Federal Environmental Statutes: Strict Criminal Liability in Substance But Not Form. *Buffalo Law Review*, 1, 307-336.

Murphy, B. (2016). Applications of Environmental Forensics. In: (B. Murphy & R. Morrison eds.), *Introduction to Environmental Forensics*. Cambridge:Elsevier Academic Press. 1 – 20. According to: Bachmeier 2016, 200.

Pisarić, M. (2011). Suzbijanje prekograničnog ekološkog kriminaliteta. *Zbornik radova Pravnog fakulteta, Novi Sad*, 2, 425 – 439.

Pisarić, M. (2015). Pretpostavke za otkrivanje ekološkog kriminaliteta. *Zbornik radova Pravnog fakulteta, Novi Sad*, 2, 785 – 795.

Schall, H. (2014). Das Umweltstrafrecht heute: ein bloßes Alibi-Instrument?. In: *Festschrift für Bernd Schünemann zum 70. Geburtstag am 1. November 2014* (815-826). De Gruyter.

Shover, N. & Routhe, A. (2005). Environmental Crime. *The University of Chicago Press*. 321 – 371.

Škulić, M. (2015), Dokazi i dokazni postupak na glavnom pretresu. In: (S. Bejatović, I. Jovanović, eds.), *Glavni pretres i suđenje u razumnom roku: regionalna krivičnoprocesna zakonodavstva i iskustva u primeni*. 193 – 217.

Statistical Office of the Republic of Serbia (2021). *Bulletin. Adult perpetrators of criminal offences in the Republic of Serbia, 2020*. Belgrade.

Stojanović, Z. (2018). *Komentar Krivičnog zakonika*. 7. izdanje. Beograd: Službeni glasnik.

Uhlmann, D. (2009). Environmental Crime Comes of Age: The Evolution of Criminal Enforcement in the Environmental Regulatory Scheme. *Utah Law Review*, 4, 1223-52.

Vagliasindi, G. M. (2016). The Fight against Environmental Crime in the European Union and its Member States: A Perspective on the Enforcement System. *Revue Internationale de Droit Pénal*, 1, 151 – 187.

Vuković, I. (2011). Kolegijalno odlučivanje i krivična odgovornost. *Pravo i privreda*, 7-9, 302 – 317.

Wolf, B. (2009). *Organized environmental crime. An analysis of corporate non-compliance with the law.* Lewiston: Edwin Melles Press.

WWF, *Position Paper*, 2022, available at: https://www.wwf.eu/?6109916/A-new-EU-Environmental-Crime-Directive, 3.

THE INTERNATIONAL LEGAL FRAMEWORK AGAINST CORRUPTION

Duško Dimitrijević, PhD[1]
Institute of International Politics and Economics, Belgrade, Serbia

PURPOSE

The dynamics of international relations in the last few decades have led to the evolution of various forms of corruption in international practice of organized crime. As one of the complex human phenomena that has a deep moral basis, corruption is often defined as a kind of "perversion" of honesty and fidelity in performing entrusted duties, i.e. as an "unfair" or "unfaithful" behavior that leads to bribery or which leads to "abuse of the entrusted authority for private gain" (Nicholls et al., 2005; Llamzon, 2014: 19). Although corruption is easier to understand in everyday colloquial speech than in legal theory and practice, it is clear that it is an extremely complicated behavior that has several modalities that have developed in parallel with the development of society. So today, corruption is manifested through covert and often long-term actions of one or more individuals involved in the functioning of the public sector (which often includes close ties to the private sector), who, through the abuse of their official position, acquire personal property benefit, which essentially affects the undermining of the foundations of the economic and legal order of the States. This has become particularly evident in the recent period when traditional ethnic and national criminal groups have given way to multiethnic and multinational macro-regional criminal groups that have taken advantage of the diversification of international trade and improved communication and financial systems around the world. As corruption raises serious moral, economic and political dilemmas, undermines institutions and democratic, ethical and legal values, good governance, efficient, transparent and com-

1 dimitrijevicd@diplomacy.bg.ac.rs

petitive market operations, the international community has been forced to adopt important international legal instruments to combat this scourge (which is usually associated with organized crime, especially economic crime, human and drug trafficking, money laundering and terrorist financing), which negatively affect the sustainable economic development of States (Dimitrijević, 2018). Money laundering and terrorist financing on international and national legal level. In: Thematical Proceedings of VIII International Scientific Conference, Archibald Reiss Days. Belgrade: University of Criminal Investigation and Police Studies). Working diligently to adopt a series of international conventions through the United Nations, the European Union, the Council of Europe, the Organization for Economic Cooperation and Development, the Organization of American States, the African Union and other important international organizations, the international community has established a comprehensive and a multidisciplinary international legal framework with the legal standards needed to effectively combat corruption (Simović & Šikman, 2017). The purpose of this study is limited to the analysis of the most important international legal instruments of international organizations that may be important for our successful and effective fight against corruption.

DESIGN/METHODS/APPROACH

Using the appropriate scientific methods for legal analysis, in the following section the author identifies and interprets the provisions of conventions and other international legal instruments of international organizations that make up the international legal framework for the fight against corruption.

UNITED NATIONS CONVENTION AGAINST CORRUPTION

The United Nations Convention against Corruption was adopted in New York on 31 October 2003 and entered into force on 14 December 2005 (UNTS, 2003). According to the general provisions, the Convention was adopted to promote and strengthen measures to prevent and combat corruption more effectively and efficiently, then to promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against corruption, including in asset recovery, as well as to promote integrity, accountability and proper management of public affairs and public property. The Convention is applied for the purpose of preventing corruption, conducting investigations and prosecuting, as well as for the purpose of freezing, seizing, confiscating and recovering proceeds of crime. Each State Party shall take the necessary measures, including legal and administrative measures, in accordance with the fundamental principles of its do-

mestic law, to ensure compliance with the obligations of this Convention. Fulfillment of these obligations, however, cannot be to the detriment of the sovereign equality and territorial integrity of other States, nor can it be to the detriment of their domestic jurisdictions (UN Office on Drugs and Crime, 2004). With regard to preventive measures, the Convention obliges States to regularly evaluate their domestic anti-corruption legislation. It also obliges States Parties to establish effective practices and to develop and implement effective, coordinated anti-corruption policies that promote public participation and reflect the principles of the rule of law, good governance of public affairs and public property, integrity, transparency and accountability. In addition, the Convention obliges States to cooperate with each other in accordance with the basic principles of their legal system and to develop such relations with relevant international and regional organizations in order to implement preventive measures. In particular, this cooperation, in accordance with the provisions of Article 5 of the Convention, may include participation in international programs and projects aimed at preventing corruption. States Parties to the Convention are obliged to establish special bodies to monitor the implementation of anti-corruption policy. They are obliged to provide such bodies with appropriate material and professional support and to provide them with an independent position in the performance of their functions. States are obliged to strengthen the systems of hiring, employment, retention, promotion and retirement of civil servants, and to adopt appropriate legislation on the appointment of public officials. In this regard, they will particularly advocate for transparency in the financing of candidacies for public office and, where necessary, for the financing of political parties. According to the Convention, they are also obliged to strengthen the transparency of systems that avoid conflicts of interest. Each State Party shall endeavor to apply, within its institutional and legal system, codes or standards of conduct for the proper, honorable and proper performance of public functions. Relevant initiatives of regional, interregional and multilateral organizations, such as the International Code of Conduct for Public Officials, contained in the annex to General Assembly resolution 51/59 of 12 December 1996, should also be taken into account. States are also required to establish measures and systems that require public officials to make statements to the appropriate authorities regarding, *inter alia,* their other activities, employment, investment, property and gifts of significant value or benefits that may give rise to a conflict of interest in relation to their work as public officials. They should also make it easier to report acts of corruption, as well as take disciplinary and other measures against public officials who violate the provisions of the code or anti-corruption standards. With regard to public procurement management, the Convention provides for the establishment of systems based on transparency, competition and objective criteria in decision-making that are effective in preventing corruption. Similarly, the Convention provides for the management of

public finances, which emphasizes the existence of procedures for the adoption of the State budget, transparency of income and expenditure reports, the existence of a system of auditing standards, effective risk management, internal control and adequate corrective measures. States are required to take such civil and administrative measures as may be necessary under the basic principles of domestic law to preserve the integrity of the accounting records. In this sense, States are obliged to take measures that may be necessary to increase the transparency of public administration, including its organization, functioning and decision-making procedures. Without affecting the independence of the judiciary and the prosecutor's office, States still have a duty to take measures to strengthen their integrity and prevent opportunities for corruption. The provision of Article 12 of the Convention, which refers to taking preventive measures to prevent corruption in the private sector, is very important. Namely, the Convention prescribes effective, proportionate and dissuasive civil, administrative and criminal penalties for non-compliance with such measures, which include, *inter alia*: improving cooperation between law enforcement agencies and relevant private entities; implementation of standards and procedures to preserve the integrity of relevant private entities, including codes of conduct for fair, honest and proper conduct of business activities and all relevant professions and to prevent conflicts of interest, and to promote good business practice among companies and in contractual relations with the State; increase transparency in relations between private entities, including, where necessary, measures relating to the identity of legal and natural persons involved in the establishment and management of corporations; preventing the abuse of procedures governing private entities, including those relating to subsidies and permits issued by public bodies for the conduct of business; prevention of conflicts of interest by introducing restrictions, where necessary and for a reasonable period of time, on the performance of professional activities of former public officials or the employment of public officials in the private sector after leaving public office or retirement, where those activities or employment are directly related to who were or were supervised by these public officials during their term of office; ensuring that private companies, taking into account their structure and size, have sufficient internal audit control and are subject to appropriate audit and certification procedures. In accordance with their regulations on bookkeeping and data storage, publication of financial statements and accounting and auditing standards, States are required by the Convention to prohibit the opening of unregistered accounts, unregistered or inadequately identified transactions, recording of non-existent expenditures, documents and intentional destruction of accounting documents before it is provided by law. States should also ban tax deductions from expenses that constitute bribes. They have a duty to take public information measures and to ensure that the public is informed of the anti-corruption bodies listed in this Convention through which corruption can be report-

ed. In addition, States have a special obligation to establish an internal regulatory and supervisory regime for banks and non-bank financial institutions, including natural or legal persons, that provide official or unofficial services for the transfer of money or valuables and, where appropriate, other bodies which are particularly susceptible to money laundering. In addition, States are required to consider establishing a financial intelligence unit to serve as a national center for collecting, analyzing, and providing information on potential money laundering. Also, States are obliged to examine the possibility of applying appropriate and feasible measures that require financial institutions to tighten control over the sending of money and payment instruments abroad without hindering the movement of legitimate capital. The Convention calls for stronger international judicial co-operation and co-operation with financial regulators. To this end, it directs States to use the guidelines and relevant initiatives of regional, interregional and multilateral organizations to combat money laundering (Art. 14). According to the provisions of Articles 15 to 25, the Convention stipulates the obligation to incriminate a wide range of criminal acts, namely: bribery of domestic and foreign public officials and officials of international organizations, embezzlement, abuse or other illegitimate use of property by public officials, abuse of influence and functions, illegal enrichment, bribery in the private sector, embezzlement of property in the private sector, laundering of proceeds of crime, concealment and obstruction of justice. In addition to the obligation of States to incriminate and punish natural persons for committing, complicity, aiding or abetting corruption, the Convention also stipulates the obligation of States to prescribe criminal, civil or administrative liability of legal entities in their legislation. The provision of Article 30 of the Convention, provides for the obligation of the Contracting Parties to prosecute and sanction perpetrators of corrupt acts. In addition to the means acquired through the commission of acts of corruption or used for their commission, in the provision of Article 31, the Convention regulates in detail the methods of their identification, freezing, seizure and confiscation. A very important incentive for reporting corruption offenses is provided for in Article 33 of the Convention, which provides for the protection of whistleblowers. The consequences of corruption under the Convention must be remedied through the prosecution of perpetrators and through compensation for damages that does not preclude the possibility of annulment or termination of the contract, revocation of the concession or other similar instrument or for taking another remedy. In fact, the Convention emphasizes that the return of goods acquired through acts of corruption is one of the basic principles and that the contracting States are obliged to cooperate with each other in this regard and provide assistance to each other. After all, Chapter V of the Convention is dedicated to this, which provides in detail the mechanisms for the return of property through international cooperation in the implementation of confiscation. It also encourages the conclusion of multilateral and bilateral

agreements in order to improve this procedure. Jurisdiction for criminal prosecution under the Convention is without prejudice to the norms of general international law, since the Convention prescribes territorial jurisdiction and jurisdiction based on the personality of the law (active and passive protective principle), which does not exclude criminal jurisdiction in the manner prescribed by domestic law. In order to successfully and effectively combat corruption, the Convention provides for the establishment of special national bodies, strengthening cooperation with competent national and international bodies for the prosecution of corruption, interstate cooperation and encouraging cooperation with the private sector. According to the Convention, international cooperation in prosecuting and punishing corruption should be conducted in accordance with the principle of *aut dedere, aut punire.* At the same time, there is a possibility of transferring proceedings in order to achieve criminal prosecution. Special measures to improve the prevention and punishment of corruption are provided for in Chapter VI of the Convention, which deals with the provision of technical assistance and the exchange of information related to these acts. Technical assistance includes the implementation of appropriate anti-corruption plans and programs, including material support and training, as well as the exchange of relevant experience and specialist knowledge, which should enable better international cooperation between States. In order to ensure the consistent application of the provisions of the Convention, the Conference of the States Parties has been established. The Conference as monitoring mechanism is established to "improve the capacity of and cooperation between States Parties to achieve the objectives set forth in this convention and to promote and review its implementation" (Article 63). The Secretary-General and the Secretariat of the United Nations shall provide the necessary services to the Conference of the States Parties to the Convention (Article 64). Given that each State Parties is given the opportunity to assess what measures it will take to fulfill its obligations under the Convention, in practice there has been inconsistent application of the stipulated anti-corruption measures, which is why the UN established the Review Mechanism at the Doha Conference in 2009. Its role is to submit annual reports with self-evaluation of the results achieved in the fight against corruption. In that way, they wanted to overcome the perceived weaknesses and encourage the States to show stronger readiness to respect the recommendations not only of intergovernmental bodies, but also of civil society organizations and independent experts. Finally, it is worth noting that the UN, in addition to this Convention, also adopted the Convention on Transnational Organized Crime in 2000, which entered into force in 2003, and which also calls on the State Parties to criminalize corruption (I.L.M., 2001: 334-394).

THE OECD CONVENTION ON COMBATING BRIBERY OF FOREIGN PUBLIC OFFICIALS IN INTERNATIONAL BUSINESS TRANSACTIONS

Twenty-nine OECD member States and five non-member States (Argentina, Brazil, Bulgaria, Chile and Slovenia) signed on 17 December 1997 the Convention Combating bribery of foreign public officials in international business transactions. The Convention entered into force on 15 February 1999 (I.L.M., 1998: 1-11). In a sense, the OECD Convention follows the guidelines contained in the UN Declaration against Corruption and Bribery in International Commercial Transactions, supplemented by General Assembly Resolution 51/191 of 21 February 1997, which calls on member States to take appropriate measures and cooperate in all levels in the fight against corruption and bribery in international commercial transactions (United Nations, 1997). Unlike the UN Convention against Corruption, which covers a wide range of incriminated persons, the OECD Convention is limited to incriminating persons who bribe foreign public officials (Balmelli & Jaggy, 2004). In other words, the Convention implies the responsibility only of those who bribe (active bribery), not the responsibility of foreign officials who seek or receive or receive bribes (passive bribery). "Foreign public official" under the Convention includes any person holding a legislative, administrative or judicial office in a foreign country, whether appointed or elected; any person holding public office for a foreign country, including there is also a function in a public service or public enterprise and any official or agent of a public international organization. The bribery of foreign public officials in international business transactions does not exclude the criminal acts of incitement, aiding and abetting, authorization, attempt and conspiracy. The perpetrators of these acts may be natural persons and legal entities. Liability of a legal entity, in addition to criminal liability, also includes civil and administrative liability. States Parties have committed themselves to sanctioning bribery, and sanctions may include seizure or confiscation of property or the application of similar financial sanctions. With regard to the determination of jurisdiction, the Convention adopts the territorial principle. States Parties are also obliged to prosecute their nationals for offenses committed abroad on the basis of personal principle, and where such jurisdiction exists for other offenses. In the event of a conflict of jurisdiction, the contracting States shall consult each other. Also, each party is obliged to consider whether its jurisdiction in the case (on territorial or nationality basis), would lead to the effective implementation of measures in the fight against bribery of foreign public officials and, if not, take corrective steps. Investigation and prosecution of the bribery shall be subject to the applicable rules and principles of each contracting States. According to the Convention, extradition should take place in accordance with internal regulations and on the basis of mutually concluded agreements. Ac-

cording to the Convention, States have an obligation to prohibit the keeping of hidden accounts, irregular accounting and to eliminate all irregularities that lead to bribery or concealment of bribery. In this regard, they are obliged to suppress the crime of money laundering and to provide each other with international legal assistance in criminal matters. Although the OECD Convention is limited in subject matter and territory compared to the UN Convention, it has not been ineffective as it has affected the harmonization of domestic legislation with international legal standards. Thus, according to Article 12 of the Convention, it follows that the States are obliged to cooperate and promote its implementation and enforcement. Monitoring of the implementation of the Convention is done within the OECD Working Group on Bribery through a peer review process, which includes first monitoring the compliance of domestic legislation with the Convention, and then monitoring the implementation of the legislative framework in practice (OECD, 2008: 12; Razzante, 2020: 170). As weaknesses have been identified in the application of certain legislative frameworks in practice, the OECD adopted on 26th November 2009, Recommendation for Further Combating Bribery of Foreign Public Officials in International Business Transactions. Previously, the Council adopted the Recommendation of the Council on Tax Measures for Further Combating Bribery of Foreign Public Officials on May 25 of the same year, which explicitly disallow the tax deductibility of bribes to foreign public officials, for all tax purposes in an effective manner. The Recommendation for Further Combating Bribery of Foreign Public Officials recommends in particular that governments encourage their enterprises to develop and adopt adequate internal controls, ethics and compliance programmes or measures for the purpose of preventing and detecting foreign bribery. This specifically includes preventive measures against small facilitation payments, protecting whistleblowers and improving communication between public officials and law enforcement authorities (Chance, 2019: 8). Two Annexes have been added to this Recommendation: "Good Practice Guidance on Implementing Specific Articles of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions", which refers to specifying the responsibilities of foreign public officials and legal entities and effective implementation of obligations under the Convention. as well as "Good practice guidance on internal controls, ethics, and compliance", which should serve as a legally non-binding guide for companies in establishing effective internal controls, ethics and compliance programs or measures to prevent and detect foreign bribery. In November 2016, the OECD Council issued a new Recommendation for Development Cooperation Actors on Managing the Risk of Corruption which recommends the application of comprehensive methods in risk management by relevant entities responsible for trade, export credit, international co-operation and diplomatic representations as well as the private sector. After that period, the special OECD Working Group undertook to conduct a comprehensive revision

of the 2009 Anti-Bribery Recommendations. The OECD Council adopted on 13th March 2019, new Recommendation directing States to take adequate measures to deter bribery in international business transactions benefiting from official export credit support. The latest Recommendation was adopted on 26th November 2021, which intensified efforts to prevent, detect and investigate foreign bribery. Taking into account the changed circumstances, these Recommendation support the strengthening of international cooperation in the implementation of foreign laws, introduce the principle of using non-judicial solutions in cases of bribery abroad, support legal entities to comply with anti-corruption rules, and promote comprehensive and effective protection for persons reporting bribes. This strong OECD anti-corruption framework covers areas such as taxes, official development assistance, export credits and State-owned enterprises (OECD, 2021).

COUNCIL OF EUROPE CRIMINAL LAW CONVENTION ON CORRUPTION

The Committee of Ministers of the Council of Europe adopted the text of the Criminal Law Convention on Corruption in November 1998. The Convention has been open for signature since 27 January 1999, and entered into force on 1st, July 2002 (European Treaty Series, 1999). The Protocol was subsequently added to the Convention, which entered into force on 1 February 2005 (European Treaty Series, 2003). Although the Convention formulates corruption as bribery (Article 13), it defines a wide range of acts of corruption that may constitute forms of transnational crime. The Convention and additional Protocol goes beyond the OECD Convention, as they criminalizes active and passive bribery of domestic and foreign public officials, national and foreign parliamentarians and members of international parliamentary assemblies, active and passive bribery in the private sector, active and passive bribery of officials of international organizations, active and passive bribery of domestic, foreign and international judges and officials of international courts, active and passive trading in influence, money laundering of proceeds from corruption offenses and accounting offenses connected with corruption offenses. With regard to the above-mentioned solution to corruption or bribery of officials of international courts, the Rome Statute of the International Criminal Court, which was adopted almost at the same time as this Convention, obviously had considerable influence (Schabas, 2004: 66). Under the provisions of the Convention, legal entities may also be held liable for bribery offenses committed in their favor. This liability includes the liability of any natural person which acts individually or within the body of the responsible legal entity, which has a leading position or power of attorney to represent that legal entity or the authority to make decisions, or to exercise control within that legal entity. Li-

ability of legal entities generally extends to criminal offenses trading in influence and money laundering (Article 18). As for the legal determination of active and passive bribery, it is considered that these are two sides of the same phenomenon. The briber's act offering, promising or giving the undue advantage and the bribe's act of accepting the offer, promise or gift are made independent criminal offences. However, the briber and the bribee will not be punished for complicity in the other one's offence (Council of Europe Explanatory Report, 1999). By the provisions of the Convention, States have accepted the obligation to incorporate the envisaged solutions into their national legislation. However, most of the provisions are of an optional nature and leave the State free to regulate the issues of incrimination of various forms of corruption in different ways. However, this does not completely relieve the State of its responsibility to apply the appropriate legal measures necessary to criminalize the commission, aiding or abetting of corruption offenses. The Convention imposes an obligation on States to provide effective, proportionate and dissuasive sanctions and coercive measures in their internal legal order, including the deprivation of liberty of perpetrators of corruption. In the case of legal entities, in addition to criminal and non-criminal sanctions, the Convention also prescribes the possibility of monetary sanctions. With regard to jurisdiction, the Convention accepts the principle *aut dedere, aut judicare*. At the same time, States may, with their internal legislation, establish territorial or personal jurisdiction in relation to the place where the criminal offense was committed, i.e. according to the citizenship of the perpetrator of the corruption. States reserve the right to regulate this issue in a different way and to make certain reservations when accepting the obligations under the Convention in relation to the application of the provisions on jurisdiction (Article 17). This, of course, does not exclude the obligation of States to establish jurisdiction for corruption offenses committed abroad when the perpetrator is on their territory and has their citizenship and for whom an extradition request has been made (Degan, Pavšić & Beširević, 2011: 308). For the effective fight against corruption, the Convention provides enhanced international co-operation and mutual assistance, extradition and the provision of information in the investigations and prosecutions of corruption offenses. In this regard, States have the possibility to form specialized bodies that would be authorized to act effectively in this area (Article 20). The provision of international legal assistance remains at the discretion of national authorities under the provisions of the relevant international instruments on international cooperation in criminal matters, or arrangements agreed on the basis of uniform or reciprocal legislation (Article 21). The Convention will be applicable whenever there is no international instrument or arrangement or when the provisions of the Convention are more favorable than the provisions of international instruments and arrangements (Art. 25). States would have the option of rejecting a request for international legal assistance with a call to protect its fundamental interests,

national security and sovereignty or *ordre public* (Art. 26). The monitoring mechanism of the implementation of the Convention is carried out by the Group of States against Corruption (GRECO) (Resolution of the Committee of Ministers of the Council of Europe, 1999). Membership in GRECO is not limited to member States (for example, the United States is a member of this body). The goal of GRECO is to effectively improve the ability of its members to fight corruption through the process of monitoring the implementation of anti-corruption measures and monitoring compliance with contractual obligations, monitoring compliance with the Twenty Guiding Principles for Combating Corruption developed by the Multidisciplinary Corruption Group and monitoring the implementation of obligations from other international instruments in accordance with the Program of Action against Corruption (Resolution of the Committee of Ministers of the Council of Europe, 1997). Accordingly, GRECO helps to identify gaps in national anti-corruption policies, encouraging the necessary legislative, institutional and practical reforms. This body also provides a platform for the exchange of best practices in preventing and detecting corruption. The evaluations carried out by this body focus on specific thematic areas that have been identified as particularly risky for most member States (Trifunović-Stefanović, 2020: 43).

COUNCIL OF EUROPE CIVIL LAW CONVENTION ON CORRUPTION

The Committee of Ministers of the Council of Europe adopted the text of the Civil Law Convention on Corruption in 1999. The Convention entered into force in November 2003, following the deposit of the required number of instruments of ratification (European Treaty Series, 1999). The Council of Europe Civil Law Convention is the first international convention to deal with the civil law aspect of corruption. Its provisions are mandatory and reservations to any of the provisions are not allowed. The Convention regulates the issues of compensation for damages, State responsibility, statute of limitations, validity of contracts, protection of employees (whistleblowers), issues of reporting and auditing, obtaining evidence and international cooperation. It is the only international convention that contains a definition of corruption. Corruption under Article 2 of the Convention means "requesting, offering, giving or accepting, directly or indirectly, a bribe or any other undue advantage or prospect thereof, which distorts the proper performance of any duty or behavior required of the recipient of the bribe, the undue advantage or the prospect thereof". It follows from this formulation that the Convention limited the definition of corruption only on its aspect of bribery. The Convention obliges the State Parties to provide in their domestic legislation effective remedies for persons who have suffered damage as a result of

acts of corruption, to enable them to defend their rights and interests, including the possibility of obtaining compensation for damage. This compensation should cover material damage, loss of profits and non-pecuniary loss. In order to obtain compensation, the injured party in the legally prescribed court proceedings has to prove the occurrence of the damage, whether the defendant acted with intent or negligently, and the causal link between the corrupt behavior and the damage. There is no liability if the person damaged by part of the corruption contributed to the damage through his own fault. States are obliged to provide in their internal legislation joint and several liability in cases where there are several perpetrators of corruption. The Convention contains a general provision on the nullity of contracts in the event of corruption. In the context of the development of modern international economic relations, this provision may be of particular importance for developing countries when the damage is caused by transnational corruption (Harvard Law and International Development Society, 2014-2015). The Convention provides for a subjective and objective limitation period. The first is 3, while the second is 10 years. The advantage of this approach is in easing the criteria for proving responsibility in civil proceedings, in which it is necessary to point out arguments about illegal behavior, direct and conscious doing or not doing, inciting or aiding, which contributes to active and passive bribery. In that sense, States are obliged to prescribe effective procedures for the acquisition of records in civil proceedings arising from an act of corruption, as well as to prescribe the possibility that courts may issue interim measures to ensure the interests and rights of parties during civil proceedings. A particularly important provision in the Convention relates to the obligation of States Parties to legislate appropriate procedures for persons who have suffered damage as a result of an act of corruption by its public officials in the exercise of their functions. In such situations the Convention incorporates the principle of vicarious liability under which injured parties may claim compensation either from a State if the defendant is a public official or from any appropriate authorities if he is not a public official (Article 5). Otherwise, the Committee of Ministers of the Council of Europe adopted on 11 May 2000 a Recommendation on Codes of conduct for Public Officials, which includes a Model Code of Conduct for Public Officials. This document gives suggestions on how to deal with real situations frequently confronting public officials, such as gifts, use of public resources, dealing with former public officials, etc. The Code stresses the importance of the integrity of public officials and the accountability of hierarchical superiors. It specifies the standards of conduct of public officials, and also contains general principles that public officials must adhere to while in public office, i.e. when they leave that position in the public service, especially in relations with former public officials. The Civil Law Convention on Corruption pays special attention to the protection of whistleblowers. In this regard, State Parties are obliged to take the necessary measures to protect all employees who

report their suspicions of corruption in good faith and on reasonable grounds. Finally, the Convention addresses also international co-operation. In this regard, there is an obligation of the parties to co-operate effectively in matters relating to civil proceedings in cases of corruption, especially concerning the service of documents, obtaining evidence abroad, jurisdiction, recognition and enforcement of foreign judgments and litigation costs in accordance with the provisions of relevant international instruments on international co-operation in civil and commercial matters as well as in accordance with their internal law. The provision of Article 12 of the Convention defines GRECO as a monitoring mechanism for implementations through previous evaluations and direct visits to countries.

CONVENTION ON THE PROTECTION OF THE EUROPEAN COMMUNITIES' FINANCIAL INTERESTS

In order to combat fraud affecting the financial interests of the European Communities, the Council of the European Union in July 1995 encouraged the drafting of the Convention on the Protection of the European Communities' Financial Interests (Council of the European Union Act, 1995). The Convention entered into force on 17 October 2002. It has been supplemented by a series of protocols over time. The First Protocol to the Convention adopted in 1996 makes a distinction between active and passive corruption of public officials. It also defines an "official" at national and EU levels and unifies criminal sanctions for corruption (First Protocol, 1996). Second Protocol, adopted in 1997, further clarified the Convention regarding the issues of the liability of legal persons. In this regard, Second Protocol criminalizes legal persons for fraud, active corruption and money laundering committed in their favor by any person, individually or within the body of a legal entity having a managerial function within the legal entity, on the basis of power of attorney or authority to make decisions on behalf of a legal entity or on the basis of powers to exercise control within the legal entity. The incrimination also extends to complicity, incitement and attempt to commit any of the aforementioned crimes (Second Protocol, 1997). The Convention replaced the previously concluded treaties on fraud prevention. It is very important as it has a preventive effect in terms of public expenditures and budget revenues. Under the Convention, "fraud" means fraudulent acts defined as all acts affecting the European Communities' financial interests, including any intentional act or commission relating to the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds from the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities; non-disclosure of information in violation of a specific obligation, with the same effect; the

misapplication of such funds for purposes other than those for which they were originally granted. In addition, fraudulent acts include the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the general budget of the European Communities or budgets managed by, or on behalf of, the European Communities, as well as non-disclosure of information in violation of a specific obligation, with the same effect. Also, the misapplication of a legally obtained benefit, with the same effect is treated as fraud. The Convention requires each Member State of the European Union to take all necessary measures to ensure that illegal conduct or fraud in both public spending and budget revenues, as well as participation in such actions, encouragement or attempt to take such actions, are subject to effective and proportionate criminal penalties that have a strong deterrent effect. In cases of serious fraud, the prescribed penalties must include imprisonment. Sanctions provided for legal entities should include criminal or non-criminal fines. Sanctions may also include other penalties such as exclusion from the right to public benefits or assistance, temporary or permanent disqualification from conducting commercial activities and placing under judicial supervision or issuing a court order for liquidation. In addition to the above obligation, the Convention stipulates that EU member States have a duty to take all necessary measures to determine their competence to prosecute corruption offenses. In this regard, the First Protocol establishes a number of criteria that determine the jurisdiction of the judicial authorities of a member State to prosecute corruption cases on a territorial and personal basis *(lex loci delicti comisii* and *lex nationalis)*. It also provides for the application of the protective principle when the offense is committed against a national of a member State, or when the offender is a Community official working for its institutions. In the event that a fraud constitutes a criminal offense involving at least two member States, it is the obligation of those countries to co-operate in investigating, prosecuting and enforcing sentences by, for example, mutual legal assistance, extradition, transfer of proceedings or execution of sentences in another EU member State. Efforts to improve the existing convention framework for the prevention of corruption at the EU level have led to the situation that the Treaty on the Functioning of the EU in Article 83 imposes an obligation on member states to criminalize corruption at the national legislative level (Treaty on the Functioning of the European Union, 2012). With a series of directives that followed, and of which perhaps the most important is Directive 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, the EU has consolidated key rules which member States should incorporate into their criminal law in order to prevent it at European level (Directive, 2017).

CONVENTION ON THE FIGHT AGAINST CORRUPTION INVOLVING OFFICIALS OF THE EUROPEAN COMMUNITIES OR OFFICIALS OF MEMBER STATES OF THE EUROPEAN UNION

Convention drawn up on the basis of the Treaty on EU on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union (Treaty on EU on the fight against corruption, 1997). The Convention entered into force on 28 September 2005 and all EU countries have acceded to it. This regional international legal instrument deals with criminalization of active and passive crimes of corruption committed by Community public official or Member State officials. By definition, "Public official" by the Convention means a European or national official, including any national official of another EU country. "European official" means also any person who is an official or other contract staff member within the meaning of the EU Staff Regulations, as well as any person seconded to the EU by EU countries or any public or private body performing functions equivalent to those performed by EU officials or other servants. "National official" means an official or public officer as defined by the national law of the EU country in which the person in question performs that function for the purposes of application of the criminal law of that EU country. "Active corruption" means the intentional act of a person who promises or gives, directly or through an intermediary, any advantage to an official, for himself/herself or for a third party, to act or refrain from acting in accordance with his/her duty or in the performance of his/her functions in violation of his official duties. "Passive corruption" under the Convention means the reckless act of an official who, directly or through an intermediary, seeks or receives any advantage for himself/herself or a third party, or accepts a promise of such an advantage, to act or refrain from acting in accordance with by his/her duty or in the performance of his/her functions in violation of his official duties. The text of the Convention implies the application of the principle of assimilation, which should oblige the member States to apply the same descriptions of corruption to national and public officials of the Community. According to the Convention, sanctions against perpetrators of the criminal offences must be effective, proportionate and dissuasive. For the establishing of jurisdiction member States may took over the legal solutions provided for in the Convention on the Protection of the European Communities' Financial Interests. It means that the judicial authorities of a member States may prosecute corruption cases on a territorial and personal basis or through the application of the protective principle. It is important to note that member States may adopt internal legal arrangements which go beyond the obligations set out in the Convention.

INTER-AMERICAN CONVENTION AGAINST CORRUPTION

The Convention was adopted on 29th March 1996 and entered into force on 6th March 1997 under the inter-governmental framework of the Organization of American States (I.L.M., 1996: 724-734). The Convention obliges states to implement a number of measures in their judicial systems and public policies that include prevention, criminalization, assistance and international cooperation. These measures were supposed to establish the mechanisms necessary to prevent, detect, prosecute and eradicate corruption, especially those related to the performance of public functions. According to the Convention, the "public function" means any temporary or permanent, paid or honorary activity, performed by a natural person in the name of the State or in the service of the State or its institutions, at any level of its hierarchy. "Public official" is defined as any official or employee of the State or its agencies, including those who have been selected, appointed, or elected to perform activities or functions in the name of the State or in the service of the State, at any level of its hierarchy. Corruption under the Article 6 of the Convention means the following acts: seeking or accepting, by a government official or a person performing public functions, any object of monetary value or other benefit, in exchange for any act or omission in the performance of his public functions; offering or giving to a civil servant or a person performing public functions, any object of monetary value, or other benefit, in exchange for any act or omission in the performance of his public functions; any act or omission in the performance of his duties by a state official or a person performing public functions for the purpose of unlawful gain for himself or for a third party; fraudulent use or concealment of property arising from any of the foregoing acts and participation as a principal, co-principal, instigator, accomplice or accessory in the execution or attempted execution, cooperation or conspiracy to commit any of the above acts. The Article 8 of the Convention covers acts of transnational bribery and illicit enrichment. Transnational bribery by definition implies "the offering or granting, directly or indirectly, by its nationals, persons having their habitual residence in its territory, and businesses domiciled there, to a government official of another State, of any article of monetary value, or other benefit, such as a gift, favour, promise or advantage, in connection with any economic or commercial transaction in exchange for any act or omission in the performance of that official's public functions". Illicit enrichment is formulated in Article 9 as the "significant increase in the assets of a government official that he cannot reasonably explain in relation to his lawful earnings during the performance of his functions". In view of the criminal offenses described above, the Convention requires States to adopt appropriate measures and legislation, as well as to strengthen mutual cooperation in order to prevent, detect, investigate and punish acts of corruption in accordance with the Convention. For the purposes of international

assistance and cooperation provided under this Convention, each States may designate a central authority or may rely upon such central authorities as are provided for in any relevant treaties or other agreements. Establishment of an institutional system for combating corruption at the national level according to Article 3 of the Convention includes establishing and strengthening general standards of conduct of public officials, adequate mechanisms for their implementation, providing instructions to government staff to ensure proper understanding of their responsibilities and ethical rules governing their activities, revenues, assets and liabilities of persons performing public functions, establishing fair, transparent and efficient public procurement and employment systems, ensuring an efficient system of state revenue control, laws denying favorable tax treatment or corporations for expenditures made in violation of anti-corruption laws, establishing a system of state protection officials and citizens in good faith, report corruption, establish oversight bodies and mechanisms to prevent, detect, punish and eradicate corruption, deter from bribery of domestic and foreign government officials, ensuring mechanisms for controlling the operations of public companies, encouragement of officials, such as mechanisms to ensure that public enterprises and civil society and NGOs engage in anti-corruption activities; and study the further application of preventive measures. The Convention deals with matters of jurisdiction in Article 5. This provision defines that each Contracting Party shall adopt such measures as may be necessary to establish its jurisdiction over offenses. The Convention adopts the personal principle according to which the States Parties will be competent to prosecute corruption when this offense is committed by one of its nationalities or by a person who habitually resides in its territory. Also, like other international legal instruments, this Convention accepts the territorial principle for determining criminal jurisdiction when it determines that States Parties may have jurisdiction when the alleged criminal is present in its territory and does not extradite. Also, the Convention does not preclude the application of any other rule of criminal jurisdiction established by a State Party under its domestic law. In any case, however, this does not mean that the State will be able to circumvent the principle of representation that derives from the customary rule: *aut dedere, aut judicare* (Stessens, 2001: 923) The Article 15 of the Convention specifically obliges States to provide the widest possible assistance with regard to measures for the identification, search, freezing, seizure and confiscation of property or proceeds derived from or used in the commission of corruption offenses. In doing so, the State conducting the enforcement procedure may, in accordance with its own legislation, dispose of such property or may transfer part or all of the property to another State which assisted in the basic investigation or procedure.

THE AFRICAN UNION CONVENTION ON PREVENTING AND COMBATING CORRUPTION

The Convention was adopted on 11 July 2003 at the AU Summit and entered into force on 5 August 2005 (ILM, 2005: 1-17: Schroth, 2005: 24-38). The Convention promotes the development of anti-corruption mechanisms, cooperation in combating corruption, coordination of policies and legislation of the contracting States, removal of obstacles to the enjoyment of basic human rights and freedoms, as well as fostering transparency and accountability in the management of public affairs. Like other previously analyzed international legal instruments, this Convention does not contain a comprehensive definition of corruption, but therefore uses an enumerative method to list acts that may constitute corruption. These offenses and related offenses include bribery (active and passive) in the public and private sectors, any acts or omissions in the performance of duties for the purpose of unlawful gain, trading of influence, diversion of property by public officials, illicit enrichment, use or concealment of proceeds from the acts listed in the Convention as well as money laundering. The Convention criminalizes these acts of corruption and related offences. It also obliges States Parties to adopt legislative and other preventive measures in the public and private sectors in order to combat these acts of corruption in an efficient and timely manner. According to the Convention, the perpetrators of the criminal offense are principal, co-principal, agent, instigator and accomplice, accessory after the fact, in a conspiracy to commit the enumerated acts. The Convention may also be applied to any other acts or practices of corruption and related offenses not described in the Convention on a reciprocal basis agreement of two or more states (Gebeye, 2011: 60). Although the Convention brings some striking innovations in international anti-corruption efforts, in particular by linking corruption and human rights (e.g. through a fair trial provision involving the application of the African Charter on Human Rights), it is interesting that it does not provide any remedy aggrieved individuals or groups of individuals could seek adequate protection of their rights through compensation or restitution. However, Article 16 of the Convention contains a solution according to which the contracting states are obliged to adopt legislative measures for the search, seizure, freezing, confiscation and repatriation of corruption. States are required to cooperate in recovering funds derived from corruption, even if extradition is not possible. This solution strengthens the cross-border fight against corruption, and provides significant funds for the future economic development of damaged countries. Jurisdiction for the prosecution of acts covered by the Convention is determined by Article 13 and it implies the application of the territorial, personal and protective passive principle. In addition, the application of the *ne bis in idem* rule is guaranteed. Extradition under the Convention presupposes the existence of bilateral treaties and agreements between States. In their absence, the

Convention itself is considered to constitute a sufficient legal basis for extradition for the acts covered by it. In each individual case, account should be taken of the solutions present in the internal legal order of States. The Convention elaborates on various types of mutual legal and international cooperation and the establishment of a Follow up mechanism in the form of an Advisory Committee on Corruption, whose tasks under Article 22 is to promote, encourage and implement anti-corruption measures throughout Africa (Olaniyan, 2004: 74-92)

FINDINGS

The previous analysis shows that in the international legal field, international organizations such as the United Nations, the Council of Europe, the Organization for Economic Cooperation and Development, the Organization of American States and the African Union, play a key role in legislation and codification of rules and legal standards on the fight against corruption. The reasons for this action of international organizations are certainly motivated by the fact that corruption is a serious international problem that hinders sustainable economic development, good governance, rule of law in many countries, and erodes other important social and democratic values. The finding arising from the analysis of conventions and other international legal acts of these international organizations suggests that these legal instruments are in fact guidelines for amending and harmonizing the domestic legislation and legal practice of State Parties. As some of these conventions are of the universal and others of the regional type, they are in principle binding *inter partes,* which does not mean that the rules in them do not have an *erga omnes* character. This certainly does not mean that corrupt crimes will fall under the jurisdiction of international courts (Starr, 2007: 1257-1314; Stephenson & Schütte, 2019). Also, considering the differences in determining illegal actions that fall under the concept of corruption (starting with traditionally accepted acts of corruption, bribery, abuse of office, illegal financing, embezzlement of public funds, theft of public property, fraud and extortion to nepotism, cronyism, clientelism and trade in interests), it is clear that these conventions contain many similarities and common features manifested through the criminalization of active and passive bribery, incrimination of legal entities, promotion of international cooperation and enforcement of effective criminal sanctions, which include, *inter alia,* the identification, seizing and confiscation of proceeds from corruption. In addition to the mandate provisions, which stipulate that States must take certain measures and provide for certain anti-corruption solutions, the conventions also include a number of dispositive provisions that contain obligations that States should undertake or consider. Namely, such provisions stipulate that the State Parties will consider the possibility of adopting certain preventive measures or

taking actions and assessing whether those measures or actions would be in accordance with the national legal system. This finding can be useful for the consistent incorporation of international anti-corruption standards into national legislation, in order to avoid situations where corrupt acts are treated unequally due to the application of different legal standards at the national level, which may be crucial for their incrimination and punishment especially when corruption acquires transnational characteristics (Shevchuk, 2010). Thus, for example, by applying the standards present in the OECD Convention against Bribery, States may opt for a much narrower approach that requires only the incrimination of active bribery. On the other hand, if States implement standards from some other international legal instruments, such as the Criminal Law Convention on Corruption of the Council of Europe, then they will sanction various corruption offences with their internal legislation. As corruption offences take on more and more forms of transnational organized crime in modern conditions, conventions have established mechanisms to monitor their implementation (for example, the Conference of the States Parties to the United Nations Convention against Corruption is established to improve the capacity of and cooperation between States Parties to achieve the objectives set forth in this Convention and to promote and review its implementation; the OECD Working Group on Bribery oversees implementation of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions through a peer review process; the Group of States against Corruption - GRECO is a monitoring mechanism for the implementation of the Criminal Law Convention on Corruption and the Civil Law Convention on Corruption of the Council of Europe, which works closely with the EU Commission to develop a comprehensive anti-corruption policy applicable in the territory of the member States). Various forms of international cooperation should lead to the improvement of the fight against corruption not only at the legislative (preventive) level, but also at the repressive level, which implies institutionalized mechanisms of international police and judicial cooperation. In this regard, the EU is a good example of establishing new institutional mechanisms of cooperation at the supranational level, such as the European Public Prosecutor's Office, the Agency for Cooperation in Criminal Matters (EUROJUST), the Agency for Police Cooperation (EUROPOL) and the European Anti-Fraud Office (OLAF) (Trifunović-Stefanović, 2020: 37-56; Jovašević, 2008: 207-228).

ORIGINALITY/VALUE

Over the past decades, the world has been plagued by a series of complex, corruption scandals perpetrated by transnational organized networks involving the public and private sectors. In practice, these networks often operate simultane-

ously in the legal and illicit spheres, with some linked to the highest levels of government, resulting in a loss of state resources. In general, such a situation has led to a breach of public confidence in democracy and the rule of law. At the same time, the weakening of institutions and governance structures provided an opportunity for the emergence of new forms of corruption with a relatively low risk of detection through independent investigation and prosecution. Given that corruption can contribute to the unequal distribution of social wealth at the local and international level, its impunity can lead to new social divisions, which in turn can lead to new looting of national resources, which usually cause conflicts and political instability (Arafa, 2021; Fuentes, 2010). Thus, in some cases of systemic corruption, market destabilization and economic depression occur, contributed to by transnational organized crime, money laundering, terrorist financing, illegal arms proliferation and environmental degradation. All this directly affects the population and their basic human rights and fundamental freedoms and provokes open insurgency and revolution, which has a negative impact on the preservation of international peace and security (Working Group on Corruption and Security, 2014: 12-15; Peters, 2015; Dimitrijević et. al., 2007). Although corruption exists in rich and poor countries, it is more pronounced in the latter where the nature, extent and dynamics of corruption are very different (Graycar, 2015: 87-96). In this regard, broad corrupt networks are characteristic of underdeveloped, transitional and post-conflict countries that crave investment and financial capital, where public services have eroded or lagged behind, where there is no developed infrastructure, health and education system, where the administration is not built, in which clientelism, nepotism, cronyism and kleptocracy reign, i.e. where corruption, as a rule, includes government officials, political leaders, civil servants at all levels of government, then representatives of the private sector and members of criminal syndicates whose activities span continents. The consequences of corruption are detrimental in many respects, so that they can undermine the ability of governments to serve the general public interest, lead to irregular funding of political parties, concealment of real corporate property, threaten, harass and harm victims, key witnesses, whistleblowers, investigators, journalists, prosecutors and judges, then prevent the work of civil movements and non-governmental organizations, free media, with visible political patronage, finally, lead to the consolidation of corrupt individuals and groups in all branches of government (Ware &. Noone, 2005: 30-45). In the context of these consequences and the United Nations data that at the global level "the cost of corruption is at least 5% of global GDP", it becomes much clearer why there has been a significant increase in activities on the prevention and punishment of corruption at the international legislative level and why key international organizations are dealing with this topic today (Connors, 2022: 963-964; Nicić & Arsenijević, Momčilović, 2020: 15; Dimitrijević, 2011: 319-321). Preliminary analysis of legal standards contained in international conventions and

other international legal instruments of international organizations indicates the importance of their incorporation into the domestic legislation of the States Parties as well as their effective, inclusive and sustainable implementation in fluctuating State and inter-State practice. Non-application or inconsistent application of these legal standards at the national and international level can lead to the above-mentioned negative consequences of corruption, which should not be justified by lack of operational capacity or political will to conduct complex and multidisciplinary prosecutions, as well as to conduct efficient and effective criminal sanctions against the perpetrators of these illegal acts. This conclusion has value in itself, as well as the fact pointed out in the analysis of the importance of consensual establishment of mechanisms for monitoring the implementation of obligations under conventions by States, then the establishment of various bodies for international judicial and police cooperation, encouraging anti-corruption initiatives international financial institutions (e.g. World Bank) and NGO's (e.g. Transparency International), which shows a sincere commitment to strengthening the fight against corruption and encourages the competent national institutions to act in accordance with the principles of transparency, accountability and integrity, which are basic preconditions for developing any democratically stable, economically and environmentally sustainable societies (Johnson & Sharma, 2004; Wouters, Ryngaert & Cloots, 2013: 1-76; Dimitrijević & Todić, 2014; Kerusauskaite, 2018). Finally, the entire international community has a shared responsibility to effectively address the challenges and risks of corruption at the national, regional and global levels, by strengthening knowledge, sharing and coordinating and promoting innovative legal approaches in solving the problem of corruption (United Nations, 2021: 16; Kimberly, 1997: 175).

REFERENCES

Additional Protocol to the Criminal Law Convention on Corruption**,** European Treaty Series, 2003/191.

African Union Convention on Preventing and Combating Corruption. (2005). ILM, 43(1): 1-17.

Arafa, M.A. (2021). Between Impunity and Imperialism: The Regulation of Transnational Bribery. *Laws,* MDPI, 10(53).

Balmelli, T., Jaggy, B. (Eds) (2004). *Les Traités Internationaux contre la corruption: L'ONU, l'OCDE, le Conseil de l'Europe et la Suisse,* Lausanne: Interuniversitaires Suisse.

Chance, C. (2019). An International Guide to Anti-Corruption Legislation. London: Cliford Chance LLP.

Connors, R.F. (2022). In the global fight against corruption, transnational bribery is still winning. *Seton Hall Law Review*, 52: 963-964.

Convention on Transnational Organized Crime. (2000). GA RES/55/25, A/C.3/51/7; I.L.M., 2001, 40(2). 334-394.

Council of Europe Civil Law Convention on Corruption, European Treaty Series, 1999/174.

Council of Europe Criminal Law Convention on Corruption, European Treaty Series, 1999/173.

Council of Europe Explanatory Report to the Criminal Law Convention on Corruption, Strasbourg, 1999.

Council of the European Union Act of 26 July 1995 drawing up the Convention on the protection of the European Communities' financial interests. (1995). OJ C 316/48.

Degan, V.Đ., Pavšić, B. & Beširević, V. (2011). *International and Transnational Criminal Law*, Belgrade: Faculty of Law, Union University, Official Gazette.

Dimitrijević, D. & Đorđević, S. (2011). The Law of International Treaties. Belgrade: Institute of International Politics and Economics.

Dimitrijević, D. & Todić, D. (2014). Priority goals in international co-operation of the Republic of Serbia in the field of environment and sustainable development. *International Enviromental Agreeements:Politics, Law and Economics,* Springer, 14: 163-179.

Dimitrijević, D. (2018). Money laundering and terrorist financing on international and national legal level. In: *Thematical Proceedings Archibald Reiss Days.* Belgrade: University of Criminal Investigation and Police Studies.

Dimitrijević, V., et al. (2007). International Human Rights Law, Belgrade: Belgrade Center for Human Rights.

Directive 2017/1371 of the European Parliament and of the Council on the fight against fraud to the Union's financial interests by means of criminal law. (2017). OJ L 198.

First Protocol to the Convention on the protection of the European Communities' financial interests. (1996). OJ C 313.

Fuentes, L.A.T. (2010). Corruption and Inequality in the European Union. *Revista de Estudios Sociales,* 37(106).

Gebeye, B.A. (2011). Rethinking international anti-corruption conventions: advancing corruption-free service as a human right. Addis Ababa: Addis Ababa University, School of Law.

Graycar, A. (2015). Corruption: Classification and analysis. *Policy and Society*, 34: 87-96.

Harvard Law and International Development Society. (2014-2015). Issues in Combatting Transnational Corruption. Cambridge: LIDS Global.

Inter-American Convention Against Corruption. (1996). OAS AG/RES 1398 (XXVI-0/96); I.L.M., 1996, 35(3): 724-734.

Johnson, R.A., Sharma, S. (2004). About Corruption. In: Johnson, R.A. (Ed.), *The Struggle against Corruption: A Comparative Study,* London: Palgrave Macmillan.

Jovašević, D. (2008). Corruption in International and Comparative Criminal Law. *Gazette of the Bar Association of Vojvodina,* (4/5), 207-228.

Kerusauskaite, I. (2018) *Anti-Corruption in International Development,* London: Routledge.

Kimberly, A.E. (1997). Corruption as an International Policy Problem: Overview and Recommendations. In: Kimberly A.E. (Ed.), *Corruption and the Global Economy.* Washington: Institute for International Economics: 175.

Nicholls, C. et al. (2005). *Corruption and the Misuse of Public Office*, Oxford: University Press. Paras. 1.01; Llamzon, A.P. (2014). The Nature of Transnational Corruption. In: *Corruption in International Investment Arbitration,* Oxford: University Press.

Nicić, J., Arsenijević, Momčilović A. (2020). The concept of corruption and anti-corruption mechanisms. In: *Manual for the Legal Clinic for Anticorruption*, Belgrade: Faculty of Law.

OECD Convention Combating bribery of foreign public officials in international business transactions, OECD document DAFFE/IME/BR (97)20; I.L.M., 37(1): 1-11.

OECD Glossaries, 2008: 12.

Olaniyan, K. (2004). The African Union Convention on Preventing and Combating Corruption: A critical appraisal. *African Human Rights Law Journal,* 4(1): 74-92.

Peters, A. (2015). Corruption and Human Rights, Basel Institute on Governance, *Working Paper*, 20.

Recommendation for Further Combating Bribery of Foreign Public Officials in International Business Transactions. (2021). OECD. Accesed on 17 June 2022. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378.

Resolution 97/24 of the Committee of Ministers of the Council of Europe on The Twenty Guiding Principles for the Fight against Corruption, 6 November 1997.

Resolution (99)5 of the Committee of Ministers of the Council of Europe: Agreement Establishing the Group of States against Corruption, 1 May 1999.

Razzante, R. (2020). The Fight Against Corruption. In: Razzante, R. (ed.), Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support, IGI Global, Bogna, 2020: 170

Schabas, W. A. (2004). An Introduction to the International Criminal Court. Cambridge: University Press: 66.

Schroth, P.W. (2005). The African Union Convention on Preventing and Combating Corruption, *Journal of African Law*, 49(1): 24-38.

Second Protocol of the Convention on the protection of the European Communities' financial interests (1997). OJ C 221.

Shevchuk, S. (2010). Rule of Law: Combating Transnational Crime and Corruption. OSCE Report, AS(10)RP 2 E, Oslo.

Simović, M.N., Šikman, M. (2017). *Criminal law response to serious forms of crime.* Banja Luka: Faculty of Law.

Starr, S.B. (2007). Extraordinary crimes at ordinary times: International justice beyond crisis situations. *Northwestern University Law Review,* 101(3): 1257-1314.

Stephenson, M.C., Schütte, S.A. (2019). *An International Anti-Corruption Court? A synopsis of the debate,* Bergen: Chr. Michelsen Institute.

Stessens, G. (2001). The International Fight Against Corruption, General Report. *International Review of Penal Law,* 72(3): 923.

Treaty on EU on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union. (1997). OJ C 2-11.

Treaty on the Functioning of the European Union. (2012). OJ C 326.

Trifunović-Stefanović, M. (2020). European standards in the fight against corruption. In: *Manual for the Legal Clinic for Anticorruption*, Belgrade: Faculty of Law.

UN Office on Drugs and Crime. (2004). The Global Programme against Corruption, UN Anti-Corruption Toolkit, Vienna: United Nations.

United Nations Convention against Corruption, 2349 UNTS 41, 2003.

United Nations Declaration against Corruption and Bribery in International Commercial Transactions. (1997). UN Doc. A/RES/51/191.

United Nations. (2021). The UN common position to address global corruption - towards UNGASS 2021, New York: United Nations.

Ware, G.T. &. Noone, G.P. (2005). The Anatomy of Transnational Corruption. *International Affairs Review.* 4(5): 30-45.

Working Group on Corruption and Security. (2014). *Corruption - The Unrecognized Threat to International Security,* Washington: Carnegie Endowment for International Peace.

Wouters, J., Ryngaert, C., & Cloots, A.S. (2013). The International Legal Framework Against Corruption: Achievements and Challenges. *Melbourne Journal of International Law,* 14: 1-76.

HISTORICAL DEVELOPMENT OF THE POLYGRAPH - APPLICATION OF THE POLYGRAPH IN HUNGARY, STATE AND PERSPECTIVE

Árpád Budaházi, PhD[1]
Faculty of Law Enforcement, University of Public Service, Budapest, Hungary

INTRODUCTION

The best known and most widely used method of instrumental confession testing is the polygraph.The polygraph, a widely used tool in the field of law enforcement, is frequently touted as being able to detect truthfulness and/or deception of suspects, victims, witnesses, and informants (Lewis & Cuppari, 2009). The modern polygraph is 100 years old, born in 1921 in the United States of America. Polygraph is a Greek word meaning "more writing". The name also refers to a multichannel instrument that simultaneously measures several physiological changes in the human body and records them on a computer hard disk. In the past, the curves were drawn on paper with a pencil, but now computer recording is commonplace. In order to be used as a polygraph, a device must have at least three units capable of measuring biological parameters: a pneumograph (a unit measuring respiratory variation), a sphygmograph (a unit measuring blood pressure variation) and a GBR (a unit measuring the electrical resistance or conductivity of the skin).

Today's modern devices have at least four channels, i.e. they are capable of recording four physiological parameters. They measure:

1. changes in respiration (deflections of the chest wall and the flow characteristics of inhaled and exhaled air);

2. changes in respiration (abdominal wall deflections and the characteristics of the flow of expired and inhaled air);

1 budahazi.arpad@uni-nke.hu

3. changes in the electrical resistance or conductivity of the skin (with electrodes placed on the fingers or palms);

4. changes in blood pressure/pulse rate (using a blood pressure cuff on the upper arm).

It is also possible to measure other parameters:

5. the volume of blood flow through the periphery (plethysmogram) is recorded with a photoelectric sensor attached to the fingers;

6. the subject's motion activity is detected by sensors placed under the legs, on the armrests or on the cushion of the test chair. (Budaházi et al., 2021)

The polygraph examiner uses the various sensors and the software available to draw conclusions about whether the examinee is honestly answering in the negative (no) to the closed questions asked.

PURPOSE

This paper aims to show the role of the polygraph in detection and evidence. The paper focuses on applying the polygraph in Hungary and takes into account foreign practices. The paper will show the advantages and limitations of the method and how it has evolved over the last 100 years.

DESIGN/METHODS/APPROACH

The paper will primarily review domestic and foreign literature and analyze domestic legal norms. It also illustrates the experience of using polygraphs through case studies.

FINDINGS

John Larson (USA) first used the modern three-channel polygraph in 1921 in the United States of America. Over the last 100 years, the instrument and the testing methodology have undergone significant changes. The instrument was first used in Hungarian criminal cases in 1978. Initially, the polygraph oriented the investigation, and the test results were not included in the investigation file. Later on, the polygraph test results became part of the investigation file, and there were also court judgments that referred to the polygraph test results as evidence. Nowadays, polygraph examinations are not used as evidence in Hungarian court practice.

The paper wants to demonstrate that it is sufficient for the polygraph to orient the investigation.

ORIGINALITY/VALUE

The paper may contribute to changing the way polygraphs are used and perceived. Monitoring changes could be the subject of other papers.

HISTORY OF THE MODERN POLYGRAPH

The need to test the sincerity of a confession using an instrument was formulated in the 19th century. This century saw the disappearance of lie detection methods with mystical or torturing elements. The void left was filled by the precursors of the polygraph. One of the first to attempt to create a lie detector was the French cardiovascular physiologist Étienne-Jules Marey (Silverman, 1996), who studied blood circulation and then created an instrument that measured pulse. He connected the pressure measuring capsule (the rubber tube) to a writing device in his instrument, called the sphygmograph. The instrument detected the arterial pressure over time and transformed it into a curve written on paper. The test result was recorded in a register showing the measured pulse changes. The instrument could also be used to test respiration variations. (Silverman, 1996) In 1882, Charles Verdin's lie detector was invented, which also measured pulse (Bunn, 2012). In 1893, Rudolf Rothe also made an instrument to test blood pressure, pulse, and respiration. (Rothe, 1893)

Lombroso, a forensic physician in Turin, concluded the falsity of a confession from changes in blood pressure, body part volume, and physiological changes (Agárdi & Kármán, 1999). Initially, Lombroso used the hydrosphygmograph to try to detect crimes. His instrument was a blood pressure monitor, but in 1893 he adapted Marey's sphygmograph; in 1895 he produced his lie detector. In one of his examinations, he used the instrument to determine that the suspect had not committed the 20,000 franc train robbery but had stolen passports and documents. When the suspect heard the latter question, his blood pressure started to drop. That was a sign that the suspect might have committed the crime (Matte, 1996). Lombroso's instrument, the hydrosphygmograph, can be considered the forerunner of the plethysmograph used in modern polygraphs (Ash, 1991). The Italian physiologist Mosso concluded from his research that fear of being found out increases the heart rate (Matte, 1996). He created an instrument which he called a "scientific cradle". It used a large bowl resting on a transverse axis. That offered the possibility to study the state of equilibrium of a person. The subject was placed

on the cradle and stimulated with a fear word discovered during the study of his history, causing the cradle to swing in the direction of the head (Szijártó, 1990).

The Italian psychologist Benussi studied breathing (Krapohl & Shaw, 2015). He believed that fear of exposure would cause a change in breathing when lying (Galianos, 2022). In 1914, Benussi's experiment was based on the idea that the duration of inhalation and exhalation could be used to detect lying. It had been known before that a given emotional state affected breathing cycles, but serious experiments were not carried out until 1914. Benussi created a fictitious testimony situation: the experimenter had to play the role of a witness in an imaginary court. He was given a card on which letters and numbers were written. The subject had to make a false or true statement about the contents of the cards. Whoever played the role of the judge asked whether the card contained letters or numbers, and finally the witness had to read out what the card said. If his task was to lie, he had to give false answers, but he had to make his lie appear authentic. The judge involved in the experiment could only tell whether the witness was telling the truth or lying by his or her behavior. However, the experimenter gave his or her opinion by graphing the breathing. He showed that the discrepancy between the cycles of inhalation and exhalation was mainly after the false statement. This experiment was repeated several times by Harold Burt, Landis, and Gulette, obtaining the same result as Benussi had done earlier (Szíjártó, 1990). The American psychiatrist Münsterberg was also involved in the development of the instrument. He realized that certain physiological changes accompanying lie (deception) are symptoms of the emotions accompanying lie.

He believed that the examination of measurable physiological changes in the body, such as pulse, blood flow, skin resistance, and respiration, could answer the question of whether the suspect had committed the crime (Andreassi, 2007). In 1908, English cardiologist James Mackenzie created the ink polygraph (Inbau, 1953), which he used to test the reactions of cardiovascular patients, their pulse, and blood pressure (Kerekes, 2022).

THE BIRTH OF THE MODERN POLYGRAPH

In 1921, the instrument that can indeed be called the polygraph was born. John Larson, a California police officer and medical student at the University of California, developed the first polygraph that could be considered modern, simultaneously measuring blood pressure, heart rate, and respiration (International League of Polygraph Examiners, 2022). Larson is also known as the father of the polygraph who developed the test of relevant-irrelevant questions (Newton, 2008). The polygraph test involved asking the subject relevant and irrelevant ques-

tions. These questions required a yes or no response from the subject. The relevant question was the question about the commission of the crime. The expert asked whether the subject had committed the crime. The irrelevant question was a question that was not related to the crime. Larson inferred guilt if the subject's body responded to the relevant question in a manner detectable by the polygraph. Larson tested the polygraph on Vollmer, the head of the Berkeley police force, and on the staff in the spring of 1921. The results of the experiments convinced Vollmer that Larson's instrument had great potential. Soon after, he put the invention to practical use: he was able to identify the perpetrator of a series of thefts on the campus of the University of California (Fisher, 2018), and he was able to select the thief from among 38 college girls (Grubin & Madsen, 2005). The priest was suspected of having been murdered. A few days later, a local baker found a body on the beach, which turned out to be that of the priest. The discovering witness was keen to know if he was entitled to a reward for his work as a tracker. However, the authorities used the polygraph to determine whether the witness could be involved in the homicide. The polygraph indicated a lie. The results were communicated to the baker, who confessed (Slavikovic, 2006).

The use of the fourth channel, measuring the skin electrical resistance, was a novelty of the modern Keeler polygraph. In 1939, Keeler attached a galvanograph to blood pressure, pulse, and respiration measuring device. With this instrument, it was possible to measure the psychogalvanic response systematically. The research on the electrical resistance of the skin began in the 19th century.

In 1888, Féré led the investigation of bioelectric phenomena, which led to the conclusion that the skin has electrical resistance. A weak current was passed through the forearm of an experimental subject and a galvanometer was connected to the circuit, allowing the skin resistance to be measured. With Jackues-Arséne d'Arson, Tarchanoff hypothesized that the skin resistance was caused by the stimulation of certain glands (Widacki, 2015). In such small circuits, stimulation of the sensory organs or activation of brain activity induces detectable changes (Szíjártó, 1990). In 1897, Sticker discovered galvanometric responses to stimulation of the brain. He believed that galvanic skin resistance changes occur when the subject is asked questions or shown images that evoke an emotional response (Gordon, 2017). Veragouth linked this to Jung's association vocabulary in 1907 (Green, 2018). Ten years later, Marston used this method in lie detection. In 1915, while still a psychology student, Marston began to study the periodic changes in blood pressure that occurred when lying (Greely & Illes, 2007). Marston's instrument was completed in 1914 and was used during the interrogation of spies during World War I (Granhag & Strömwall, 2009). Keeler polygraph was widely used by the US counterintelligence community during World War II and was a significant factor in the spread of the Keeler polygraph (Larin, 1982). In 1948, Keeler established the world's first polygraph school in

Chicago, where many later prominent polygraph examiners learned the test skills (Volyk 2018). Keeler is also credited with having developed the polygraph questioning technique, which at that time consisted solely of alternating relevant and irrelevant questions, further in the 1920s. He invented the card test in which the subject had to choose a card and used the polygraph to determine which card the subject had drawn (Alder, 2022). The card test was intended to convince the subject that he could be exposed (Alder, 2007). Keeler used the polygraph successfully in several cases, e.g. he investigated Virgil Kirkland, whose polygraph test results also proved that he had murdered his girlfriend, Arlene Draves (The Pittsburgh Press, 1981). He also used the instrument on Joseph Walker, the murderer of an 18-year-old woman (Kerekes, 2022). In addition to solving cases, Keeler is known for his work on the investigation of the US military personnel accused of crimes after World War II (Fisher, 2018), and his investigations contributed to the acquittal of dozens of defendants. (Budaházi, 2014)

IMPROVEMENTS TO THE MODERN POLYGRAPH

In 1945, Reid added another channel to the Keeler four-channel polygraph, and the instrument became capable of measuring muscle activity. Reid created a particular photoluminescent device to detect and measure the arm and leg movements of the subject. He discovered that voluntary muscle movement could influence the measured values (Agárdi & Kármán, 1999).

Reid also improved Keeler's questioning technique, developing the Control Question Test (Furedy & Heslegrave, 1998) in 1947, a major advancement in the polygraph testing methodology (Galianos, 2022). Whereas previously relevant and irrelevant questions had been asked, Reid wedged between these questions the so-called 'control' question, which is a question about the subject's history that would be unpleasant for the subject if not denied. He denies having committed the offense in question (Did you ever steal anything at your previous job?). If his/her body reacts more strongly to the control question than to the relevant one, it can be concluded that he/she has not committed the crime for which the polygraph test is being carried out. In its early usage, this question was often referred to as a 'control' question; today, it is simply called a 'comparison' question (Horvath, 2020).

First among these technical issues is the development by John E. Reid (1947) of what he referred to as the 'comparative response question'. In 1959, David Lykken created the Concealed Information Test (Lykken, 1959). A key question and irrelevant questions are used, e.g. suppose the authorities know that the victim was poisoned. In that case, a question on the method of killing by poisoning is asked as a key question, and irrelevant questions on different methods of killing are also

asked - does the person know that the victim was strangled, shot, stabbed, etc. The test can be used if the person denies that he or she is the perpetrator of the crime or knows anything about how the victim was killed. If the subject responds to the question with strangulation as the method of killing, it can be concluded that the subject is being tested as a person who, despite his/her denial, knows the method of killing. This finding may be reinforced by the results of the Comparison Question Test when the subject responds to the question by being asked whether he or she has committed the crime. Both the Comparison Question Test and the Concealed Information Test are still used today as polygraph examination.

A further advance was the introduction in the 1960s by Cleve Backster of the numerical assessment (Matté, 1996), which is still used today (Grubin & Madsen, 2005). Numerical assessments determine whether the respondent honestly denies having committed the crime or has any information about the case. The numerical assessment further objectifies the polygraph methodology by providing elaborate scoring criteria. In the late 1970s, Joseph F. Kubis, a researcher at Fordham University in New York, pioneered computer applications in the paper on the polygraph curve. Kubis expected computerized polygraph testing to bring additional objectivity (Matté, 1996).

These years marked the beginning of the era of the analog polygraph on the road to the digital instrument. In the early 1980s, John C. Kircher and David C. Raskin at the University of Utah researched the computerized polygraph. In 1988, the Computer Assisted Polygraph System was developed, which included the first algorithm used to evaluate psychophysiological data collected for diagnostic purposes. In 1992, the polygraph officially entered a new era, the computer age, meaning that modern digital technology replaced analog (Alder, 2022). In the beginning, the Stoelting and Lafayette polygraph systems were the market leaders (Kerekes, 2022) and are also used in our country. Nowadays, Axiton and Limeston have also caught up with them competitively. In the last decades, polygraph testing has made significant strides in human development, transparency, and recognition worldwide (Gárdonyi, 2020). The polygraph should not be used as a tactical bluff or psychological pressure because while there were examples of this in the past, it is now outdated.

THE PLACE OF THE POLYGRAPH EXAMINATION IN THE PREPARATORY PROCEDURE AND THE INVESTIGATION

In Hungary, the preparatory procedure precedes the investigation. The purpose of the preparatory procedure is to examine whether there is a suspicion of a criminal offense. If the authority concludes that there is a suspicion at the end of the prepa-

ratory procedure, an investigation is opened. In the preparatory procedure, concealed means may give rise to the polygraph examination. A confidential person may be subject to the polygraph test, who free of charge or in return for a fee, provides information to the authorities concerning a criminal offense. However, it is questionable whether it is worthwhile to the polygraph the information provided by a person of trust, as this could also entail the risk that the person providing the information does not feel the relationship of trust between him and the authority and therefore does not provide the authority with the information at other times.

Th polygraph test has its place both in an investigation detection and investigation phases (Budaházi, 2013). In the detection phase, it can assist in identifying the perpetrator, where the polygraph examines the witness to determine whether the perpetrator may have committed the crime. In Hungary, the detection phase ends with the questioning of the suspect. Therefore, the investigation phase may include the polygraph examination of the suspect to check whether he or she is the perpetrator of the crime. The investigation phase may also include the polygraph examination of the witness when there is doubt as to whether the witness knows what he or she has told the authorities about the case or whether he or she was not the perpetrator of the crime. The authority may order the polygraph examination ex officio and on request (Horgos, 2021), but the consent of the person to be examined is required for the examination to be carried out. Without consent, the examination is prohibited. The polygraph may examine adult witnesses and adult suspects. The counselor shall note the examination, which shall form part of the investigation file.

Both at the discovery stage and during the investigation, the polygraph examination result alone is insufficient to either suspect or terminate the investigation; other data are needed to make these decisions.

THE POLYGRAPH EXAMINATION AND THE COURT PHASE

In Hungary, the polygraph examinations cannot take place in court proceedings. That does not mean that a note containing the polygraph examination results cannot be made part of the trial material. The court may refer to the result of the polygraph examination in the reasoning part of its judgment. According to the opinion of the Budapest Regional Court of Appeal (Fővárosi Ítélőtábla) No. 5/2014 (IX.29.), the result of the polygraph examination does not constitute an evidentiary instrument. "Its role in advancing the investigation is indisputable. However, precisely the result of the polygraph examination may lead to the discovery of material evidence or document or the interrogation of another witness.

The polygraph examination is not an 'evidence gathering' exercise but a verification of the credibility of the evidence from the evidence" (Belegi, 2018).

In Hungary, in the early 2010s, there were court decisions that considered the results of the polygraph examinations as evidence corroborating a confession. Since 2014, however, it has been observed that the courts have repeatedly referred to the fact that the polygraph examinations are not listed as an evidentiary tool and therefore cannot be considered as evidence. The result of the polygraph examination can be used to confirm or weaken the sincerity of a confession. The answer to whether direct evidence is derived from the instrumental test is no since the expert cannot comment on the facts to be proved, so what he or she says is not evidence of the act of guilt (Bejczi, 2013). In the case of the polygraphs, the expert can comment on whether the physiological changes in the subject's reactions indicate deception in denying the relevant questions, e.g. whether he or she deceptively denied having committed the crime or whether his or her body reacted to the questions that would lead to the conclusion that he or she knew about the crime, e.g. the polygraph test will show that the subject gave a deceptive answer when denying knowledge that he or she had been stabbed in the abdomen), (Gálig, 2011). The relevant questions used in the polygraph test also include the facts to be proved since questions about the facts to be proved are also asked (e.g. the body was embedded by the subject), i.e. physiological response changes reveal knowledge of the facts. In one disappearance case, e.g. the Comparison Question Test yielded the result that "the lover killed the missing woman and knows where she is at the time of the investigation", (Krispán & Pusztai, 2016). Furthermore, the Concealed Information Test revealed the homicide (the woman was strangled) and the way the body was hidden (the "buried in concrete" question elicited the most substantial effect from the respondent but also attracted the attention of the buried and hidden in a building option), (Krispán & Pusztai, 2016). Such expert findings are of great importance because the investigator often only suspects that a homicide may have occurred when the place where the body was hidden may be questionable. In the case shown as an example, the polygraph examination also resulted in the exact location of the body's concealment being determined and, as in many cases, the body was recovered and a confession was obtained as a result of the polygraph examination, meaning that the polygraph method gained more evidence for the criminal case.

POLYGRAPH LIMITATIONS

The inherent limitations of the polygraph subjects can make it difficult for the polygraph examination to be effective. If the investigating authority using polygraphs is being investigated, it may be problematic if the investigator has little experience

with polygraphs (Budaházi, 2015). This inexperience and incompetence are because the number of the polygraph cases in Hungary is less than 1% of all criminal cases, so the investigator rarely comes into contact with the polygraph. Inexperience may result in the investigator not timing the use of the polygraphs correctly. The investigator needs to find the ideal time to carry out the test depending on the purpose for which he is using the instrument. Sometimes the polygraph is used too soon - if the investigation had been conducted for two or three more days, the consultant could have asked better questions during the polygraph examination. It is also a problem if the exhausted subject is examined after a lengthy interrogation. Concentration may not be sustainable, so the use of the polygraph is not recommended. Insufficient knowledge of the subject may also be a limitation. The investigator should assess beforehand whether the subject is fit to be tested and whether he or she is in a suitable mental or health condition. The investigator should also know whether the subject will agree to undergo the polygraph examination. Inadequate investigation can also make the polygraph examination difficult. On the other hand, insufficient thoroughness may lead to inaccuracies, which may result in the wrong questions being asked by the investigator to the subject because of inadequate investigative data. Providing more investigative information than necessary to the subject will not help the polygraph examination.

The polygraph examiner is an essential subject in the polygraph examination. The more investigative numbers the consultant has behind him/her, the more likely he/she is to conduct a good quality and effective examination. That also depends on the subject, but generally, a counselor with more experience is very likely not to make mistakes in the assessment and ask the right questions. There is also a problem of inexperience if the counsellor does not notice if the subject tries to manipulate the test. Unpreparedness is also a barrier. The counselor is unprepared if he or she does not spend sufficient time studying the investigation file and formulating the right questions. It is a problem if the counselor is overworked and has to wait a long time to complete the polygraph examination. The requirement for appropriate timing may be compromised.

As humans are being tested by the polygraph, this fact alone may be a limitation. There are times when the subject is unfit for the polygraph examination. The subject's unfitness may be due to his or her medical condition (e.g. asthma attacks, circulatory problems), intellectual (e.g. inability to interpret the questions asked), and self-awareness (e.g. psychopathy). Anyone who has used drugs, taken sedatives, or is sleep deprived before the test is unsuitable. They will also not be tested if, e.g. a pregnant woman is to be tested so as not to endanger the health of herself or her unborn child. Lack of fear of exposure may also render the subject unfit to be examined, as may a confession. This is a problem because the test methodology is based on the exposure of the person in denial by the instrument. The subject

denies having committed the crime and denies having certain information about the circumstances in which the crime was committed (Budaházi et al., 2020).

Non-cooperation with the investigation is a barrier to the use of the polygraph. Refusal to consent can be made before the investigating authority or the polygraph examiner. Wherever the subject does not consent to the examination, the polygraph examination cannot be carried out.

The most commonly used test in the polygraph examinations is the Comparison Question Test (CQT). Whether the polygraph subject is a witness or a suspect, this test can be used. A limitation of the CQT is that the polygraph examiner must properly construct the questions. The examinee should be afraid of being exposed to the relevant or the comparison question. It is also a problem if the examinee answers yes to the relevant question. That is, he or she admits to having committed the offence. In this case, the polygraph examination cannot be continued. If the person answers yes to the comparison question, another comparison question must be asked. The other limitation of the Concealed Information Test (CIT), which is often used, is that it is mostly used with witnesses. The use of CIT on a suspect is infrequent. When the authority communicates the text of the suspect's statement to the suspect, it shares information with the suspect that relates to the circumstances of the commission of the crime. What information is given should not be included in the CIT questions. The suspect may know information from the case file, the media, or the authorities should not be part of the CIT. His body can only recognize the concealed information because he is the perpetrator. If the person conceals the source of information under investigation, the polygraph examination may even produce erroneous results. The subject is not responding to the question because he committed the crime but because he has obtained the information from another source. CIT is more common in the case of a witness, but the abovementioned problems also need to be considered. In his case, it is advantageous that he may have little information about the case from the authorities from case files because his rights of access to the case are considerably more limited than those of the suspect.

A limitation of the polygraph method is that it is not 100% accurate, it is costly to use, and it can never be excluded that the subject will not manipulate the polygraph examination.

SOME EXAMPLES FROM ABROAD

In the birthplace of the polygraph, the United States of America, a Supreme Court decision was handed down in 1923 in Frye v. the United States. The court ruled that the results of the polygraph test could not be used as evidence in court be-

cause they had not yet reached a scientific level of sophistication among psychologists (Frye v. United States, 293 F. 1013 (D.C. Cir. 1923)). The polygraph used at the time was rudimentary, William Martson did not use Larson's polygraph, and he only tested blood pressure. He measured Frye's blood pressure after the questions were asked. For nearly 70 years, the US courts have relied on this ruling in refusing to admit the polygraph test results into evidence (Kelly, 2022). Although the court in the Frye case did not consider Marston's test as evidence, it did not sentence the defendant to death, meaning the polygraph impacted the case. It was not until the late 1970s that references to the Frye case began to disappear. The first step in this process was the 1976 Supreme Court ruling that the polygraph results could be circumstantial evidence. Subsequently, on 20 July 1977 (V KZ 54/77) and 6 May 1983 (IV KR 74/83), the Supreme Court obliged the authorities to evaluate the expert's opinion in criminal proceedings in the light of modern science. California, the Supreme Court classified polygraph tests as communicative or confirmatory evidence because the measurement of changes in bodily functions can be designed to elicit essentially confirmatory responses (Kertész, 1991). Finally, in its decision of 5 November 1999 (V KKN 440/99), the Supreme Court ruled that the method itself must have sufficient reliability about the reliability of the polygraph test (Zubanska, 2009).

The polygraph examinations have been part of the everyday work of the criminal police in Serbia for the last four decades. During that time, polygraphy has found its place and earned the trust of detectives working in the field. Investigation lead and support of polygraphists are of great value for solving severe crimes of all kinds (Kolarević, Matejić, Koljić & Kojić, 2011). As for the Republic of Serbia, the polygraph is often used in police investigations to verify and check the suspects' statements to eliminate the possibility of the implication of innocent people as suspects (Baić, Ivanović & Oljača, 2018).

The first polygraph - a six-channel Stoelting - arrived in Bulgaria in 1968. This instrument was for the needs of Bulgarian intelligence to develop a system for training in deceiving the polygraph. In 1972, Bulgaria bought another Stoelting Ultrascribe. After creating a laboratory (and later institute) of psychology at the Ministry of the Interior, all polygraph experiments were conducted there. After 1997, the use of the polygraph increased considerably. In the following years, the polygraph examination became decisive in resolving many criminal cases - murder, serial assaults, robbery, and burglary. In 1999, the first results from polygraph examinations were presented before the court. They were presented as "psychological expertise for the investigation of truthfulness". This is the only legal way to introduce the polygraph examination in the court system since Bulgaria, until this day, has no law on the usage of the polygraphs (Vladimirova & Todorov, 2020).

In the 1970s, the polygraphs began to be used in Poland to examine people suspected of committing ordinary crimes, mostly homicide. As much as in the 1970s and 1980s the polygraph examinations were used in Poland mostly in criminal cases, today such examinations are but a few percent of all the procedures. A great majority of examinations are performed for pre-employment and screening purposes (Widacki, 2020). Since the breakdown of the USSR, more polygraph examinations have been conducted in Russia, Ukraine, Belarus, Kazakhstan, other Asian republics of the former USSR, and China than in the US, Latin America, and Europe. These examinations are performed both for the organs of the states, and in private business for pre-employment and screening purposes. There is much to suggest that such examinations are abused, and their quality raises doubts (Widacki, 2020). The Polish Supreme Court made it clear that the polygraph is not a test of truthfulness or a lie detector. Evidence from an opinion of an expert witness in the field of the polygraph examinations is indirect evidence, i.e. evidence that leads only to findings based on which conclusions about the main fact can be drawn by way of reductive reasoning (Kury & Redo, 2021).

The use of the polygraph test results in court was initially considered "unconstitutional" by the German Federal Court of Justice in a famous ruling in 1954. However, it was later seen as merely "not suitable" in 1998. While the broader public still perceives the polygraph testing as being prohibited for court use, there is in fact a small group of practitioners who conduct the lie detection tests as part of court proceedings. However, this practice is little known and hardly ever talked about in public. Unlike other countries where polygraph testing is a practice used by the police or in probation services, it is pretty much limited to the field of legal psychology in Germany. It is essential to highlight that the legal situation prohibits using the polygraph for a confessional motivation (as it is used in e.g. the United States), and it may not be used to someone's disadvantage. Today, the polygraph testing in the German court system lives a niche existence, but one that is seen to be of great potential by those involved (Paul, Fischer & Voigt, 2020). The polygraph test in Germany although producing material and visual results is classified as part of expert testimony and cannot be treated as independent evidence. (Paul, Fischer & Voigt, 2020)

The polygraphs are used in many countries around the world to orientate investigations. Typically, a court may take note of the results of the polygraph examination. We believe the place to carry out the polygraph examination is in the investigation.

CONCLUSION

The modern polygraph has undergone many changes over the past 100 years. The 3-channel polygraph has become capable of measuring new channels, and the test methodology has changed. The test structures have changed, the digital polygraph has replaced the analog polygraph, and numerical evaluation has been introduced. The polygraph is generally a good orientation for the investigation, but the polygraph is not a panacea, and there are potential errors. Despite its limitations, the polygraph has proven over the past decades that it is worthwhile to proceed with it rather than without it in criminal cases if the case is suitable for the polygraph use. In our view, the polygraph examination has its place in the investigative phase and is most useful for detection. The aim is to assist in the identification of the perpetrator. It is crucial that the use of the polygraphs is voluntary and should not be used anywhere in the world without consent. There is no reason for the results of the polygraph examination to become evidence; it is sufficient to serve as an orientation for the investigation.

REFERENCES

Agárdi, T. & Kármán, G. (1999): A hazugságvizsgálatról más szemmel. *Belügyi Szemle,* 47(10), 92–106.

Alder, K. (2007). America's Two Gadgets: Of Bombs and Polygraphs. *Isis,* 98(1), 124–137.

Alder, K. (2022) The Lie Detectors, Downloaded June 20. 2022 www.kenalder.com/liedetectors/portrait.htm

Andreassi, J. L. (2007). *Psychophysiology: Human behavior and physiological response.* Mahwah: Lawrence Erlbaum Associates.

Ash, P. (1991). *A History of Honesty Testing*. In J. W Jones (Ed.), *Preemployment HonestyTesting: Current Research and Future Directions.* New York: Quorum Books.

Baić, V., Ivanović, Z.& Oljača, M. (2018). Beliefs of Convicts on the Validity of the Polygraph. "Archibald Reiss Days" Thematic Conference Proceedings of International Significance. Belgrade: University of Criminal Investigation and Police Studies, 237-246

Bejczi, A. (2013). Kételyek a poligráfkörül. *Ügyészek Lapja,* 20(3–4), 69–77.

Belegi, J. (2018). A bizonyítás. In J. Belegi (Ed.), *Büntetőeljárás jog I–II. Új Be. – Kommentár a gyakorlatszámára.* Budapest: HVG-ORAC.

Budaházi, Á. (2013). A poligráfos vizsgálat helye a felderítésben és a vizsgálatban. *Belügyi Szemle*, 61(11), 90-111.

Budaházi, Á. (2014). *Poligráf. Műszeres vallomás-ellenőrzés a bűnügyekben.* Budapest: NKE Szolgáltató Kft.

Budaházi, Á. (2015). Testing Procedure of the Polygraph Examination. *Studia Universitatis Babes-Bolyai Iurisprudentia,* 2(4-6), 190-207.

Budaházi, Á., Fantoly, Zs., Kakuszi, B., Bitter, I. & Czobor, P. (2021). *A műszeres vallomás-ellenőrzés fejlődési irányai.* Budapest: Ludovika Egyetemi Kiadó.

Bunn, G. C. (2012). *The Truth Machine: A Social History of the Lie Detector.* Baltimore: The Johns Hopkins University Press.

Dag Kolarević, Mirko Matejić, Goran Koljić & DejanKojić (2011). Efficiency of Polygraph Techniques Using Experiment in Serbia. "ARCHIBALD REISS DAYS" THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE. Belgrade: University of Criminal Investigation and Police Studies, 343-350.

Fisher, J. (2018) The Polygraph Wars. DownloadedJanuary 20. 2018 http://jimfisher.edinboro.edu/forensics/polywar1.html

Furedy, J. J. & Heslegrave, R. J. (1988). Validity of the Lie Detector: A Psychophysiological Perspective. C*riminal Justice and Behavior*, 15(2), 219-246.

Galianos, J. (2022) Brief History of the Polygraph. Downloaded June 20. 2022 http://home.total.net/~galcar/html/brief_history_of_the_polygraph.html

Gálig, P. (2011): A kihallgatás etikája és taktikája. Downloaded June 20. 2022 www.jogiforum.hu/files/publikaciok/galik_peter__a_kihallgatas_etikaja_es_taktikaja[jogi_forum].pdf

Gárdonyi, G. (2020). A poligráfos vizsgálat jogi és szakmai környezetének változásai, a szakterület kihívásai. *Rendőrségi Tanulmányok*, 3 (1), 82-92.

Gordon, N. J. (2017). *Essentials of Polygraph and Polygraph Testing.* Boca Raton: CRC Press.

Granhag, P. A. &Strömwall, L. A. (2009). The Detection of Deceit. In N. Kocsis, R. (Ed.), *Applied Criminal Psychology: A Guide to Forensic Behavioral Sciences.* Springfield: Charles C Thomas Publisher.

Greely, H. T. &Illes, J. (2007). Neuroscience-Based Lie Detection: The Urgent Need for Regulation. *American Journal of Law & Medicine,* 33(2–3), 377–431. DOI: https://doi. org/10.1177/009885880703300211

Green, C. D. (2022) Classics in the History of Psychology. Downloaded June 20. 2022 http://psychclassics.yorku.ca/Jung/Association/lecture1.htm

Grubin, D. – Madsen, L. (2005). Lie detection and the polygraph: A historical review. *Journalof Forensic Psychiatry & Psychology,* 16(2), 357–369. DOI: https://doi.org/10.1080/14789940412331337353

Horgos, L. (2021). *A ius puniendi jogállami tartalmának kiteljesedése.* In Cs. Szabó & D. Molnár (Eds.), Studia Doctorandorum Alumnae. Válogatás a DOSz Alumni Osztály tagjainak doktori munkáiból. II. kötet (pp. 11-260). Budapest: Doktoranduszok Országos Szövetsége.

Horvath, F. (2020). A Hundred Years of Polygraphy: Some Primary Changes and Related Issues. *European Polygraph* 14(1), 30-43.

Inbau, F. E. (1953). The First Polygraph. *Journal of Criminal Law and Criminology,* 43(5), 679–681.

International League of Polygraph Examiners (2018) *Polygraph/Lie Detector FAQs.* DownloadedJanuary 20. 2018 www.theilpe.com/faq_eng.html

Kelly, D. M.. Polygraphs ("Lie Detectors"). DownloadedJune 20. 2022 http://criminal.findlaw.com/crimes/more-criminal-topics/evidence-witnesses/polygraphs-lie-detectors.html

Kerekes,T. (2022) A poligráf használatának története fényképeken. Downloaded June 20. 2022 https://prezi.com/pde5-6t1lf-z/a-poligrafos-vizsgalatok-tortenete-kepekben/

Kertész, I. (1991). A poligráfos vizsgálat helye a büntetőeljárásban. II. rész. *Főiskolai Figyelő,* 3(1), 3–19.

Krapohl, D. & Shaw, P. (2015). *Fundamentals of Polygraph Practice.* San Diego: Academic Press.

Krispán, I. & Pusztai, L. (2016): Egy gyanús eltűnés poligráfos vizsgálatának módszertana és tanulságai. *Belügyi Szemle,* 64(7–8), 141–150.

Kury, H. & Redo, S. (2021). *Crime Prevention and Justice in 2030. The UN and the Universal Declaration of Human Rights.* Cham, Switzerland: Springer.

Larin, A. M. (1982). Poligráf és személyiségi jogok a büntetőeljárásban. *Magyar Jog,* 29(4), 354–358.

Lewis, A. J. & Cuppary, M. (2009). The Polygraph: The Truth Lies within. *The Journal of Psychiatry & Law,* 37(1), 85-92.

Lykken, D. T. (1959). The GSR in the Detection of Guilt. *Journal of Applied Psychology,* 43(6), 385–388. DOI: https://doi.org/10.1037/h0046060

Matte, J. A. (1996). *Forensic Psychophysiology Using the Polygraph: Scientific Truth-Verification – Lie Detection.* Williamsville – New York: J. A. M. Publications.

Newton, D. E. (2008). *DNA Evidence and Forensic Science*. New York: Infobase Learning.

Paul, B., Fischer, L. & Voigt T. H. (2020). Anachronistic Progress? User Notions of Lie Detection in the Juridical Field. *Engaging Science, Technology, and Society* 6, 328-346.

Rothe, R. (1893). *Specialitäten physiologischerApparate: Preliminary catalog.* Prag: Hofbuchdruckerei A. Haase.

Silverman, M. E. (1996). Etienne-Jules Marey: 19th Century Cardiovascular Physiologist and Inventor of Cinematography. *Clinical Cardiology,* 19(4), 339–341. DOI: https://doi.org/10.1002/clc.4960190412

Szíjártó, I. (1990). *A pszichofiziológiai (poligráf) vizsgálat és eredményeinek felhasználási lehetősége az életelleni bűncselekmények felderítésében.* Tansegédlet. Budapest: Rendőrtiszti Főiskola.

Szlavikovics, I. G. (2006). A poligráf alkalmazásának lehetőségei és korlátai. In T. Drinóczi (Ed.), Studia Iuvenum Iurisperitorum 3. *A Pécsi Tudományegyetem Állam- és Jogtudományi Kara hallgatóinak tanulmányai*, 3, 316-339.

The Pittsburgh Press 47(21 May 1931) Kirkland loses 'lie detector', 3.

Vladimirova, V. & Todorov, T. B. (2020). The Essence of the Polygraph Method and its Usage in Bulgaria. In T. V. Petkova & V. S. Chukov (Eds), *5th International e-Conference on Studies in Humanities and Social Sciences*. Belgrade: Conference Proceedings, 219-224.

Volyk, A. (2018) History of the Polygraph.DownloadedJune 20. 2022 www.argo-a.com.ua/eng/history.html

Widacki, J. (2018). Polygraph Examination in Poland. History, Law, Experimental Research, and Practice. *European Polygraph,* 12(4), 141-155.

Widacki, J. (2020). A Half-Century of Experiences with the Polygraph. *European Polygraph*, 14(1), 58-61.

Zubanska, M. (2009). Accuracy of Polygraph Testing and its Status as Scientific Evidence. *Internal Security,* 1(1), 51–60.

MOBBING – A HARMFUL PRESENT-DAY PHENOMENON

Mojca Rep
District Court Celje; Higher Court in Ljubljana, Slovenia[1]

DEFINITION OF MOBBING

In the 1990s, the Swedish work psychologist Prof. Heinz Leymann, PhD (1996), who dealt with behavior in the work environment, gave an expert definition of mobbing. Mobbing in the work environment involves hostile and unethical communication by one or more individuals, systematically and most often directed against one individual. Due to mobbing, a person is pushed into a position of helplessness, where they have no protection and where they also remain due to constant acts of mobbing. These acts occur very often, at least once a week, and last for a long time, at least for six months. The definition of mobbing is therefore as follows: "Mobbing is conflict-filled communication in the workplace between co-workers or between subordinates and superiors, where the attacked person is in a subordinate position and exposed to systematic and prolonged attacks by one or more persons with intent and/or exclusion from the system, and the attacked person perceives this as discrimination." Leymann's (2012) definition defines mobbing as a procedural act, and practice seeks to extend the definition to any act of psychological or emotional violence. Due to the above, the correct conclusion is that it is possible to talk about mobbing only when the disruptive act or behavior lasts for a long time and when this behavior includes exposure to psychological and emotional attacks in the workplace. The term "harassment" is usually used to describe this phenomenon. The word means intentionally causing inconvenience, disturbance. From the above-mentioned professional definition and definition of mobbing, it primarily follows that mobbing takes place in a precisely defined social framework, namely at the workplace or in the work environment (Heinz Leymann, 1996). It is typical here that workers work together in organized units with other workers, who are usually not chosen by themselves, but the circle of

1 mojca_rep@yahoo.com

co-workers is predetermined and a worker cannot influence it, but must persevere with co-workers because they work with them and because of any other obligations arising from the employment relationship. Furthermore, mobbing is characterized by a distinction between two groups of roles, namely between superior and subordinate(s), which is not necessarily the same as hierarchical role in the work environment. So it is not necessarily a matter of a relationship of superiority and subordination in the labor law hierarchy. It is essential that a relationship is formed between the subordinate individual and the attacking co-worker(s) or superior(s). It is important that these roles are formed as a rule through the process of mobbing itself, because in the beginning both mobbing participants are often equal participants in the conflict, but later one of them loses control and finds themselves in a subordinate position. Conflict communication is also typical, which can also mean a lack of communication. However, all of the above must be present for a long time and must be systematic. Only in this case can it be said that a certain behavior or behavior is mobbing. In connection with the above, it should be pointed out that in the Slovenian environment in recent years, since mobbing has become an extremely modern term, it is also used unprofessionally and often incorrectly to describe acts and actions other than mobbing. Namely, people try to use the term mobbing to describe all kinds of conflicts in the workplace, even though they do not contain elements of mobbing. For this reason, the author would like to point out that any unjust decision of a superior worker or conflict between co-workers cannot automatically be considered mobbing. Thus, we only talk about mobbing (Leymann, 1996 – 1) when it is a systematic, long-lasting and repetitive behavior (Leymann, 1996 – 1; Rep, 2021) that is directed at only one person, as a result of which the victim loses control and falls into a subordinate position (Leymann, 1996 – 1)

FORMS OF MOBBING

Mobbing is a behavior in which an individual or a group of individuals with a negative impact on another individual trigger a reaction in the latter, which usually has consequences for their efficiency and health. Mobbing can be identified as (Leymann, 1996 – 1):

- behavior and conduct that affects the self-expression and the way the victim is communicating,
- behavior and conduct that restricts and prevents the social contacts of the abused person,
- behavior and conduct that damages the victim's reputation,
- an attack on the quality of the victim's professional and life situation,
- a direct attack on the health of the victim.

In most of the countries where the research took place, mobbing has been shown to be more common in the public than in the private sector, and especially in the fields of education, health care, social work and hospitality (Brečko, 2013, 2021). The data in the figures show that e.g. mobbing is present in public administration at 14%, in education and health 12%, in the tourism sector 12%, in transport and communication 12%, and in trade 9%. Victims are more likely to be employed in larger companies where employers do not have direct control. Women are more likely to be victims, especially younger ones, and men are more likely to be perpetrators. Harassment in the workplace can be encountered at all organizational levels and among the perpetrators are superiors as well as co-workers. So it occurs in the superior-subordinate, co-worker and subordinate-superior relationships (Bohl, 2019). Often there are more persons responsible and in this case the torture lasts longer. The results of the research also show large differences between countries. In Finland, there are e.g. 15% of workers subjected to mobbing, in the Netherlands 14%, in Sweden 12%, in Belgium 11%, in France and Ireland 10%, in Denmark 8%, in Germany and Luxembourg 7%, in Austria 6%, in Greece and Spain 5%. (Eurofound). In Slovenia, only 2.8% of workers surveyed stated that they had been victims of mobbing. According to Daniela Brečko, PhD (2013), who conducted the research in Slovenia, there are obvious cultural differences in tolerance to psycho-terror in the workplace. In Sweden, for example, the day-to-day behavior of a superior delegating tasks to employees in a high-pitched tone is defined as unacceptable and often labelled as an act of mobbing, while in the Mediterranean countries such behavior is tolerated.

CAUSES OF MOBBING

Among the causes, Prof. Heinz Leymann, PhD (1996, 2012) emphasized organizational factors such as work organization, quality of leadership, organizational culture, etc. He rejected the idea that the personality traits of the victim play any role in the emergence and development of workplace harassment. Much more research supports the thesis that workplace harassment occurs in organizational cultures that allow or even reward such behavior. In some organizations, we could also talk about the institutionalization of torture with authoritarian leadership. When we talk about the causes of harassment in the workplace, organizational factors are therefore very important, but we cannot satisfactorily define it without taking into account the personality characteristics of both the perpetrator and the victim, and their impact on the course of harassment.

Causal explanations for workplace harassment should therefore take into account (Leymann, 1996 – 1):

- characteristics of the organization,
- characteristics of the causative agent,

- characteristics of the victim, and
- socio-psychological characteristics of the work environment.

Harassment in the workplace most often occurs in organizations characterized by (Leymann, 1996 – 1):

- a highly competitive work environment with a culture of careerism and a strictly hierarchical structure,
- attention focused exclusively on increasing economic profits or achieving set goals, and not on the working atmosphere and mutual relations between employees,
- high concern over the surplus workforce,
- authoritarian style of leadership and management,
- poor planning of organizational goals and constant uncertainty about their selection,
- poor and inconsistent involvement of employees in decision-making,
- poor opportunities for vocational training and education,
- lack of mutual respect and respect for mutual cultural differences,
- lack of clear rules of work and conduct,
- excessive workload or pointless work tasks,
- insufficiently defined roles and lack of professionalism.

LEGAL REGULATION OF MOBBING

Mobbing is illegal or prohibited at international, European and national level. For example, Article 5 of Council Directive 89/391/EEC of June 12, 1989 stipulates that the employer is obliged to take care of safety and health in all areas related to work. However, the European Social Charter obliges all EU members to protect workers from negative and offensive acts. Article 34 of the Constitution of the Republic of Slovenia stipulates that everyone has the right to personal dignity and security. Article 46 of the Employment Relationships Act – 1 stipulates that the employer must protect and respect the employee's personality and take into account and protect the employee's privacy. Article 47 of the same law stipulates that the employer is obliged to provide such a working environment in which no employee will be exposed to sexual and other harassment or torture by the employer, superiors or co-workers. Mobbing is also mentioned in the general provisions of the Employment Relationships Act – 1, namely in Article 7, according to which sexual and other harassment is prohibited. Sexual harassment is any form of unwanted verbal, non-verbal or physical conduct or behavior of a sexual nature with the effect or intent to harm a person's dignity, especially when creating an intimidating, hostile, degrading, humiliating or offensive environment. Other harassment, however, is any unwanted behavior related to any personal

circumstance, with the effect or intent of affecting a person's dignity or creating an intimidating, hostile, degrading, shameful, or offensive environment. Pursuant to Article 7 of the Employment Relationships Act – 1, harassment at the workplace is also prohibited. Harassment in the workplace is any repetitive or systematic, reprehensible or manifestly negative and offensive conduct or behavior directed against individual workers in the workplace or in connection with work. A worker who is a victim of harassment must not be exposed to adverse consequences as a result of action aimed at enforcing a ban on harassment in the workplace. Article 24 of the Occupational Safety and Health Act – 1 stipulates that the employer must take measures to prevent, eliminate and manage cases of violence, harassment, maltreatment and other forms of psychosocial risk at work that may endanger the health of workers. Failure to do so could result in a fine of 2,000 to 40,000 Euros. Mobbing is also banned in the civil service sphere. Article 15a of the Public Employees Act stipulates that any physical, verbal or non-verbal conduct or conduct of a civil servant based on any personal circumstance and creating an intimidating, hostile and humiliating, shameful or offensive work environment, or offending the person's dignity, is prohibited. Mobbing can also be a crime under certain circumstances. Article 197 of the Criminal Code 2021 stipulates that anyone who humiliates or intimidates another employee at work or in connection with work with sexual harassment, psychological violence, torture or unequal treatment shall be punished by imprisonment for up to two years. If the above-mentioned act results in a mental, psychosomatic or physical illness or a reduction in the employee's work performance, the perpetrator shall be punished by imprisonment for up to three years.

REVERSE BURDEN OF PROOF − THE PROBLEM OF PROOF

The favorable legal circumstance for the worker against whom the mobbing is carried out is that the burden of proving that the mobbing did not take place is on the employer. If, in the event of a dispute, the employee cites facts justifying the presumption that the employer has not provided a working environment in which no employee will be exposed to sexual or other harassment by the employer, superiors or co-workers and that they have not taken appropriate measures to protect workers from such harassment or maltreatment, the burden of proving that no mobbing has taken place is on the side of the employer. If the employee in the dispute cites facts that justify the presumption that the employer did not provide protection against harassment, the burden of proof is that they provided such a work environment in which the employee is not exposed to harassment by the employer, superiors or co-workers (Article 45 of the Employment Relationships Act – 1). But the devil's in the detail; despite the fact that the employer has to prove

that the worker was not exposed to harassment or that they provided such a working environment that the worker was not exposed to harassment, the worker is the one who must first state all the relevant facts that justify the presumption that harassment has occurred. And this is where judiciary have big problems in practice, because in a large number of cases, lawsuits are too general (Rep, 2009). Namely, workers generally state that their employer did not provide them with e.g. work tasks, but do not list specific events. Erjavec is convinced (2018) that the employer defends themselves against the allegations, but also very generally because specific events are not listed. Only then, during the interrogation, do the workers want to testify about concrete cases related to the alleged violation, but they cannot replace the assertion basis with their statement. The Court cannot and must therefore not allow the plaintiff to cite cases where, in their view, there has been torture if they have not previously cited this in their submissions, otherwise the principle of adversarial proceedings is infringed, which means that the defendant, i.e. the employer is not given the opportunity to comment on the alleged infringements. On the other hand, we have lawsuits of more than 100 pages, where the plaintiffs actually describe all the events that are supposed to affect the evidentiary process.

CASE LAW – EXAMPLES

In case law, we would like to mention the judgment and decision Pdp 85/2018 of October 24, 2018 of the Higher Labor and Social Court (2018), in which the court ruled on the very existence or non-existence of mobbing (harassment at work). Namely, it stated that harassment, according to the legal definition, is a recurring or systematic negative treatment of a worker. However, a one-off event (such as an extraordinary termination of an employment contract) does not yet indicate that there has been harassment in the workplace. Very common examples in practice are that the employer deprives the employee of work tasks or no longer provides them with work. In accordance with the provision of Article 41 of the Employment Relationships Act – 1 (2013), the employer is obliged to provide the employee with the work for which they agreed in the employment contract (first paragraph). The employer must also provide the employee with all the necessary resources and work materials that the employee needs in order to be able to fulfill their obligations without interruption (second paragraph). In the judgment of the Higher Labor and Social Court (2010) opr. no. Pdp 41/2010, the court rejected the plaintiff's claim for payment of compensation for mental pain or interference with personal dignity in the amount of EUR 55,454.04. It found that the director of the defendant did not cut off communication with the plaintiff when he took office, that he had not been assigned tasks below the level of professional qualifications, that he had not been prevented from advancing and that his conduct towards

her was not arrogant and irritable. In addition to the fact that the employer does not provide the employee with work, there is also an example when they do not provide the employee with a working space at the same time. From the judgment of the Higher Labor and Social Court (2011) opr. no. Pdp 831/2011 thus follows that failure to provide work, setting up a desk in another department, the fact that the attacked person is constantly under control of who they speak to and what they say, that co-workers avoid them because they were under verbal and psychological pressure from the director (if they talked or listened to them, they would lose their jobs) means signs of psychological violence. As a result, the plaintiff was awarded damages in the amount of EUR 6,000.00.

Transfer to other jobs is often cited as harassment. In the decision of the Higher Labor and Social Court opr. no. Pdp 1297/2006, it is stated that the plaintiff was allegedly subjected to sexual harassment by her superior and was transferred to an inappropriate job due to disobedience. The plaintiff filed a lawsuit against the director of the defendant and the defendant at the same time, jointly and severally demanding payment of damages in the amount of EUR 8,400.00. In this dispute, the Court of First Instance dismissed the claim on the ground that it found that there was no causal link between the first and second defendan's conduct and the plaintiff's state of health, but the VDSS upheld the appeal on appeal. In the judgment of the Higher Labor and Social Court (2010 – 1) opr. no. Pdp 404/2010, however, the plaintiff stated that she had been transferred because she had applied for protection against harassment. At the same time, she claimed that her superior was rudely harassing her, threatening her and spreading untruths about her, and demanded payment of compensation in the amount of EUR 100,000.00, which the court rejected. In this dispute, the court clarified that harassment is when the holder exercises the right with the sole intention of harming another or when the employer conducts proceedings regarding the employee's rights and obligations solely with the intention of harming the employee (the same definition is given in the Maribor High Court (2008), Ref No. Cp 579/2007, stating that harassment means intentionally causing inconvenience, discomfort, neglect, intentionally illegal (corrupt) transfer to a lower post). Mobbing is a case of systematic and prolonged ill-treatment that causes the victim social, psychological and health problems. *Discrimination*, on the other hand, is an act by which an employer puts an employee in an unequal position or grants them less rights and benefits compared to co-workers. The obligation of the employer in accordance with the provision of the first paragraph of Article 45 of the Employment Relationships Act is also to provide such a working environment in which no employee will be exposed to sexual and other harassment or torture by the employer, superiors or co-workers. To this end, the employer must take appropriate measures to protect workers from sexual and other harassment or harassment in the workplace. In this regard, it is necessary to draw attention to the above-mentioned decision of the Higher

Labor and Social Court (2008) ref. no. Pdp 387/2007, in which the Higher Labor and Social Court explained that the defendant acted unlawfully because they did not provide the described working environment or because they did not prevent unwanted behavior. In the judgment and decision of the Higher Labor and Social Court (2009) ref. no. Pdp 945/2008, it is stated that the various pressures exerted by the defendant on the plaintiff (attempt to reassign him, assessment of failure, reduction of salary, accusation of liability for missing inventory, pressure on the attending physician) constitute inadmissible conduct and the defendant is liable for the damage suffered by the worker. In the present case, the court also pointed out that the server on behalf of the defendant had acted inappropriately in the service, as he had pasted a written warning and termination of the employment contract on the door of the plaintiff's residence so that every passer-by could see it. The least you would expect from an employer is to seal the writing in an envelope and not hang it on everyone's door for viewing. From the judgment of the Higher Labor and Social Court (2011 – 2) opr. no. Pdp 1047/2010, it is stated that signs of harassment in the workplace include high-pitched speech, shouting, repeated reminders of mistakes made, derogatory markings of the work done and the remark that the person attacked is a "sheep" or a "wimp", and the defendant was, for allowing such behavior, ordered to pay damages in the amount of EUR 7,250.00. A similar scenario happened with the Higher Labor and Social Court 82007) by the opr. no 814/2007 judgment. The defendant was ordered to pay damages in the amount of EUR 4,041.23 for finding that the defendant did not ensure the protection and respect of the employee's personality at work. It was found that the branch manager, with ridicule and insulting remarks, systematically and continuously attacked the plaintiff and put her in mental distress. Harassment in the workplace is any repetitive or systematic, reprehensible or manifestly negative and offensive conduct or behavior directed against individual workers in the workplace or in connection with work. In this regard, the decision of the Higher Labor and Social Court (2010 – 2) decision ref. No. Pdp 96/2010) is interesting: the provisions of the Employment Relationships relating to the prohibition of harassment in the workplace and the protection of the dignity of the worker at work apply in full. Also in this dispute, the plaintiff filed a claim for damages against the director and the employer and jointly and severally demanded payment of EUR 16,000.00 (or EUR 55,000.00 at first).

In the judgment opr. no. Pdp 694/2011, however, the Higher Labor and Social Court (2011 – 1) stated that if the defendant changed their internal organization and therefore gave the plaintiff regular termination of the employment contract, this does not mean that she was mobbing the plaintiff. Also, failure to follow the employer's proposals does not mean harassment or pressure on workers, nor does it mean confiscating a company car during leave.

CONCLUSION

The phenomenon of mobbing should not be underestimated in any case. The fact is that nowadays many employees are exposed to great, often inhuman burdens and that mobbing is a frequent companion of their work. In addition, in Slovenia, where the system of "balancing" and negative selection is still established in many work environments, mobbing is increasingly being carried out against employees who stand out positively and want to transfer good business practices to those who work poorly, slowly or irresponsibly. Compared to other EU Member States, the legislation in the field of harassment in Slovenia is appropriate and also provides victims of harassment with adequate protection. With regard to the harassment itself, it is essential that the employer does not insult or violently treat the worker. If the employer, despite the employee's warnings, does not prevent such conduct by other employees, the employee is entitled to compensation. However, this compensation must be high enough to recognize both the preventive and punitive function of compensation and not just satisfaction with the injured party. However, it should be emphasized that any alleged unethical behavior does not constitute illegal behavior (mobbing) and that the feeling when someone experiences mobbing is sometimes subjective and deceptive – often the result of personal resentment. Therefore, in assessing whether mobbing takes place in an environment, it is necessary to be precise and, of course, reasonable so that it can separate the wheat from the chaff and be recognized as truly wasteful and socially harmful.

REFERENCES

Brečko, D. (2013). Say no to mobbing, Coping with psychological and emotional violence. Ljubljana, GV Planet.

Brečko, D. (2021). Truths and misconceptions about mobbing. Ljubljana: GV Planet.

Bohl. T. (31. 1. 2019). What is mobbing: definition and manifestations. Accessed on June 5, 2022. https://www.e-kadrovik.si/vsebine/varstvo-pri-delu-in-promocija-zdravja/mobing/kaj-je-mobing-opredelitev-in-pojavne-oblike/

Constitution of the Republic of Slovenia. Official Gazette, nos. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a).

Council Directive 89/391/EEC of June 12, 1989. Official Gazette 393, 30/12/1989 p. 0001 – 0012. Accessed on June 5, 2022. https://osha.europa.eu/en/legislation/directives/the-osh-framework-directive/1

Criminal Code. Official Gazette, nos. 50/12, 6/16, 54/15, 38/16, 27/17, 23/20, 91/20, 95/21 in 186/21.

Eurofound: European research on quality of life (EQLS) European and International cooperation. Accessed on June 5, 2022. https://www.eurofound.europa.eu/sl/surveys/european-quality-of-life-surveys

Erjavec, K. (2018). The case law of labor courts in the field of torture. Commission for the Prevention of Corruption. Accessed on May 4, 2022. www.kpk-rs.si › wp-content › uploads ›

Employment Relationships Act – 1. Official Gazette, nr. 21/13, 78/13, 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS, 81/19, 203/20 – ZIUPOPDVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22 in 54/22 – ZUPŠ-1.

Heinz, L. (1996). The content and development of mobbing at work. Journal of Work and Organizational Psychology, (5)3, 165 – 184.

Heinz L. (1996 – 1). Mobbing and victimization at work. Psychology, Hove.

Heinz, L. (2012). Somatic and psychological symptoms after the experience of life threatening events. A profile analysis, Victimology, 10 – (1,4), 512 – 538.

Public Employees Act. Official Gazette, nos. 63/07, 65/08, 69/08 – ZTFI-A, 69/08 – ZZavar-E, 40/12 – ZUJF, 158/20 – ZIntPK-C,

203/20 – ZIUPOPDVE, 202/21 – odl. US in 3/22 – ZDeb.

Higher Labor and Social Court (2007). Judgement and Decision Pdp 814/2007 issued on October 18, 2007. Accessed on June 5, 2022. https://www.sodnapraksa.si/?q=814/2007%20&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2010040815248760

Higher Labor and Social Court (2008). Judgement and Decision Pdp 387/2007 issued on February 15, 2008. Accessed on June 5, 2022. https://www.sodnapraksa.si/?q=387/2007&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=42747

Higher Labor and Social Court (2009). Judgement and Decision Pdp 945/2008 issued on April 16, 2009. Accessed on June 5, 2022. https://www.sodnapraksa.si/?q=945/2008%20&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=65760

Higher Labor and Social Court (2010) Judgement and Decision Pdp 41/2010 issued on May 6, 2010. Accessed on June 5, 2022. http://www.sodnapraksa.si/?q=id:2010040815248208&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=2010040815248208

Higher Labor and Social Court (2010 – 1). Judgement and Decision. Pdp 404/2010 issued on May 6, 2010. Accessed on June 5, 2022. https://www.sodnapraksa.si/

?q=404/2010&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2010040815252021

Higher Labor and Social Court (2010 – 2). Judgement and Decision Pdp 96/2010 issued on May 6, 2010. Accessed on June 5, 2022. https://www.sodnapraksa.si/?q=96/2010&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2010040815248291

Higher Labor and Social Court (2011). Judgement and Decision Pdp 831/2011 issued on December 20, 2011. Accessed on June 5, 2022. https://www.sodnapraksa.si/?q=694/2011&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2010040815260425

Higher Labor and Social Court (2011 – 1) Judgement and Decision Pdp 694/2011 issued on September 26, 2011. Accessed on June 5, 2022. https://www.sodnapraksa.si/?q=Pdp%20694/2011%20%20&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2010040815260425

Higher Labor and Social Court (2011 – 2). Judgement and Decision Pdp 1047/2010 issued on March 10, 2011. Accessed on June 5, 2022. https://www.sodnapraksa.si/?q=1047/2010&database[VDSS]=VDSS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2010040815253644

Higher Labor and Social Court (2018). Judgement and Decision Pdp 85/2018 issued on October 24, 2018. Accessed on June 5, 2022. http://www.sodnapraksa.si/?q=id:2015081111424771&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=2015081111424771

Rep, M. (2009). Can reverse burden of proof in criminal cases increase trials effectiveness? Criminology and crime policy between human rights and effective crime control, Annual Conference. The European Society of Criminology, Cambridge; The Slovenian Academy of Sciences and Arts, Ljubljana. The Faculty of Law, The Faculty of Criminal Justice and Security, The Institute of Criminology at the Faculty of Law, Ljubljana, p. 92.

Rep, M. (2021). Respect for human rights as an important aspect of the democratic functioning of civil society. Towards a better future: state and society, fourth International Scientific Conference.15–16 October, 2021 Bitola, Republic of North Macedonia, pp 392 -400.

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

343.85:343.9.02(082)
351.74/.76:005.7(082)

INTERNATIONAL scientific conference "Archibald Reiss Days" - Investigating and Proving Contemporary Forms of Crime: Scientific Approaches (2022 ; Belgrade12)

Thematic Conference Proceedings of International Significance / XII International scientific conference "Archibald Reiss Days" - Investigating and Proving Contemporary Forms of Crime: Scientific Approaches, Belgrade, 8-9 November 2022 ; [editor in chief Tanja Kesić]. - Belgrade : University of Criminal Investigation and Police Studies, 2023 (Belgrade : Birograf Comp). - X, 183 str. : ilustr. ; 24 cm

Tiraž 150. - Bibliografija uz svaki rad.

ISBN 978-86-7020-496-6
ISBN 978-86-7020-190-3 (za izdavačku celinu; broš.)

а) Криминалитет -- Сузбијање -- Зборници б) Криминалистика -- Зборници в) Полиција -- Организација -- Зборници

COBISS.SR-ID 113380105