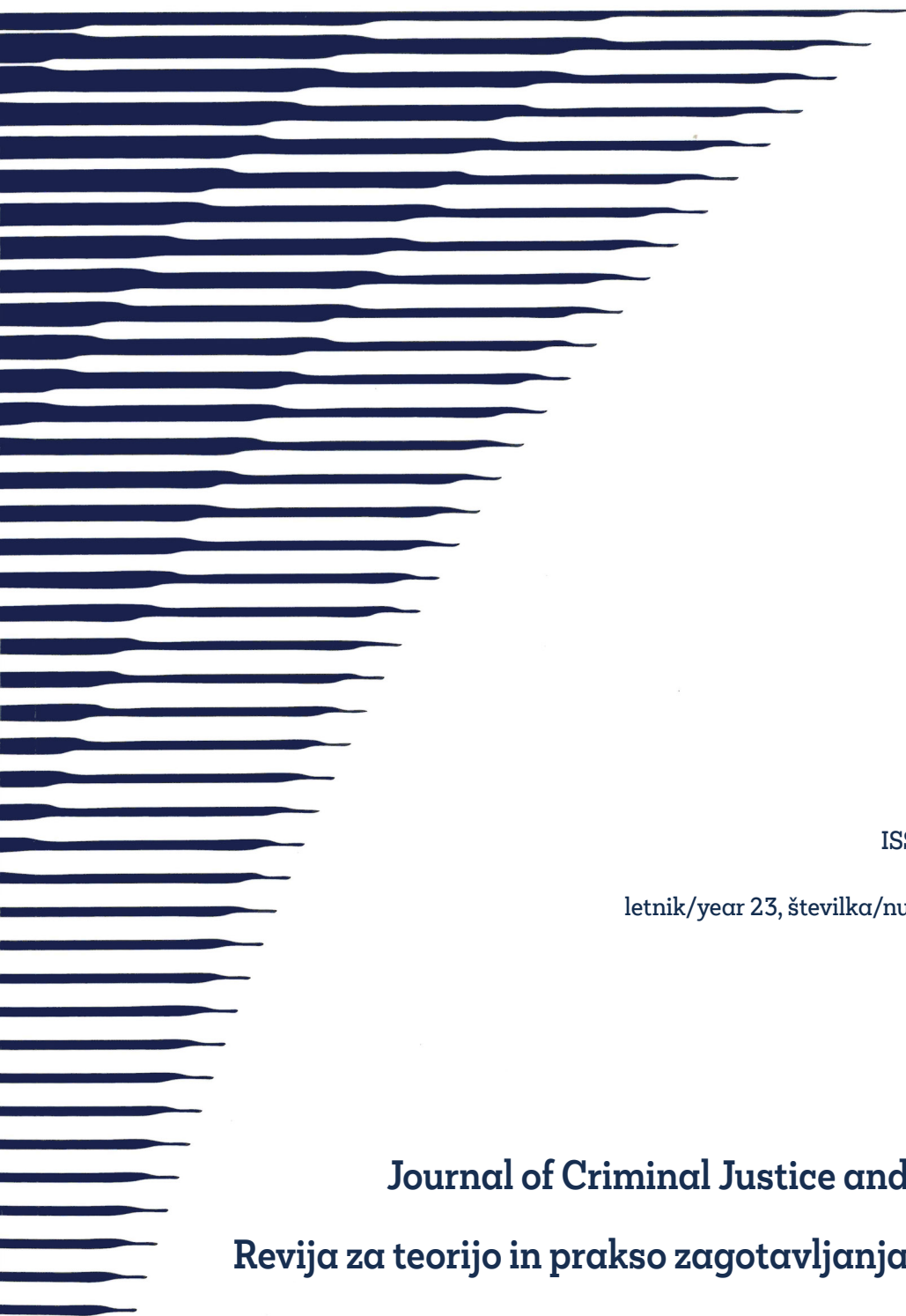


Varstvoslovje



ISSN 2232-2981

letnik/year 23, številka/number 2021/4



Journal of Criminal Justice and Security

Revija za teorijo in prakso zagotavljanja varnosti

O reviji

Varstvoslovje je znanstvena revija, ki spodbuja interdisciplinarno razpravo in izmenjavo ugotovitev s področja proučevanja varnosti. Prizadeva si osvetliti pravne, organizacijske, kriminološke, kriminalitetopolitične, politološke, sociološke, psihološke in druge vidike varnostno relevantnih pojavov in konceptov. Revija prispeva h globljemu razumevanju vloge in delovanja skupnosti, organizacij in posameznikov, ki sodelujejo pri zagotavljanju varnosti.

Primeri tematskih sklopov, ki jih revija pokriva, so:

- teoretične osnove varnosti,
- organizacija in upravljanje varnostnih mehanizmov,
- zatiranje kriminalitete,
- policijska dejavnost,
- zasebnovarnostna dejavnost,
- obveščevalno-varnostna dejavnost in
- informacijska varnost.

Revija Varstvoslovje je odprto dostopna revija in izhaja v skladu s pogoji licence Creative Commons Attribution CC BY 4.0.

Journal of Criminal Justice and Security is an open-access journal, published under the terms of the Creative Commons Attribution licence CC BY 4.0.

Glavni in odgovorni urednik / Editor-in-Chief

Urednik števil v slovenskem jeziku / Editor of Slovene Issues

Urednika števil v angleškem jeziku / Editors of English Issues

Uredniški odbor /Editorial Board

Marcelo Aebi, University of Laussane, Laussane, Switzerland

Igor Areh, Univerza v Mariboru, Maribor, Slovenija

Branko Ažman, Univerza v Mariboru, Maribor, Slovenija

Hans-Juergen Albrecht, Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany

Goran Basic, Linnaeus University, Växjö, Sweden

Igor Bernik, Univerza v Mariboru, Maribor, Slovenija

Tore Bjorgo, Norwegian Police University College, Oslo, Norway

Gleb Bogush, Moscow State University – Lomonosov, Moscow, Russia

Hans Boutellier, Verwey-Jonker Institute, Utrecht, The Netherlands

Aleš Bučar-Ručman, Univerza v Mariboru, Maribor, Slovenija

Jiří Buriánek, Charles University, Prague, The Czech Republic

Bojan Dobovšek, Univerza v Mariboru, Maribor, Slovenija

Ioan Durnescu, University of Bucharest, Bucharest, Romania

Katja Eman, Univerza v Mariboru, Maribor, Slovenija

Chris Eskridge, University of Nebraska-Lincoln, Lincoln, NE, USA

Benjamin Flander, Univerza v Mariboru, Maribor, Slovenija

Loraine Gelsthorpe, University of Cambridge, Cambridge, UK

Peter Grabosky, Australian National University, Canberra, Australia

Beata Z. Gruszczynska, University of Warsaw, Warsaw, Poland

Alistair Henry, University of Edinburgh, Edinburgh, UK

Tim Hope, Keele University, Keele, UK

Djordje Ignjatović, University of Belgrade, Belgrade, Serbia

About the Journal

The Journal of Criminal Justice and Security is a scientific magazine fostering interdisciplinary discussion and exchange of findings in the field of safety and security studies. In its effort to shed light on legal, organisational, criminological, political, sociological, psychological, and criminal-policy aspects of security-relevant concepts and phenomena, it facilitates a deeper understanding of the roles and the functioning of society, organisations, and individuals cooperating in the provision of security.

As such, the Journal of Criminal Justice and Security covers the following thematic areas:

- theoretical foundations of safety and security,
- organisation and management of security mechanisms,
- combating criminality,
- policing,
- private security,
- intelligence and security, and
- information security.



Andrej Sotlar, Univerza v Mariboru, Maribor, Slovenija

Andrej Sotlar, Univerza v Mariboru, Maribor, Slovenija

Branko Lobnikar, Univerza v Mariboru, Maribor, Slovenija

Sanja Kutnjak Ivković, Michigan State University, East Lansing, MI, USA

Zoran Kanduč, Inštitut za kriminologijo, Ljubljana, Slovenija

Klara Kerezi, National Institute of Criminology, Budapest, Hungary

Krzysztof Krajewski, Jagellonian University, Krakow, Poland

Gary LaFree, University of Maryland, College Park, MD, USA

Rene Levy, GERN, Guyancourt, France

Tomaš Loveček, University of Žilina, Žilina, Slovak Republic

Alida V. Merlo, Indiana University of Pennsylvania, Indiana, PA, USA

Mirjam Milharčič Hladnik, Znanstvenoraziskovalni center Slovenske akademije znanosti in umetnosti, Ljubljana, Slovenija

Mahesh Nalla, Michigan State University, East Lansing, MI, USA

Tinkara Pavšič Mrevlje, Univerza v Mariboru, Maribor, Slovenija

Borislav Petrović, University of Sarajevo, Sarajevo, B&H

Paul Ponsaers, Ghent University, Ghent, Belgium

Iztok Prezelj, Univerza v Ljubljani, Ljubljana, Slovenija

Amedeo Recasens i Brunet, CESDIP, Paris, France

Bojan Tičar, Univerza v Mariboru, Maribor, Slovenija

Andromachi Tseloni, Nottingham Trent University, Nottingham, UK

Gregor Urbas, Australian National University, Canberra, Australia

Peter Wetzels, Institute of Criminology, Hamburg, Germany

Sabina Zgaga Markelj, Ustavno sodišče Republike Slovenije, Ljubljana, Slovenija

Editorial353
Uvodnik355

ARTICLES

Anica Ferlin Criminal Liability and Prosecution of Islamic State Fighters in Iraq357
Branko Gabrovec, Tilen Zupan, Srečko Felix Krobe, Branko Lobnikar Police Instruments of Restraint against Persons with Health Problems – Analysis of the Use of Expert Grips and Holds as Forms of Physical Force379
Miha Dvojmoč, Patricija Lunežnik, Kaja Prislan Adoption of Advanced Technological Solutions in Slovenian Private Security Companies402
Žiga Primc The Use of Tools for Obtaining Data From Publicly Accessible Sources for the Purpose of Competitive Intelligence in Enterprises425

Editorial

Dear readers.

We have included four articles in the last 2021 issue of the Journal of Criminal Justice and Security. The articles are very diverse in their content, but they address important content in criminal justice and security studies. The authors address issues of fairness and efficiency in the prosecution of terrorist fighters, the competence of police officers in dealing with aggressive psychiatric patients, the use of advanced technology in private security activities and the importance of competitive intelligence to ensure the efficiency of contemporary businesses. The contents thus range from public policing to private security and corporate security.

In the paper *Criminal Liability and Prosecution of Islamic State Fighters in Iraq*, **Anica Ferlin** summarises the operation of the Islamic State in Iraq and includes a review of law enforcement by the authorities. This paper aims to add to the body of expertise by presenting the measures taken by the authorities to prosecute fighters of this terrorist organisation. The results show that the Islamic State did commit war crimes, crimes against humanity and crime of genocide in Iraq. However, no individual has been held accountable for these crimes at the international level and to date. The paper identifies some shortcomings related to the prosecution of the Islamic State in Iraq. The author indicates the direction of further necessary practical measures that should be taken to guarantee effective and fair prosecution of Islamic State fighters and the limitation of the risk of further radicalisation.

In the paper *Police Instruments of Restraint Against Persons with Health Problems – Analysis of the Use of Expert Grips and Holds as Forms of Physical Force* **Branko Gabrovec**, **Tilen Zupan**, **Srečko Felix Krobe**, and **Branko Lobnikar** aim is to determine the capability of police officers to control violent patients with health problems and analyse the competencies of police officers in controlling violent persons. The specific nature of the situation dictates the need for additional skills and training for the successful implementation of police procedures that do not jeopardise the subsequent treatment procedures with the patient. The authors' analysis has shown the lack of knowledge and skills of police officers in dealing with violent persons who have health issues or are under the influence of drugs or medications, and in addition to that, the police officers are not afforded appropriate training in this field.

Miha Dvojmoč, **Patricija Lunežnik** and **Kaja Prislan** in the paper *Adoption of Advanced Technological Solutions in Slovenian Private Security Companies*, analyse the use of advanced technological solutions in the private security industry. Its primary purpose is to upgrade security services and resolve private security companies' human resource issues. Based on the interviews, the authors concluded that introducing digitalisation into the private security industry could appropriately address the shortage of human resources while also expanding

the products provided by security services. The authors also emphasise that the findings could have implications for **both public and private policing**.

The last paper in the current issue of the Journal of Criminal Justice and Security is written by **Žiga Primc**. Using the systematic review of the literature, the author thoroughly analyses *The Use of Tools for Obtaining Data from Publicly Accessible Sources for the Purpose of Competitive Intelligence in Enterprises*. Over the past decade, obtaining data from publicly accessible sources has developed extremely rapidly, and more effective tools are being developed to automate processes. Existing studies highlight the importance of competitive intelligence activities in companies utilising obtaining data from publicly accessible sources for better decision-making. The author identifies a lack of trained personnel and adequate software systems for optimal business use.

The editorial board hope the readers will find the articles worth reading and a good source of fresh ideas for future research and hopefully new papers.

Prof. Branko Lobnikar, PhD
Editor of English Issues

Uvodnik

Dragi bralci in bralke.

V zadnjo številko revije *Varstvoslovje* za leto 2021 smo vključili štiri članke; le-ti so po svoji vsebini zelo raznoliki, obravnavajo pa pomembne vsebine s področja kazenskega pravosodja in varnostnih ved. Avtorji naslavljajo vprašanja pravičnosti in učinkovitosti pri kazenskem pregonu islamskih terorističnih borcev, kompetence policistov pri obvladovanju agresivnih psihiatričnih bolnikov, uporabe napredne tehnologije pri dejavnostih zasebnega varovanja ter pomena konkurenčne obveščevalne dejavnosti za zagotavljanje poslovne uspešnosti sodobnih podjetij. Vsebine se tako raztezajo od javne policijske dejavnosti do zasebnega varovanja in korporativne varnosti.

Anica Ferlin v članku *Criminal Liability and Prosecution of Islamic State Fighters in Iraq* (Kazenska odgovornost in pregon borcev Islamske države v Iraku) povzema delovanje Islamske države v Iraku in v svojo analizo vključuje pregled kazenskega pregona terorističnih borcev Islamske države. Avtorica ugotavlja, da je Islamska država v Iraku izvajala vojne zločine, zločine proti človeštvu in genocid, vendar na mednarodni ravni do danes za te zločine še ni odgovarjal noben posameznik. Avtorica opozarja na kršitve pravic osumljencev v procesu kazenskega pregona in potrebo po kategorizaciji osumljencev glede na resnost kaznivih dejanj, ki je do določene mere uvedena zgolj v iraškem Kurdistanu, ter tudi na potrebo po reintegraciji borcev Islamske države, tako da je treba poleg kazenskega pregona v dejavnosti vključiti tudi deradikalizacijo.

Branko Gabrovec, Tilen Zupan, Srečko Felix Krobe in Branko Lobnikar v članku *Police Instruments of Restraint Against Persons with Health Problems – Analysis of the Use of Expert Grips and Holds as Forms of Physical Force* (Uporaba strokovnih prijemov pri osebah z zdravstvenimi težavami – policijski vidik) analizirajo mnenja policistov glede njihovih znanj za obvladovanje nasilnega pacienta. Ker obravnava nasilne osebe ni enaka obravnavi nasilne osebe z zdravstveno težavo ali pod vplivom drog oziroma zdravil, je pomembno, da je obravnava takšne osebe drugačna in prilagojena. Na podlagi empirične študije so ugotovili, da je znanje policistov za obravnavo nasilnih oseb, ki imajo zdravstvene težave ali pa so pod vplivom drog oziroma zdravil, pomanjkljivo ter da policisti niso deležni ustreznih usposabljanj. Specifičnost situacije namreč narekuje potrebo po dodatnem znanju in usposabljanju za uspešno izvedbo policijskega postopka na način, da ta ne bo ogrozil kasnejšega tretmajskega postopka s pacientom.

Miha Dvojmoč, Patricija Lunežnik in Kaja Prislan v članku *Adoption of Advanced Technological Solutions in Slovenian Private Security Companies* (Prevzem naprednih tehnoloških rešitev v slovenskih zasebnih varnostnih podjetjih) analizirajo pomen uporabe naprednih tehnoloških rešitev v varovanju kot enega izmed aktualnih razvojnih trendov v sektorju zasebnega varovanja. Ugotavljajo, da uporaba naprednih tehnoloških rešitev predstavlja priložnost za nadgradnjo varnostnih storitev in reševanje kadrovskih težav, s katerimi se soočajo zasebna

varnostna podjetja. Pri tem opozarjajo, da gre za temo, ki je enako pomembna tako za javno kot zasebno policijsko dejavnost.

Zadnji članek *The Use of Tools for Obtaining Data from Publicly Accessible Sources for the Purpose of Competitive Intelligence in Enterprises* (Uporaba orodij za pridobivanje podatkov iz javno dostopnih virov v okviru konkurenčne obveščevalne dejavnosti v podjetjih) v tej številki revije Varstvoslovje je napisal **Žiga Primc**. Namen njegovega prispevka je s pomočjo sistematičnega pregleda literature ugotoviti uporabnost orodij za pridobivanje podatkov iz javnih virov v okviru konkurenčne obveščevalne dejavnosti v podjetjih. V svojem prispevku avtor ugotovi, da obstoječe študije izpostavljajo pomembnost konkurenčne obveščevalne dejavnosti z uporabo pridobivanja podatkov iz javno dostopnih virov za organizacije, hkrati pa ugotavlja pomanjkanje usposobljenega kadra in programskih rešitev za njeno optimalno poslovno uporabo.

V uredništvu upamo, da bodo bralci članke prebrali z zanimanjem in jim bodo predstavljali vir svežih idej za prihodnje raziskave. Upamo, da tudi za nove prispevke v reviji Varstvoslovje.

Prof. Branko Lobnikar, urednik angleških izdaj revije Varstvoslovja

Criminal Liability and Prosecution of Islamic State Fighters in Iraq

VARSTVOSLOVJE
*Journal of Criminal
Justice and Security*
year 23
no. 4
pp. 357–378

Anica Ferlin

Purpose:

This paper summarises the operation of the Islamic State in Iraq and includes a review of law enforcement by the authorities. The purpose of this paper is to add to the body of expertise by presenting the measures taken by the authorities to prosecute fighters of this terrorist organisation.

Methods:

The descriptive research methodology was applied when reviewing primary and secondary sources and to interpret the data obtained from interviews, which provide practical insights into the subject matter.

Findings:

The results show that the Islamic State did commit war crimes, crimes against humanity and crime of genocide in Iraq. However, at the international level and to date, no individual has been held accountable for these crimes. As Iraq is not a partner in certain international instruments, it is not possible to prosecute such acts in the country where the acts were committed. In the absence of a national strategy to prosecute suspected Islamic State fighters, processes under counter-terrorism law are thus being carried out in Iraq. The available data point to violations of the rights of suspects of fair prosecution process and the need to categorise suspects according to the severity of the crimes, which has been introduced to some extent only in Iraqi Kurdistan. In addition to prosecution, de-radicalisation must be included in the process of reintegrating Islamic State fighters into society, and thus procedures to achieve this need to be developed. At the level of society, it is necessary to address risk factors that could lead to radicalisation and to establish mechanisms to detect and prevent it.

Practical Implications:

The paper identifies some shortcomings related to the prosecution of the Islamic State in Iraq, and indicates the direction of further necessary practical measures that should be taken to guarantee effective and fair prosecution of Islamic State fighters, and the limitation of the risk of further radicalisation.

Originality:

The content of the article deals with a relatively poorly researched area and is to some extent based on interviews with government officials in Iraqi Kurdistan

who have highlighted challenges that will need to be addressed in the future.

Keywords: prosecution, war crimes, crimes against humanity, genocide, Islamic State, Iraq

UDC: 343.1:341.322.5(567)

Kazenska odgovornost in pregon borcev Islamske države v Iraku

Namen prispevka:

Prispevek povzema delovanje Islamske države v Iraku in vključuje pregled kazenskega pregona s strani oblasti. Namen prispevka je razširiti strokovno znanje in predstaviti ukrepe, ki jih oblasti izvajajo za pregon borcev te teroristične organizacije.

Metode:

Uporabljena je bila deskriptivna metoda za pregled primarnih in sekundarnih virov ter interpretacijo podatkov, pridobljenih z intervjuji, ki prinašajo praktični vpogled na obravnavano tematiko.

Ugotovitve:

Rezultati kažejo, da je Islamska država v Iraku izvajala vojne zločine, zločine proti človeštvu in genocid. Na mednarodni ravni do danes za te zločine še ni odgovarjal noben posameznik. Ker Irak ni partner v določenih mednarodnih instrumentih, kazenski pregon tovrstnih dejanj ni mogoč v državi, kjer so bila dejanja izvršena. V Iraku se tako izvajajo procesi po protiteroristični zakonodaji, pri čemer je opazna odsotnost nacionalne strategije za pregon osumljenih borcev Islamske države. Razpoložljivi podatki kažejo na kršitve pravic osumljencev v procesu kazenskega pregona in potrebo po kategorizaciji osumljencev glede na resnost kaznivih dejanj, ki je do določene mere uvedena zgolj v iraškem Kurdistanu. V proces reintegracije borcev Islamske države je treba poleg kazenskega pregona vključiti tudi deradikalizacijo. Oblikovati je treba postopke za deradikalizacijo posameznikov in njihovo ponovno vključitev v družbo, na ravni družbe pa nasloviti dejavnike tveganja, ki bi lahko vodili k radikalizaciji, ter vzpostaviti mehanizme za zaznavanje in preprečevanje radikalizacije.

Praktična uporabnost:

Prispevek identificira nekatere pomanjkljivosti, povezane s kriminalizacijo in kazenskim pregonom Islamske države v Iraku, ter nakazuje smer potrebnih nadaljnjih potrebnih praktičnih ukrepov, ki jih bi bilo treba izvesti za učinkovit in pravičen pregon borcev Islamske države ter zmanjšanje tveganja ponovne radikalizacije.

Izvirnost prispevka:

Vsebina prispevka obravnava relativno neraziskano področje in v določenem delu temelji na izvedenih intervjujih s predstavniki oblasti v iraškem Kurdistanu,

v katerih so bili izpostavljeni izzivi, ki jih bo treba nasloviti v prihodnosti.

Ključne besede: kazenski pregon, vojni zločini, zločini proti človeštvu, genocid, Islamska država, Irak

UDK: 343.1:341.322.5(567)

1 INTRODUCTION

Islamic State represents the biggest security threat that the world has faced in recent years or even decades. The world has never seen such a rapid advance of any terrorist organisation, which has seized assets, taken control over territory, key military and economic centres, natural resources and critical infrastructure, and seen great success in spreading its message with the use of social networks. In doing so, it has resorted to extreme violence, with abductions, rapes, beheadings and other criminal acts. The methods used have intimidated opponents and recruited foreign fighters, and resulted in mass killings, forced displacements and conversions, the exploitation of women and children, genocide and other war crimes and crimes against humanity.

Many criminal behaviour theories, such as those set out by Bavcon and Šelih (2003), Masters and Roberson (1990), Hartjen (1978), Meško (2016), and even that by the sociologist Durkheim (1973), who researched crime and deviance as elements of a functional society, could be applied to Islamic State. Comprehensive reviews of the criminalisation and prosecution of Islamic State fighters in Western countries have been carried out by individual authors, who have done research on the criminalisation and prosecution of Islamic State fighters. Such research has mostly focused on the foreign terrorist fighters who travelled from Western countries to Iraq and Syria, from the proclamation of the Caliphate in June 2014 to the present day, and taking into account the risk factors during the active operation of the Islamic State and after its defeat. Fewer studies have focused on the Middle East region and the countries where the Islamic State won the biggest numbers of supporters, along with large territorial and administrative areas and almost unlimited financial resources.

A review of the literature shows that the field is poorly theoretically researched, as research related to the Islamic State is focused mainly on the treatment of foreign fighters and their de-radicalisation upon return to their home states. Many studies and analyses forget about one important element of the process after someone has forcibly or voluntarily left the organisation. While life after leaving the Islamic State should be marked by a process of the de-radicalisation, which has become highly sophisticated in Western countries in recent years, in Iraq and Syria far less work is being done to achieve this. Individuals who are suspected of Islamic State membership are subjected to criminal investigation, prosecution, trial and imprisonment or other form of punishment, and not included in any de-radicalisation programmes.

Since criminal prosecution and imprisonment are the prevailing forms of confronting and managing Islamic State fighters in Iraq, we wanted to analyse the

legislation which could be applied to these cases at the international and national levels. Furthermore, the procedures and some cases of prosecuting Islamic State fighters will be re-examined using the available analyses of international organisations which work in the region. The various human rights violations, war crimes and crimes against humanity that the Islamic State committed during its active years of operation in Iraq have been identified. In this paper, we will focus on genocide, war crimes and crimes against humanity in general, and not specific actions. The paper will analyse the prescribed penalties for those actions and their actual implementation at national and international levels.

The purpose of this article is to add to the body of expertise by reviewing the operation of the Islamic State in Iraq and the crimes committed by its fighters. The aim is to analyse the human rights violations, war crimes and crimes of genocide committed by the Islamic State, at the normative and implementation levels in Iraq and internationally. The potential measures that should be taken by authorities to successfully prosecute Islamic State fighters and prevent and combat further radicalisation will be pointed out. The research questions are as follows: What law enforcement processes are the Islamic State supporters and members subject to internationally and in Iraq? Are there uniform prosecution procedures and punishments for crimes committed by Islamic State at the international level and in Iraq? Is the imprisonment of Islamic State fighters based on the existing legislation sufficient measure to get justice for victims and to reduce the risk of further radicalisation? To answer the research questions, we first analyse Islamic State operations, with an emphasis on Iraq. The article then summarises the international and Iraqi legislation to prosecute crimes committed by the Islamic State, and its implementation based on the cases that have already been carried out in accordance with it. Concluding remarks draw findings on punishment as a possibility for victim recovery, justice and the deterrence of radicalisation.

The methods used to address these issues include analysis of primary and secondary sources. Additionally, some data will be used from four earlier interviews the author conducted for other research purposes with the representatives of military and security-intelligence authorities in Iraqi Kurdistan in 2019 and the director of International Institute for Middle East and Balkan Studies in 2015. Note has to be made that Iraq is a federal parliamentary republic, administratively divided into 18 governorates and one region, the autonomous Kurdistan Region in Iraq with its own separate and autonomous executive, legislative and judicial branch. The analysis within the article applies to Iraq as a whole, with Kurdistan Region included. If they are found, any discrepancies in legislation and its implementation or outstanding findings connected to both entities will be explained in the article.

2 CRIME, WAR CRIMES, CRIMES AGAINST HUMANITY AND GENOCIDE

Human behaviour and operation are led by certain rules established in society. Breaching those rules and operating in socially unusual way means engaging in deviant behaviour, which is perceived as a “socially negative phenomenon”

(Meško, 2016, p. 15). This includes crime, which generally represents behaviours that threaten fundamental human values and are legally defined as criminal acts. Hartjen goes further and identifies five conditions for a criminal act (in Meško, 2016):

- causes damage,
- is prohibited at the time of occurrence,
- criminal intent,
- criminal act connected with the consequence,
- legally prescribed penalty.

Bavcon and Šelih (in Meško, 2016) believe that crime is set of actions which threaten basic human values, such as life, physical integrity, security, property and human rights and basic social values. The interpretation of criminal acts varies in different societies and cultures, and therefore many criminologists define criminal offenses as those acts which are punishable and prosecuted by law (Kanduč, 2007, 2015). Durkheim (in Kanduč, 2007) advocated a similar definition, noting that the consequence of any criminal act is punishment. A criminal act affects the moral consciousness and beliefs of a social group, and with punishment this impact is softened. He went even further and argued that a crime is treated as such because of the social perception of the related act, and not merely because of the nature of the act itself. According to utilitarian theory, punishment prevents further criminal activities and deters offenders from breaking the law. On the other hand, retributivist theory advocates the idea of punishment as imposing penance, by which the crime is nullified (Kanduč, 2007).

The perception of crimes is socially or culturally conditioned, so punishments could vary in different societies and countries. Some acts are not punishable by law in all countries or – and in most cases – they are not subject to the same penalties. Mechanisms for prosecution of the worst criminal acts are therefore set at national and international levels. Criminal liability for war crimes, crimes against humanity and crimes of genocide at the international level was established with United Nations General Assembly Resolution 95 (I) of 11 December 1946. Even when national law does not define these cases as international crimes, the perpetrators could be prosecuted under the international criminal law which was in force at the time such crimes were committed (Cassese, 2009). This legality principle derives from the Universal Declaration of Human Rights (1948, article 11) and applies to national law, so retrospective prosecution is not possible.

The United Nations General Assembly recognised genocide as a crime under international law in 1946 (United Nations, 2021). Two years later genocide was qualified as an independent crime in the Convention on the Prevention and Punishment of the Crime of Genocide (the Genocide Convention). The Convention defines genocide as actions committed with intent to destroy (whole or in part) a national, ethnic, racial or religious group. These actions may include killing or seriously harming members of the group, influencing the living or other conditions of the group to destroy it, preventing births within the group or transferring children to another group (Convention on the Prevention and Punishment of the Crime of Genocide, article 2). The same definition of genocide as in the Genocide Convention is also included in the Rome Statute of the International Criminal

Court (article 6), along with the statutes of other international organisations, and the national legislation of many states (Rome Statute of the International Criminal Court, 1998; European Asylum Support Office, 2021).

War crimes derive from the International Humanitarian Law, which defines the rules of armed conflicts with the objective of restricting of the means and methods used, and protecting civilians and individuals no longer taking part in the hostilities. Based on the classification of the armed conflict (international or non-international), the applicable set of rules is determined and thus the international criminal responsibility of the participating parties. More precisely for the context of this study, the fourth Geneva Convention – which protects the civilian population and individuals taking no active part in the hostilities – and customary international law apply in Iraq, where we have witnessed an intense armed conflict between the state's security forces and organised non-state armed groups. Based on the case law for the former Yugoslavia, additional criteria connected to the intensity of the conflict and to the organisation of the parties need to be fulfilled for a non-international armed conflict to be recognized. The required intensity of the conflict was already reached in the first few months after the proclamation of the Caliphate due to the high number of confrontations, type of weapons used, number of people fighting, casualties and displaced civilians. At the same time, the Islamic State was highly organised with a clear command structure and the ability to plan and carry out military operations, and can be therefore defined as an organised non-state armed group. The relevant International Humanitarian Laws are thus applicable to Islamic State as well (IV Geneva Convention relative to the protection of civilian persons in time of war of 12 August 1949; Eurojust, 2020). The exact definition of war crimes is also included in Article 8 of the Rome Statute (Rome Statute of the International Criminal Court, 1998). According to this, breaches of the Geneva Conventions are the most serious war crimes, prosecuted under national and international laws, and specifically wilful killing, torture, causing great suffering or injuries, unnecessary and extensive destruction of property, exploitation of prisoners of war as combat forces or depriving them of their rights, unlawful deportation or transfer of the population and hostage-taking.

Crimes against humanity are defined in article 7 of the Rome Statute as murder, extermination, enslavement, forcible transfer or disappearance of people, imprisonment, torture, sexual violence, persecution of any group (religious, political, racial etc.), segregation or other inhumane acts intentionally causing suffering or serious harm, if these acts are committed widely and systematically against civilian population (Rome Statute of the International Criminal Court, 1998). It is not necessary that crimes against humanity target the whole population, but only that the attacks target a broad and intentionally selected group. Crimes against humanity are acts committed in accordance with the policy of a government or an organisation capable of carrying attacks against civilians. The attacks are widespread based on both the number of victims and scale of the attacks. Systematicity, however, derives from the organisation and pattern of the attacks, which is planned and coordinated (Eurojust, 2020).

This theoretical chapter on different types of the worst crimes known to humanity and a review of the legislation addressing these crimes provides a basis for the identification and categorisation of Islamic State actions, which are presented in the next chapter. Based on the presented actions, it is thus possible to quickly determine their gravity and legality, according to the relevant national and international legal standards.

3 ISLAMIC STATE IN IRAQ

3.3 The rise and fall of the Islamic State

The Islamic State is an international Sunni terrorist organisation whose ideology is based on an extreme Salafist interpretation of Islam. According to experts, it arose in response to Western military intervention in Iraq in 2003. It was founded on the remains of the Jama'at al-Tawid wal-Jihad organisation known as Al-Qaeda in Iraq, founded by al-Zarkawi in 2004. The Zarqawi-led Al-Qaeda in Iraq was focused on jihad in Muslim countries, and launched violent actions against foreign forces in Iraq, bombings and public executions and became a magnet for foreign fighters. After its leader's death in 2006 it seemed that Al-Qaeda in Iraq would collapse, but a few months later its leadership was taken over by Abu Omar al Baghdadi, and the organisation was renamed the Islamic State of Iraq (Clarke, 2019). The period after that, marked by execution of Saddam Hussein and the constant pressure by US and coalition forces, was very violent, with more than 50 civilians killed by the Islamic State of Iraq or other violent militias each day. After the death of his predecessor, Abu Bakr al Baghdadi took command in May 2010. Under his leadership, the Islamic State of Iraq carried out a number of suicide bombings in the country in 2010 and 2011, and released a number of prisoners who had sworn allegiance to it. Following the escalation of the civil war in Syria, the Islamic State of Iraq unilaterally declared affiliation with the Syrian Jabhat al Nusra in 2013 and renamed itself the Islamic State of Iraq and Syria. Its unification in Iraq was possible due to sectarian tensions and the civil war in Syria, which enabled the expansion of its activities (Cockburn, 2015; Gaffney, 2019; Inkret, 2016; Stern & Berger, 2015). During this time, at the beginning of 2014, Al-Qaeda publicly distanced itself from the Islamic State of Iraq and Syria, which had begun to build its visibility on social media by posting videos of executions. It thus gained sympathisers around the world and started to attract foreign fighters as well as home-grown terrorists who started to carry out attacks in their home countries around Europe (Stern & Berger 2015). After the proclamation of the Caliphate in June 2014, the group became known as the Islamic State.

Gaffney (2019: 315) attributes the Islamic State's rapid rise to "large numbers of supporters, unlimited financial resources, skilful use of social media and the ability to operate as a military organization". The group operated on two levels – online with its own use of social media, and on the territories it seized by immediately establishing its authority. With the help of modern technology, it managed to connect thousands of supporters online who were willing to take

part in the fight against the rest of the world. In the physical environment, it established a fully functioning economy and civilian institutions. At both levels of operation it relied on extreme violence, which served as a tool to intimidate opponents and recruit foreign fighters. The Islamic State thus succeeded in doing what no terrorist organisation had done before – mastering social media and social networks, and becoming extremely rich due to the seizure of assets, taking control of companies and oil stocks (Gurcan, 2014; Stern & Berger 2015,).

The Islamic State's strength began to wane after the intervention of international forces, which joined with the national armies in Iraq and Iraqi Kurdistan and local militias in both countries. The biggest, richest terrorist organisation in the world thus started to lose territory and power, and was finally defeated in 2017. However, these territorial losses did not mean the end of the Islamic State, as its influence is still present in the Middle East and globally (Chatham House, 2021).

3.3 Islamic State criminal operations in Iraq

The Islamic State changed the map of the Middle East by conquering some strategically important cities in Iraq and Syria. The operations in Iraq started in January 2014 with the group taking control of the Sunni city of Fallujah in the Iraqi province of Anbar. Within a few months, the entire province had become a battleground. In addition to operations that would open the way to the Iraqi capital, the Islamic State took control of the border region between the cities of Wilayat Al-Barakah in Syria and Wilayat Ninawa in Iraq. However, the Islamic State gained the global attention in June 2014 with capturing of Mosul. The second largest city in Iraq then served as an Iraqi capital of the self-proclaimed Caliphate until its liberation in 2017. In addition, the Islamic State captured the cities of Abbasi and Tikrit, areas around Mount Sinjar, Tel Afar and the Ninewa Plateau and a good part of the northern provinces by rapid offensives (BBC, 2014; Human Rights Council, 2015; Islamic State Report, 2014).

By the end of 2014, the Islamic State controlled almost 32% of the territory of Iraq, excluding territories under the control of Kurdish forces (Peshmerga) in the autonomous region where the group failed to penetrate. Its rapid advance was due to unified leadership and a focus on gaining key military and economic centres, natural resources, and critical infrastructure (Aljaf, interview, August 20, 2015; Cockburn, 2014; Vovk, 2014).

In 2015 the Islamic State continued with its offensives, occupied the city of Ramadi and began a march on Baghdad. It took over a nearby international airport and launched a large-scale offensive on the city of Baiji, home to Iraq's largest oil refineries. In Iraq and Syria, the group took control of most of the countries' oil and natural gas reserves (Engel, 2015; Macias, 2015; Vick, 2015).

In regions under its control the Islamic State "introduced its own judicial system based on a strict interpretation of the Sharia" (European Asylum Support Office, 2021) with this resulting in severe crimes and human rights violations:

- forced displacements,
- forced religious and ideological conversions,
- ethnical cleansing and genocide,

- abductions,
- systematic and widespread killings of opponents, mass executions, beheadings,
- sexual violence, including sexual slavery,
- exploitation of children (child soldiers),
- human trafficking,
- destruction of cultural heritage.

Such violations were also common in the day-to-day operations of the Islamic State.

The Islamic State is well known for serious human rights violations and deliberate and systematic attacks on minorities in the territories it controlled. It targeted Shia Muslims as well as ethnic and religious minorities such as Christians, Yazidi, Shabaks, Turkmen, Kaka'i, and Kurds. In 2014 it committed "the 21st century's clearest case of genocide so far" (Yale University – Genocide Studies Program, 2021) when its troops invaded Sinjar region where the Yazidi people are located. In an extremely short period of time an estimated 5,000 Yazidi men and elderly women were killed, and approximately 6,000 women and children were held captive, sold as slaves, raped, beaten or used as child soldiers. The Yazidi group was intentionally targeted by the Islamic State and subjected to such acts that are defined as genocidal.

In addition to ethnic, religious, and sexual violence, Islamic State members committed many politically motivated crimes. They attacked members of the police and armed forces, civil servants, members of parliament, local religious and political leaders and anyone who publicly opposed them.

To achieve its goals, the Islamic State used the following methods: suicide attacks, car bombings, improvised explosive devices, beheadings, kidnappings, cyber terrorism, and piracy, among others. Human rights violations and war crimes resulted in mass migrations of 3.3 million Iraqis within and outside their country (Ellis, 2014; Human Rights Council, 2015). Despite the defeat of Islamic State in 2017, not all the refugees and displaced persons have yet returned to their homes.

Many Islamic State fighters originate from Iraq, although the exact number of Iraqi fighters or supporters is not known. The biggest group joining Islamic State was the Sunnis, who joined or associated the terrorist organisation as retaliation for Shia domination after the fall of Saddam Hussein's regime. At that time a minority Shiite population gained power under the auspices of the United States and international coalition. Many who joined the group mistakenly believed that the Islamic State would give control and power back to Sunnis and banish foreign forces from the country. Many who joined the Islamic State or moved to territories the group had seized for the above-mentioned reasons later regretted the decision, since the reality of life under the control of the Islamic State did not meet their expectations (Representative of Ministry of Peshmerga Affairs, Interview, October 31, 2019; Representative of Ministry of Peshmerga Affairs, Reforms Directorate, Interview, October 31, 2019). On the other hand, the group's ideology also played an important role in encouraging Sunni Iraqis to join. According to these reasons

and motives behind radicalisation and the decision to join the Islamic State, we can categorise its members in Iraq into three groups:

- extremely radicalised members who share the Islamic State's ideology and joined it because of this and do not regret their decision,
- individuals of Sunni origin who chose membership as a form of opposition to Shia power and foreign presence in the country, but later regretted their decision,
- foreign fighters from the West with a distorted view of Islam or different motives, such as adventure, money, rewards, sense of belonging, etc. (Representative of Ministry of Peshmerga Affairs, Interview, October 31, 2019; Representative of Ministry of Peshmerga Affairs, Reforms Directorate, Interview, October 31, 2019).

Kurds, who represent the biggest ethnic minority and are united in the autonomous Kurdistan Region in Northern Iraq, were much rare among members of the Islamic State.

Since the military defeat of the Islamic State group does not hold any territory in Iraq, but continues to operate as an insurgent and terrorist group with many active and sleeper cells around the country. The number of areas with active Islamic State cells has doubled since 2018, and the group's activities have been detected in Anbar, Ninewa, Erbil, Baghdad Belts, Diyala, Kirkuk and Salah al-Din cities and regions. An estimated 1,300 active fighters and 12,700 supporters of the Islamic State were still present in Iraq in 2020 (European Asylum Support Office, 2021). The group has gained more and more freedom to operate in recent years, especially in areas where conventional military forces are not as much present, such as valleys, mountains, deserts and disputed areas, the latter of which have been revived as an indirect consequence of the fight against the Islamic State. Disputed areas between the Iraqi government and Kurdistan Regional Government came to the fore again in 2014 after the Kurdish forces drove out the Islamic State and took control of some strategically important cities that were historically Kurdish, but have been controlled by the Iraqi government in recent years. This caused tensions in 2017 when Iraqi security forces tried to retake the city of Kirkuk and its surroundings, but was resolved with the peaceful withdrawal of Kurdish forces. However, the old territorial dispute has once again been revived, and with the deliberate avoidance of conflict on both sides the resulting smaller military presence has created a security vacuum and safe haven for radicalised individuals, groups, and Islamic State sleeper cells (Mohammad, Interview, October 31, 2019; Representative of Ministry of Peshmerga Affairs, Interview, October 31, 2019; Representative of Ministry of Peshmerga Affairs, Reforms Directorate, Interview, October 31, 2019; Representative of Asayish, Interview, November 4, 2019).

4 CRIMINAL LIABILITY AND PROSECUTION OF ISLAMIC STATE FIGHTERS AT THE INTERNATIONAL LEVEL

The Islamic State was recognised as a terrorist organisation by most of nations and international organisations, although it did not operate as classical terrorist group. Soon after the proclamation of the Caliphate in June 2014, it established

a fully functioning state apparatus. However, it was not recognised as a state by other international subjects nor as an international organisation. As such it did not gain international legal subjectivity, had no international rights and obligations, and was not a subject to the rules of customary international law. It also had no authority to establish military forces and conduct military operations (Sancin et al., 2009). However, as Greenwood and Bowett point out (in Sancin et al., 2009), the existence of an armed conflict activates the application of the International Humanitarian Law (and the laws of armed conflict) and applies equally to all participating subjects, regardless of their legal status. Therefore, according to the International Humanitarian Law, the Islamic State fulfilled the criteria as a party to a non-international armed conflict acting as an organised non-state armed group. The International Humanitarian Law is thus applicable to Islamic State fighters, who could be held responsible for committing war crimes and other core international crimes.

Although its actions in Iraq and Syria are recognised as criminal, since they had criminal intent, caused damage and brought severe consequences, the operation of the Islamic State or any other group was not expected to this extent, and thus was not prohibited in all segments. In some cases, there were no or lenient prescribed penalties for individual actions at the state level or internationally. Despite mechanisms for prosecution of the worst criminal acts at both national and international levels, many changes to legislation have been made in the wake of the Islamic State, and its success in Iraq and Syria. In EU member states in particular, new judicial practices have developed to cumulatively prosecute and hold foreign terrorist fighters, fighting in Iraq and Syria, “accountable for war crimes, crimes against humanity and the crime of genocide, in addition to terrorism-related offences” (Eurojust, 2020: 3).

No adjustments have been made to the international legislation connected to the crime of genocide. Although 149 states have ratified the Genocide Convention, its principles are, according to the International Court of Justice (ICJ), part of general customary international law and thus legally binding regardless of ratification (United Nations, 2021). All crimes of genocide should be punished under the legislation, using competent tribunals of the country where the genocide was committed or an international tribunal with the jurisdiction recognised by the affected country (Convention on the Prevention and Punishment of the Crime of Genocide, article 4–6). Preliminary analysis of the crimes perpetrated against the Yazidi community, based on widely accessible resources, confirms basic the elements of the genocide, as killing or seriously harming the physical or mental health of the members of this ethnic group, along with harming their living conditions and transferring children by force have been detected. At present, no official conclusions on this matter have been made by international organisations, other subjects or individual states. Further investigations and research could lead to the formal conclusion that Islamic State committed the stated crimes with the intent of destroying whole or in part the Yazidi community and thus committing crime of genocide against this group.

The Islamic State committed war crimes in Iraq and Syria against the civilian population within the territories it controlled, especially targeting religious and

other minorities, like Yazidis. Even individuals who did not take part in hostilities orchestrated by the Islamic State became victims of “murder, execution without due process, mutilation, torture, cruel treatment, enforced disappearance, abductions and hostage-taking”. Women and girls suffered from sexual slavery, gang rape, executions and stoning, and were forced into pregnancy. Children were recruited as soldiers to participate in hostilities. Islamic State fighters wilfully perpetrated these war crimes while they were aware of status of civilians or individuals no longer participating in hostilities, and thus violated obligations towards civilians and persons *hors de combat* under international law (Eurojust, 2020: 12–13).

The Islamic State committed crimes against humanity in Iraq in the form of widespread and systematic attacks, targeting the civilian population. The group had all the means to carry out the attacks within a large part of the territory of the two states, Iraq and Syria, where it exercised control. The civilian population in Central and Northern Iraq, especial religious and ethnic minorities, were victims of the group’s killings, enforced disappearances, mutilation and torture. Islamic State fighters systematically targeted woman who were then subjected to sexual violence, enslavement, rape, forced pregnancy, stoning and murder. Another group that was systematically targeted by Islamic State were Yazidis, who were victims of the crimes against humanity “of sexual slavery, rape, sexual violence, enslavement, torture, other inhuman acts and severe deprivation of liberty” (Eurojust, 2020: 15). Such attacks were committed under the command of the Islamic State, which was highly organised and hierarchically structured. These details, together with the discriminatory, widespread and systematic nature of the attacks of the Islamic State on the civilian population in Iraq, thus meet the criteria for crimes against humanity prosecuted under international law.

Criminal liability for crimes of genocide, war crimes and crimes against humanity at the international level was established with United Nations General Assembly Resolution 95 (I) of 11 December 1946. Even when national law does not define these cases as international crimes, the perpetrators could be prosecuted under international criminal law (Cassese, 2009). Perpetrators could be prosecuted, for example, at the International Criminal Court, which was established in 2002. It has jurisdiction to prosecute crimes of genocide, crimes against humanity and war crimes (Türk, 2007), but it does not have any jurisdiction over perpetrators originating in Iraq, since the country is not a member of the International Criminal Court. Only foreign fighters who committed war crimes, crimes against humanity or the crime of genocide on Iraqi territory and are at the same time nationals of a state that is member of the court can be prosecuted by it.

The grounds for prosecuting Islamic State fighters at the international level lay in several international acts, which depend on the gravity and type of crime committed. There are also international institutions that prosecute the worst crimes under international regulations, or specialised courts are set up for particularly serious crimes, such as the international courts for Rwanda and the former Yugoslavia. Due to the scale of atrocities committed by Islamic State fighters in Iraq and Syria, the idea of establishing an international tribunal to prosecute those who had committed the worst crimes arose in 2019. As of today, however, no specialised tribunal for Iraq or Syria has been established. Not a single individual

who committed war crimes, crimes against humanity or the crime of the genocide has been held accountable under international law or has been brought to justice at the international level.

Iraq is one of the parties to the International Covenant on Civil and Political Rights, which ensures equal civil and political rights (1976). It applies to the prosecution of individuals and should be considered when national legislation is being drafted or implemented. The provisions related to the prosecution and enforcement of civil and procedural rights in trials will be outlined below in the context of the implementation of national legislation.

5 CRIMINAL LIABILITY AND PROSECUTION OF ISLAMIC STATE FIGHTERS IN IRAQ

The judicial system in Iraq combines a mixture of civil and Islamic law. It is divided into four areas, based on the jurisdiction: constitutional, general, administrative and military/internal security forces judiciary.

The highest authority in the Iraqi judicial system is the Federal Supreme Court, with jurisdiction over constitutional issues and disputes among the Kurdish region, governorates and central government (Central Intelligence Agency, 2021). The highest authority of the general judiciary is the Supreme Judicial Council, which is specialised in administration of general judiciary and thus has courts in nine different areas and on different levels. The courts of the Supreme Judicial Council (Republic of Iraq, Supreme Judicial Council, 2021) include:

- Court of Cassation as supreme judicial commission that examines the decisions with sentences of more than five years in prison in civil, criminal and family court.
- Appeal Courts in each governorate (with the exception of two in Baghdad and none in Kurdistan), specialised in civil and criminal claims with a maximum penalty of five years in prison.
- Courts of First Instance / Trial Courts specialised in civil cases.
- Family Courts specialised in family cases, marriage, divorces, etc.
- Courts of Investigation specialised in investigations of all crimes with minimum penalties of five years, misdemeanours under five years and violations with penalties under three months.
- Courts of Assizes in each governorate specialised in cases with penalties over five years. The verdicts are reviewed by Court of Cassation.
- Courts of Misdemeanours specialised in crimes with maximum penalties of five years. The verdicts are reviewed by Appeal Courts.
- Courts of Juveniles specialised in cases with minors (under age 18) involved.
- Courts of Labour specialised in cases in the field of labour.

Although the Republic of Iraq is a party to some international legal instruments, it is not a signatory to the Rome Statute of International Criminal Court and it has not submitted an International Court of Justice declaration yet (Central Intelligence Agency, 2021). Therefore, the Iraqi courts do not have

jurisdiction over the crime of genocide, war crimes or crimes against humanity committed within Iraqi territory.

The Republic of Iraq is a party to the abovementioned four Geneva Conventions of 1949 which in article 3 prohibits sentencing without the judgement of the competent court, providing the judicial guarantees of civilised society. The rights of defence and fair trial and the prohibition of forced confessions are provided under article 19 of Iraq's Constitution (Constitute, 2005). Further rights in all phases of investigation and trial are defined under the Criminal Procedure Code, which also allows statements from secret informants and judgements based only on the confession of defendant without any evidence. These provisions raised some concerns with the United Nations Assistance Mission for Iraq in the past, along with the minimum age of criminal liability of just nine years (United Nations Assistance Mission for Iraq, 2020).

Anti-terrorism legislation has been in force for fifteen years now, both at the level of central government and Kurdistan Regional Government. Both the Federal Anti-Terrorism Law and KRI Anti-Terror Law are based on a broad definition of terrorism, and describe terrorist acts as using violence with intention of spreading fear, as acts with motives that threaten unity of the state or damage public property. The laws differ in the criminalisation of the membership of a terrorist organisation and the prescribed penalties. The federal legislation anticipates the death penalty for all terrorist offences (incitement, planning, financing, assisting terrorists or carrying out a terrorist attack). The prescribed sentences under the Kurdish law vary for different acts of terrorism, ranging from the death penalty to life imprisonment or imprisonment under fifteen years. As the United Nations Assistance Mission for Iraq notes in its analysis of the functioning of the judicial system in the prosecution of the Islamic State, the legislation should be based on a more precise definition of terrorist acts, since too broad definitions make anti-terrorism laws susceptible to subjective interpretations. At the same time, the legislation should correspond to the general »characteristics of conduct to be suppressed in the fight against international terrorism« (United Nations Assistance Mission for Iraq, 2020, p. 4). Meaning that the strictest penalties should be limited to the worst terrorist offences, which is not the case with the Federal Anti-Terrorism Law nor the KRI Anti-Terror Law. The laws differ on fair trial rights, too, since only Kurdish law includes provisions related to them, but at the same time allows the court to use confessions obtained under duress.

The right to liberty, equality before courts and fairness of hearings derives from the International Covenant on Civil and Political Rights (1976, article 9–10, 14), which enables the presentation of cases and enjoyment of procedural rights. On this regard, the United Nations Assistance Mission for Iraq has noted issues related to the provision of adequate time and facilities for defence, effective legal representation, and reliance on anonymous informants (United Nations Assistance Mission for Iraq, 2020).

The right to adequate time and facilities to prepare defence and of provision of effective legal representation in all stages of the process is stated in the International Covenant on Civil and Political Rights (1976, article 14) and through principles 3, 6, 7 and 8 of the United Nations Principles and Guidelines on Access

to Legal Aid in Criminal Justice Systems (United Nations Office on Drugs and Crime, 2013). In the case of Iraq, courts did appoint lawyers to defendants in most cases. However, these court-appointed lawyers played a passive role in the proceedings. Non-compliance with the provisions of this international regulation and guidelines was noted by the United Nations Assistance Mission for Iraq, since court-appointed defence lawyers were mostly assigned on the first day of trial, leaving them with no time to prepare the defence. In the case of terrorism-related procedures, the right to public hearings, granted through public access to trials, was limited or authorised by courts. In some cases, family members of defendants or victims and their representatives were not allowed to participate in the trials. That left victims without answers about the causes and conditions that led to their victimisation, and without the possibility to see the perpetrators punished for their crimes (United Nations Assistance Mission for Iraq, 2020).

More than two thirds of criminal cases in Iraq related to Islamic State were based on anonymous witness with no opportunities for cross-examination. The transfer of most of the weight of the legal procedure to anonymous statements without compensation for the disadvantage is contrary to the International Covenant on Civil and Political Rights (1976, article 14; United Nations Assistance Mission for Iraq, 2020). According to Human Rights Watch, when investigating suspected Islamic State members both Iraqi and Kurdistan Regional Government forces derive evidence from unreliable sources, and identify suspects based on wanted lists or reports from the community. The lack of further evidence may result in the unlawful detention of individuals. Furthermore, conditions in detention and during interrogation were found to be overcrowded and sometimes inhumane, and the process rights of suspects were systematically violated (Human Rights Watch, 2017). There were even some reports of torture, which is in contravention of both international law and the Iraqi Constitution (2005, article 35). Many confessions were obtained from defendants during the proceedings and withdrawn at the trial, and allegations of torture or ill-treatment have been made in almost half of the terrorism-related cases. International organisations such as Human Rights Watch (2017) and the United Nations Assistance Mission for Iraq (2020) have received reports of forced confessions obtained by torture and ill-treatment by law enforcement and security authorities in Iraq. These confessions were mostly not questioned by judges during the related trials, and were thus used as evidence. In a few cases medical reports confirmed torture, but in only one case was such a confession excluded as evidence. Use of these methods in the proceedings would mean violation of article 7 of International Covenant on Civil and Political Rights.

The armed forces of the Iraqi government and Kurdistan Regional government have detained thousands of suspected Islamic State fighters and affiliates, including hundreds of children during the years of active military campaigns against this terrorist organisation from 2014 to 2017, and even after its defeat (Human Rights Watch, 2017). In the absence of a national strategy for prosecution and under the high expectations of a severe approach against terrorism being adopted by the judiciary, Human Rights Watch reported on the rapid prosecution of thousands of suspected members of the Islamic State in counterterrorism courts in Iraq and Iraqi

Kurdistan, with little distinction made on the severity of offenses. As prescribed under international law, such trials should be based on the principles of legality and individual criminal liability. That means that individuals should be punished for acts they have committed, based on a precise law. Broad definitions under the Federal Anti-Terrorism Law and interpretations of membership of and association with the Islamic State allowed allow convictions for a wide range of defendants. In most of the cases the indictment was no more specific than “joining the terrorist organisation”. According to Human Rights Watch (2017), the penalties based on the counterterrorism legislation are disproportionate. The indictment only requires proof of membership or proof that an individual worked in an Islamic State institution, and not proof of an individual crime. This way of interpreting the legislation and prosecution allows for the long imprisonment of individuals who were perhaps only living on the seized territories. On the other hand, it might happen that those committing the most serious crimes and atrocities will not get penalties commensurate with their actions. However, federal courts in Iraq have imposed a range of sentences for terrorist offences, despite the death penalty being required under the Federal Anti-Terrorism Law, but with no clear sentencing criteria and no distinction made on voluntary or coerced association with the Islamic State (United Nations Assistance Mission for Iraq, 2020). In contrast, officials in Iraqi Kurdistan have attempted to avoid such indiscriminate punishment and highlighted two groups of suspects and sentences based on the categorisation of membership. The first group of suspects has been categorised as Islamic State supporters and members who mostly joined to oppose to Shia control and foreign presence in the country. Those individuals lived inside or outside the Islamic State territories and actively showed their support for this terrorist organisation, were confirmed members or worked at one of the civilian organisations under Islamic State’s control but did not participate in any killings. If these individuals show clear and unmistakable signs of remorse and there was no proof of previous violent behaviour, then they were imprisoned from two to five years. The second group represent Islamic State fighters, who were extremely radicalised, shared the group’s extreme ideology, actively participated in fighting, killings and executions, or have committed other crimes against humanity and not shown any remorse (Mohammad, Interview, October 31, 2019; Representative of Ministry of Peshmerga Affairs, Interview, October 31, 2019). In Kurdistan courts the most common sentence for extremely radicalised members or fighters of Islamic State is from 10 years to life imprisonment, rather than the death penalty. Both groups of suspects have been prosecuted in accordance with counterterrorism legislation, which regulates radicalisation and terrorism to some extent. The counterterrorism legislation in Iraq and Iraqi Kurdistan and its broad interpretation allows prosecution and punishment in case of individuals who were involuntary associated with the Islamic State. Along with low standards of proof and tother disadvantages when presenting the defence case, this could lead to collective punishment of certain communities (United Nations Assistance Mission for Iraq, 2020).

Another issue of concern for international organisations like Human Rights Watch and the United Nations Assistance Mission for Iraq regarding the

prosecution and criminal liability of Islamic State fighters is the sentencing and execution of a death penalty. The death penalty is strictly limited to the most serious crimes in those states where it still exists under the International Covenant on Civil and Political Rights (1976, article 6). Due to the above-described issues with regard to getting adequate time and facilities for defence, effective legal representation, and reliance on anonymous informants or even forced confessions, concerns about the execution of the death penalty and its compliance with article 6 and 14 of this international regulation have been raised. Furthermore, violations of the Geneva Convention (IV Geneva Convention relative to the protection of civilian persons in time of war of 12 August 1949, article 3) may have taken place with executions carried out without trials, and death sentences being given for mere membership of the terrorist organisation. Death sentences may be given due to a general interpretation of the terrorism legislation, and not tied to specific terrorist acts (United Nations Assistance Mission for Iraq, 2020). The death penalty is allowed as a punishment for significant violations of legislation and severe crimes in Iraqi Kurdistan, but according to officials from the Ministry of Peshmerga Affairs¹ and Asayish² it is not imposed often, due issues with regard to human rights. A moratorium on the death penalty was in place in this autonomous region for more than a decade, but it was lifted in 2015 and 2016 with at least two recorded executions of Islamic State fighters (Mohammad, Interview, October 31, 2019; Representative of Ministry of Peshmerga Affairs, Interview, October 31, 2019; Representative of Asayish, Interview, November 4, 2019; United Nations Assistance Mission for Iraq, 2020).

Based on the above-described observations, registered events and analysis of international and national legislation, we can easily claim that the operation of the Islamic State contained elements of terrorist acts, crimes of genocide, war crimes and crimes against humanity. Countries facing the threat of the Islamic State on a larger scale due to the high active presence of their fighters, members and supporters or countries of origin of the foreign fighters, have adapted their legislation and procedures to prosecute its fighters. However, Peshmerga Chief of Staff Lieutenant General Jamal Mohammad (Mohammad, Interview, October 31, 2019) believes that such adaptation of legislation should be done in all countries around the world which are facing the threat of the Islamic State. Terrorists cannot be prosecuted according the traditional legislation, and this is why Western countries should tighten the legislation and imprison foreign Islamic State fighters for a long time. The legislation, its implementation and prescribed penalties should be harmonised on all levels and in all countries. Offenders would then face the same prosecution procedures and punishments for the same types of crimes. However, the penalties should result from the categorisation of crimes based on the precise definition of the type and degree of involvement of an individual with the Islamic State, and the severity of the crimes committed.

Another issue, raised by Mohammad (Mohammad, Interview, October 31, 2019), is the sole focus on punishing Islamic State fighters. The reintegration and reconciliation process for Islamic State fighters is much more complicated

¹ Armed forces of the Kurdistan Regional Government, authorised under the auspices of the Iraqi Constitution.

² Security and intelligence organisation of the Kurdistan Regional Government, often referred as the Kurdish intelligence agency or police.

and wider than a prison sentence. If we take into account the background and process of the emergence of the Islamic State, how it extended its influence and operation to such dimensions, we can see several factors which need to be addressed. The elements and circumstances that allowed Islamic State to flourish or drove individuals to join this terrorist organisation will not disappear with the imprisonment of individual offenders. Those elements are mostly the political and security situation in Iraq and the wider region, unsolved historical disputes over territories or among religious groups, and the specific circumstances of the individuals. In the case of Iraq, the conflict between Shia and Sunni Muslims played a key role in the population supporting the Islamic State. Most of the Islamic State fighters of Sunni origin from Iraq joined the organisation for historical reasons, such as opposition to Shia domination after the fall of Saddam Hussein (Representative of Ministry of Peshmerga Affairs, Reforms Directorate, Interview, October 31, 2019). All this and more are push and pull factors that led to the radicalisation of individuals to the extent of joining the Islamic State, and all of them need to be addressed. Therefore, the Islamic State fighters need to undergo a process of de-radicalisation and not merely be imprisoned. Furthermore, risk factors for radicalisation must be eliminated at the levels of society and state, and effective mechanisms for recognising and preventing further radicalisation need to be established. Even after the military defeat of the Islamic State in 2017, it looks like the group will not be destroyed any time soon. It thus still represents a threat that must be approached thoughtfully, strategically and comprehensively, especially in those countries where it was present for many years, such as Iraq.

6 CONCLUSIONS

The Islamic State controlled more than a third of Iraqi territory at its peak, and took over key military and economic centres, natural resources and critical infrastructure. It established a fully functioning state apparatus in the territories it controlled with its own economic, social, educational, security and judicial system that was based on Sharia Law. The operations of this organisation were marked by numerous human rights violations and crimes, as forced displacements, forced religious and ideological conversions, ethnic cleansing and genocide, abductions, mass executions, beheadings, sexual violence and exploitation of woman and children, and the destruction of cultural heritage. These are serious crimes under the international law which Islamic State fighters should be accountable for, since the group fits the criteria as a party to a non-international armed conflict acting as an organised non-state armed group, and thus could be held responsible for committing war crimes.

However, things are not so black and white in this case, since prosecution under international law falls under international courts when the party or state in question is the party or a signatory to the relevant international document. Although criminal liability for crimes of genocide, war crimes and crimes against humanity was established at the international level and thus enables the prosecution at this level when national law does not define these crimes, in the case of Iraq this is not possible. The International Criminal Court, which

addresses these cases, does not have jurisdiction over perpetrators originating in Iraq, since the country is not a member. Only foreign fighters who are nationals of a member state could be prosecuted by this court. As of today, however, not a single foreign fighter who committed war crimes, crimes against humanity or the crime of genocide in Iraq has been held accountable under international law. Furthermore, no specialised tribunal for Iraq or Syria has been established as one of the possible solutions to bring to justice the Islamic State fighters from all over the world. Although all the data confirms the crime of genocide was perpetrated by the Islamic State in Iraq, no official conclusions and declarations on this matter were made by international organisations or individual states.

Similarly, there are no reports of the prosecution of Islamic State fighters of Iraqi origin who would be specifically accountable for war crimes, crimes against humanity or the crime of genocide under national legislation, since the Iraqi courts do not have jurisdiction over those crimes. There are several reports on finalised or on-going prosecution and trials, but with no distinction on the severity of the crimes committed. The suspects are mostly prosecuted for cooperation with the Islamic State, but it is usually not clear from the indictments or sentences whether the individual had been committing the crime of genocide, war crimes, worked as Islamic State administrative worker or just lived in a territory held by the group. Furthermore, severe human rights and international law violations have been reported in connection to these prosecution procedures. The suspects are denied the right of defence and fair trial, since court-appointed lawyers play a passive role or are appointed at the last minute. Another issue of concern are statements from secret informants and judgements based on confessions without any evidence, especially under the assumption, based on reports, that some of the confessions could have been forced.

The case of the Islamic State has shown that the related legislation, its implementation and prescribed penalties should be harmonised on all levels and in all countries. Offenders should face the same prosecution procedures and punishments based on the severity of the crimes committed. The same applies to the rights of the suspects during the trials and while serving the sentence.

Additionally, prosecution is not the only procedure the Islamic State fighters should undergo. The procedures and protocols for de-radicalisation of Islamic State fighters should be in place in every country facing the threat. Those procedures should take into account the background and factors that drove individuals to join this terrorist organisation. Furthermore, risk factors for radicalisation must be addressed at the levels of society and state. Special attention should be paid to vulnerable groups, as well as to converts and families of known and convicted Islamic State supporters and members. Effective mechanisms for recognising and preventing further radicalisation, as well as reintegration back into society, need to be established. Although the Islamic State has lost its influence and territories, this does not mean the end of the organisation. Its influence and ideology are still present in the Middle East and globally, and there are many sleeper cells present in Iraq. The authorities in this country and its constitutionally independent Kurdish region did not take many steps forward in this regard after the defeat of the Islamic State, as preventive and de-radicalisation programmes have still not

been created and procedures for prosecution and prescribed punishments have not been unified, while most of the risk factors for radicalisation have remained, or new ones have arisen.

LITERATURE:

- IV Geneva Convention relative to the protection of civilian persons in time of war of 12 August 1949. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf
- Bavcon, L., & Šelih, A. (2003). *Kazensko pravo – splošni del* [Criminal law – general part]. Uradni list Republike Slovenije.
- BBC. (2014). *Syria Iraq: The Islamic State militant group*. <http://www.bbc.com/news/world-middle-east-24179084>
- Cassese, A. (2009). *Affirmation of the Principles of International Law recognized by the Charter of the Nürnberg Tribunal General Assembly Resolution 95 (I) – Introductory note*. https://legal.un.org/avl/ha/ga_95-I/ga_95-I.html
- Central Intelligence Agency. (2021). *The World factbook – Iraq*. <https://www.cia.gov/the-world-factbook/countries/iraq/#government>
- Chatham house. (2021). *Radicalization*. <https://www.chathamhouse.org/topics/radicalization>
- Clarke, M. (2019). Iraq. In A. Silke (Ed.), *Routledge handbook of terrorism and counterterrorism* (pp. 563–573). Routledge.
- Cockburn, P. (2015). *The rise of Islamic State: ISIS and the new Sunni revolution*. Verso.
- Convention on the Prevention and Punishment of the Crime of Genocide, December 9, 1948. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf
- Durkheim, E. (1973). *Moral education*. Free Press.
- Ellis, R. (2014). *U.N. panel details ISIS abuses in Syria, says they amount to war crimes*. CNN. <http://edition.cnn.com/2014/11/14/world/meast/isis-war-crimes/> (22nd June 2021).
- Engel, P. (2015). This detailed Syria map shows what territory ISIS is truly fighting for. Accessible at: <http://www.businessinsider.com/map-of-syria-shows-what-isis-is-truly-fighting-for-2015-6>
- Eurojust. (2020). *Cumulative prosecution of foreign terrorist fighters for core international crimes and terrorism-related offences*. https://www.eurojust.europa.eu/sites/default/files/Partners/Genocide/2020-05_Report-on-cumulative-prosecution-of-FTFs_EN.PDF
- European Asylum Support Office. (2021). *Country guidance Iraq 2021*. <https://www.easo.europa.eu/country-guidance-iraq-2021>
- Gaffney, F. (2019). Islamic State. In A. Silke (Ed.), *Routledge handbook of terrorism and counterterrorism* (pp. 315–324). Routledge.
- Gurcan, M. (2014). *Don't expect Peshmerga to beat Islamic State*. <http://www.al-monitor.com/pulse/originals/2014/09/turkey-syria-iraq-kurdistan-isis-military-pesmerga.html#>
- Hartjen, C. A. (1978). *Crime and criminalization*. Praeger Publishers.

- Human Rights Council. (2015). *Report of the Office of the United Nations High Commissioner for Human Rights on human rights situation in Iraq in the light of abuses committed by the so-called Islamic State in Iraq and the Levant and associated groups*. <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Pages/ListReports.aspx> (3rd July 2021).
- Human Rights Watch. (2017). *Flawed Justice: Accountability for ISIS Crimes in Iraq*. <https://www.hrw.org/report/2017/12/05/flawed-justice/accountability-isis-crimes-iraq>
- Inkret, G. (2016). Protiislamski diskurz v Evropi ni nekaj novega: Primož Šterbenc, politolog, sociolog in strokovnjak za islam [Anti-Islamic discourse in Europe is nothing new: Primož Šterbenc, a political scientist, sociologist and expert on Islam]. *Pogledi*, 7(4), 12–13. <https://pogledi.delo.si/ljudje/protiislamski-diskurz-v-evropi-ni-nekaj-novega>
- Institute. (2005). *Iraq's Constitution*. https://www.constituteproject.org/constitution/Iraq_2005.pdf?lang=en
- International Covenant on Civil and Political Rights, December 16, 1996. <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.
- Islamic State Report. (2014). *Smashing the borders of the Tawaghit*. <https://azelin.files.wordpress.com/2014/06/islamic-state-of-iraq-and-al-shc481m-e2809cislamic-state-report-422.pdf>
- Kanduž, Z. (2007). *Kriminologija: (stran)poti vede o (stran)poteh* [Criminology: (Side) paths about (side) paths science]. Inštitut za kriminologijo pri Pravni fakulteti.
- Kanduž, Z. (2015). Uvodni opis problemskih sklopov [Introductory description of problem sets]. In A. Šelih, & K. Filipčič (Eds.), *Kriminologija* (pp. 25–48). GV Založba.
- Macias, A. (2015). *These maps show what ISIS has achieved in the last year*. <http://www.businessinsider.com/isis-gains-in-syria-and-iraq-2015-5>
- Masters, R., & Roberson, C. (1990). *Inside criminology*. Prentice Hall.
- Meško, G. (2016). *Kriminologija* [Criminology]. Fakulteta za varnostne vede.
- Republic of Iraq, Supreme Judicial Council. (2021). *The judicial system*. <https://www.hjc.iq/Judicial-system-en.php> (8th October 2021).
- Rome Statute of the International Criminal Court, July 17, 1998. <https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf>
- Sancin, V., Švarc, D., & Ambrož, M. (2009). *International law of armed conflict. Command for Doctrine, Development, Education and Training*.
- Stern, J., & Berger, J. M. (2015). *ISIS: The state of terror*. HarperCollins Publishers.
- Türk, D. (2007). *The foundations of the international law*. GV Založba.
- United Nations. (2021). *Office on Genocide Prevention and the Responsibility to Protect – Genocide*. <https://www.un.org/en/genocideprevention/genocide.shtml>
- United Nations Assistance Mission for Iraq. (2020). *Human Rights in the Administration of Justice in Iraq: Trials under the anti-terrorism laws and implications for justice, accountability and social cohesion in the aftermath of ISIL*. https://reliefweb.int/sites/reliefweb.int/files/resources/Iraq_-_ISIL_trials_under_the_anti-terrorism_laws_and_the_implications_for_justice_28012020.pdf
- United Nations Office on Drugs and Crime. (2013). *United Nations Principles and*

Guidelines on Access to Legal Aid in Criminal Justice Systems. . https://www.unodc.org/documents/justice-and-prison-reform/UN_principles_and_guidelines_on_access_to_legal_aid.pdf.

Universal Declaration of Human Rights, December 10, 1948. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

Vick, K. (2015). *As ISIS grows its territory, it becomes increasingly dangerous*. In Time. <http://time.com/3917097/as-isis-grows-its-territory-it-becomes-increasingly-dangerous/>

Vovk, T. (2014). Fifteen shocking numbers about Islamic State. Accessible at: http://www.siol.net/novice/svet/2014/08/isil_irak_sirija_islamisti_stevilke.aspx (17th July 2021).

Yale University – Genocide Studies Program. (2021). *Iraq/Yazidi*. <https://gsp.yale.edu/case-studies/iraq-yazidi>

About the author:

Anica Ferlin, PhD student at the University of Ljubljana, Faculty of Social Sciences. E-mail: anckaferlin@gmail.com

Police Instruments of Restraint against Persons with Health Problems – Analysis of the Use of Expert Grips and Holds as Forms of Physical Force

VARSTVOSLOVJE
*Journal of Criminal
Justice and Security*
year 23
no. 4
pp. 379–401

Branko Gabrovec, Tilen Zupan, Srečko Felix Krope, Branko Lobnikar

Purpose:

The purpose of this article is to analyse whether police officers have sufficient expert knowledge to control a violent patient with health problems. The aim is to determine the actual capability of police officers to control such persons and analyse the competencies of police officers in controlling violent persons.

Design/Methods/Approach:

Utilising the quantitative method of research and an adapted questionnaire by Gabrovec et al. (2014) as the method of data collection, we determined the state of the capability of police officers to control violent patients.

Findings:

In order to deal with and control violent persons, police officers can make use of a wide range of powers, including the use of instruments of restraint. However, since dealing with a violent person is not the same as dealing with a violent person with health issues or a person under the influence of drugs or medications, coercive means against such persons must be used differently and adapted. The specific nature of the situation dictates the need for additional skills and training for the successful implementation of police procedures that do not jeopardise the subsequent treatment procedures with the patient. Our analysis has shown the lack of knowledge and skills of police officers in dealing with violent persons who have health issues or are under the influence of drugs or medications. Police officers are not afforded appropriate training in this field.

Research Limitations/Implications:

The research was conducted in one of the eight police administrations in Slovenia. However, the frequency of police procedures with violent persons who have health issues is similar to that in the other police administrations, so with certain reservations we may generalise the findings to cover the whole of Slovenia.

Practical Implications:

This article offers some basic information to police managers for upgrading training and education programmes in this area of exercising police powers.

Originality/Value:

The article uncovers an entirely new field of police operation for which the police force is not specifically prepared.

Keywords: violence, patient, police, assistance, physical force, means of coercion

UDC: 351.741:614.253.8

Uporaba strokovnih prijemov pri osebah z zdravstvenimi težavami – policijski vidik

Namen prispevka

Namen prispevka je ugotoviti, ali policisti menijo, da imajo na voljo dovolj strokovnih znanj za obvladovanje nasilnega pacienta. Cilj je ugotoviti dejansko usposobljenost policistov za obvladovanje nasilnega pacienta ter ugotoviti prednosti in slabosti pri kompetencah policistov pri obvladovanju nasilnih.

Metode

S pomočjo kvantitativne metode raziskovanja, kjer je bil za metodo zbiranja podatkov prilagojen vprašalnik Gabrovca idr. (2014), smo ugotavljali stanje usposobljenosti policistov za obvladovanje nasilnega pacienta.

Ugotovitve

Ker obravnava nasilne osebe ni enaka obravnavi nasilne osebe z zdravstveno težavo ali pod vplivom drog oziroma zdravil, je pomembno, da je obravnava takšne osebe drugačna in prilagojena. Tako zdravstveni delavci in policisti pogosto sodelujejo pri obravnavi nasilnih bolnih oseb in se medsebojno dopolnjujejo. V mnogih primerih pa se zgodi, da so policisti prvi na kraju intervencije in so sami soočeni s takšno osebo. Specifičnost situacije narekuje potrebo po dodatnem znanju in usposabljanju za uspešno izvedbo policijskega postopka na način, da ta ne bo ogrozil kasnejšega tretmajskega postopka s pacientom. V analizi smo ugotovili, da je znanje policistov za obravnavo nasilnih oseb, ki imajo zdravstvene težave ali pa so pod vplivom drog oziroma zdravil, pomanjkljivo ter da niso deležni ustreznih usposabljanj.

Omejitve/uporabnost raziskave

Raziskava je bila opravljena na območju ene izmed osmih policijskih uprav v Sloveniji. Frekvenca postopkov policistov z nasilnimi osebami, ki imajo zdravstvene težave ali pa so pod vplivom drog oziroma zdravil, je podobna kot na območju ostalih policijskih uprav, zato lahko (z zadržkom) ugotovitve posplošujemo na celotno območje Slovenije.

Praktična uporabnost

Prispevek podaja ugotovitev dejanskega stanja usposobljenosti policistov pri ukrepanju v postopkih z obravnavano kategorijo oseb in daje osnovne informacije policijskim vodjem za nadgradnjo programov usposabljanj in izobraževanj s področja izvajanja policijskih pooblastil.

Izvirnost/pomembnost prispevka

Prispevek analizira novo neraziskano področje dela policije. Gre za izvirno delo na tem področju in lahko pomeni osnovo za nadaljnje raziskovanje.

Ključne besede: nasilje, pacienti, policija, strokovno sodelovanje, telesna sila, prisilna sredstva

UDK: 351.741:614.253.8

1 UNDERSTANDING THE INTERACTION OF AGGRESSIVE BEHAVIOUR OF ILL PERSONS AND POLICE INSTRUMENTS OF RESTRAINT

In the healthcare sector, staff often encounter a wide range of patients and persons in their care. It is frequently the case that these persons are violent, both to health workers, other persons, those close to them and even to themselves. A few years ago, aggression in the health sector was regarded as just part of the job, but nowadays there is zero tolerance towards it (Jambrošič & Bregar, 2015). Nevertheless, healthcare workers still see violence as part of their everyday work and accept it more than people in other occupations (Kores Plesničar & Kordić Lašič, 2004). The general belief is that it is mainly staff in psychiatric hospitals who encounter violent patients, which is valid to a certain extent, for as Kobal (2009, p. 104) found, »there is no psychiatry that does not encounter violence«. Most commonly, the violence of psychiatric patients is something encountered by health workers employed in care positions. At the same time, other stakeholders in dealing with such persons are also faced with it – police officers, external security operatives, emergency service personnel, and those in old people's homes (Gabrovec, 2014).

People with mental health issues are often violent, especially those affected by substance abuse, psychotic symptoms, and comorbidities with personality disorders (Davison, 2005). The main cause of aggressive behaviour in patients with mental health issues is their illness, while it is also partly due to the negative influence of their surroundings (Duxbury & Whittington, 2005). In psychiatry, the following groups of potentially violent patients are encountered: those dependent on psychoactive substances, patients with personality disorders, psychotic patients, psycho-organic syndrome patients, those with dementia, persons with learning difficulties, patients with epilepsy and those with depression (Perne, 2005). Data on violent behaviour in psychiatric hospitals, especially closed sections, shows that it ranges from 3.9% to 37% in different parts of the world and from 6% to 7% in Slovenia. Here, staff suffer the highest number of injuries due to violent behaviour in psychiatric wards, which points to the need for adequate knowledge among all

psychiatric staff regarding timely recognition and prevention of violent behaviour in psychiatric patients (Groleger, 2009). A total of 92.6% of health professionals working in intensive psychiatric wards stated that they had experienced verbal aggression from a patient in the past year, and 84.2% had experienced physical violence from a patient. Moreover, 63.5% of such staff had already been injured by a patient, while 24.6% had experienced sexual harassment from patients (Gabrovec et al, 2014; Gabrovec & Lobnikar, 2015). Emergency and rescue services also encounter violence from patients when administering care, and Gabrovec (2015) found that 78.0% of such health professionals had experienced verbal violence from a patient, 49.6% had experienced physical violence, and 26.8% had at some time in their career been injured by a patient.

Zeller et al. (2009) noted the frequency of violence suffered by health staff providing care in older adults' homes. Similarly, Gabrovec, and Eržen (2016) found that in the previous year care staff in older adults' homes most often encountered verbal violence (71.7%), physical violence (63.8%) and sexual violence (35.5%). A total of 35.5% of those surveyed had suffered injuries due to such violence. Staff most often experience verbal abuse from patients, but frequently also physical abuse and sexual harassment, with the levels of violence especially high in psychiatric care, older adults' homes, and in-home care (Gabrovec, 2017).

The purpose of this article is to present a review of the available literature, legislative regulations and research conducted on a sample of police officers in determining whether they consider that they have at their disposal sufficient expert knowledge to control a violent patient. The aim is to determine the actual capability of police officers to control a violent patient, and their strengths and weaknesses in this regard.

In article we will present terms and specific regulations and refer to police powers that relate to instruments of restraint and assistance, which are defined in detail in the Police Tasks and Powers Act (»Zakon o nalogah in pooblastilih policije [ZNPPol]«, 2013).

1.3 Violence, aggression, and aggressiveness

Violence should not be confused with aggression, nor should aggression be equated with aggressiveness, although they are similar and related concepts. Aggression is any form of behaviour intended to hurt someone and demonstrate dominance over them (Šolc, 2001). Aggressiveness is a lasting characteristic of an individual and is defined as an originally non-destructive and non-affective energy expressed in the desire to establish one's position through some activity and enterprise (Škrila Čuš, 2005). However, as a behavioural characteristic it can be seen in overbearing, violent or attacking actions towards other people. In the broader sense, it is a form of behaviour aimed at impacting or wounding another living being that wishes to avoid such behaviour. People are aggressive principally because, based on past experience, they have learned that they can be rewarded for such behaviour, or see specific reactions and aggressive behaviours as rewards in themselves. Their immediate environment also often directly encourages them towards violence (Pačnik, 1989). Aggressiveness has been observed both among

people and animals, where for animals it is necessary for survival, while people use it to attain mastery over individual conflicts and difficulties (Kores Plesničar, 2006).

Violence involves an expression of loss of control over one's actions, and in many respects, it thus becomes a normal part of everyday life that we often no longer even notice. Common to all forms of violence is that they disregard the freedom of the individual to decide for themselves. Violence means using physical force, grievous threats, insults, and power. The use of power by the strong over the weak adversely affects the dignity and integrity of the affected individuals (Močnik, 2009). The essential difference between violence and aggression is that aggression does not always end in violence involving physical force, grievous threats, insults, and power (Šolc, 2001). Violence is just one of form of aggression and is aggression that includes physical force and the causing of damage or injury to persons or property. Aggression also involves threatening, hateful or harmful behaviour in non-physical ways (Škrila Čuš, 2005).

We can observe various forms of violence: physical violence, psychological violence, sexual violence, verbal violence, economic, legal, ideological, and political violence. In the broadest sense, physical violence is the use of physical force or power against another person or group of persons that has a physical, sexual or psychological impact (Cvetežar & Pretnar Kunstek, 2005). We count the following as physical violence or abuse: striking (with or without an object), lashing out, beating, shoving, pushing, shaking, slapping, kicking, pinching and causing burns. It can also include the unjustified administering of medications, physical restriction, forced feeding and various physical punishments. Physical violence can be seen for the most part in outward signs, such as scratches, bruises, contusions, lacerations, grazes, breaks, wounds, cuts, puncture wounds, sprains, internal injuries, bleeding (Močnik, 2009).

The most refined and non-provable violence, and at the same time the most widespread, is psychological violence (Šolc, 2001). It is characterised by the causing of suffering, emotional pain, or sadness resulting from various verbal attacks, insults, threats, shaming, denigration, and harassment. Psychological violence is evident in emotional disturbance or agitation, extreme closure within oneself, being uncommunicative or unresponsive, being quick to anger, sadness, tearfulness, self-criticism, loss of self-respect, and poor self-image. Most physical violence begins with verbal violence, usually with an outbreak of anger (Močnik, 2009). Sexual violence usually begins with verbal harassment, which frequently crosses over into actual violence. It is present in both sexes and is a form of violence that the victims are less likely to talk about, since they are ashamed of it, which further emboldens the perpetrator. It relates to any involuntary sexual contact with a person who cannot give their consent to such behaviour, such as undesired groping, rape, sodomy, forced nudity and photographing for sexual stimulation. The outward signs are scratches and grazes in the area of the breasts and genitals, unexpected venereal diseases, anal and vaginal bleeding, and torn, dirty or bloody underwear (Močnik, 2009).

1.3 Violent ill persons and special protective measures

The concept of special protective measures (hereinafter referred to as SPM) is defined in Article 29 of the Mental Health Act (»Zakon o duševnem zdravju [ZDZdr]«, 2008). These are urgent measures whose use is intended to enable the treatment of a person or neutralise or control the dangerous behaviour of a person in cases where their own life or the lives of others are in danger, their health or the health of others is seriously endangered, or where such behaviour causes grave damage to themselves or others, and these dangers cannot be prevented with other, gentler measures. SPM accompanies emergencies in psychiatry – in other words, any situation of urgency where there is a need for immediate treatment to prevent the advance of a deteriorated state and heteroaggressive or autoaggressive behaviour (Pregelj & Kobentar, 2009 in Gabrovec, 2014).

SPM is used by psychiatric care staff only in cases where it is truly necessary, since their work mode is oriented towards applying other methods before this. The type of coercive protective measure that will be used is prescribed by a physician (Dernovšek & Novak Grubič, 2001). In cases of severe violent behaviour both internal and external security services are required, since, in line with ethical criteria, their education and training, medical staff are not professionally required to control such behaviour (Novak Grubič et al., 2018). The use of SPM is not limited just to psychiatric institutions, and reasons for their use also arise outside the hospital treatment of patients and in other types of institution or social protection institutions. Healthcare institutions are bound in terms of spatial conditions, the number of health staff and appropriate training to ensure the professional and most humane possible implementation of SPM (Novak Grubič et al., 2018). SPM represent a major encroachment on the patient's integrity and liberty. We may observe two groups of measures, with the first being intended to deal with patients, and the second to eliminate a patient's dangerous behaviour (self-injury, threatening others, destruction of property) (Možgan, 2009). The »ZDZdr« (2008) prescribes as SPM physical restraint and confinement to one space or room.

In addition to these, some would add various degrees of more or less invasive forms of control, the use of an enclosure bed, and restraint in a wheelchair, armchair or ordinary chair (Možgan, 2009). In terms of the method imposing these, according to Možgan (2009) we may differentiate (a) the use of medications (receiving antipsychotics, benzodiazepine, or a combination of both); (b) physical measures (discrete control, constant control, the use of an enclosure bed for prone patients, standard restraints using special belts, restraining upper and lower extremities and restraint in a wheelchair), and (c) a combination of both.

The indications for physical restraint are the prevention of direct threat of injury for the patient, other patients in the ward and staff. They are also used to prevent serious disruption in the therapeutic programme (agitated patient whose behaviour significantly hinders normal activities in the ward) and serious damage to the inventory, by reducing stimulation from the environment that harms the patient (for a manic or delirious patient who cannot become calm in the normal ward environment). Physical restraint can also be carried out at the patient's request, when they can envision not being able to control their behaviour clearly. Contraindications for physical restraint include the use of this approach

as a substitute for treatment using a medication, as a punishment for a patient's disagreeable behaviour that is not dangerous, when physical restraint cannot be imposed without significantly endangering the safety of the patient and staff, and when physical restraint could have a severe adverse effect on the patient's physical condition. Caution should thus be used when applying physical restraint, especially with children, the elderly or patients with severe physical impairments (Novak Grubič et al., 2018).

The use and specific features of SPM are approved by the relevant physician, but the entire medical team is involved in the actual decision-making. Where the use of SPM is needed, the measure selected is the one that is most effective and least restrictive in the given situation. If the selected SPM does not suffice, a more restrictive method of applying SPM can then be employed. It is possible right from the outset to opt for the most restrictive SPM, if the assessment is that this is the only possibility of ensuring safety. The use of SPM should last only for as long as is necessary with regard to the reason for imposing it, but in any case no longer than four hours for the measure of restraining with belts or no longer than 12 hours for the measure of restricting freedom of movement within a single space or room (Možgan, 2009). In cases where a physician is not present, SPM may also be implemented by another health worker in a psychiatric hospital or professional worker in a social protection institution. However, they must immediately notify the physician, who will assess the justification for imposing the measure. If the physician does not order the measure, it is immediately ceased (»ZDZdr«, 2008).

Throughout the duration of the SPM, the person who has been subjected to it is supervised, their vital functions are monitored, and they are dealt with professionally. Equally, the precise details of the reason, purpose, duration and supervision of the implementation of the SPM are entered in the medical records of the patient. Records are kept of SPM, and with regard to the actual ordering and implementation such measures the physician must within 12 hours of ordering the measure notify in writing the director of the psychiatric hospital or social protection institution, the next of kin, lawyer and authorised representative of the patient (»ZDZdr«, 2008).

a. Legal basis for special protective measures

In Slovenia, the primary legal document defining the use of SPM is the Mental Health Act (»ZDZdr«, 2008), which applies only to psychiatric hospitals and social protection institutions. The Act defines SPM as just two measures: physical restraint and confinement within one space or room. The Act lays down that SPM should be used under special supervision and in secure wards. Equally, the Act lays down who may order SPM and in what cases, who needs to be notified of such measures, how much time the measure can last, and the supervision of the person during the imposition of the measure (Bregar et al., 2012). Since the Act permits such measures only within psychiatric hospitals or social protection institutions and not in other hospitals or public health institutions, a consideration arises as to the use of SPM or similar measures in non-psychiatric hospitals (Bregar et al., 2012). In 2012 the Nurses and Midwives Association of Slovenia adopted a Protocol on the physical restraint of patients in hospitals using belts (Bregar et

al., 2012). The Protocol, with which staff must be familiar and which they must observe consistently, is intended to standardise the approach and steer action in cases where a patient needs to be restrained using physical protective measures. It precisely defines the methods of ensuring safety and enabling treatment by means of restraining and tools of restraint (Bregar et al., 2012). In 2018 the Association of Psychiatrists at the Slovenian Medical Association adopted Recommendations and guidelines for the use of special protective measures in psychiatry (Novak Grubič et al., 2018). These are necessary in order to ensure the appropriate handling of emergencies in patients with mental disturbances. They contain a review of SPM, their criteria, when they can and must be used, and their implementation and methods of documentation. These guidelines, which emphasise the need for professionalism and continuous training of personnel, are also necessary to protect and respect the integrity and rights of the patient (Novak Grubič et al., 2018).

b. Physical restraint with belts

As Marinič (1999) states, physical restraint is one of the most stressful events for patients and staff. In Slovenia staff use Segufix belts and straps to physically restrain the patient in a hospital bed, for the purpose of enabling treatment, and neutralising or controlling their behaviour (Marinič, 1999). The belts are felt-lined and connected to each other with a magnetic locking system. Their application requires the participation of at least five properly trained health professionals. Most often medication measures are applied simultaneously with the use of belts. While the measure is being carried out, continuous monitoring of the patient is needed with the direct presence of staff or observation from a neighbouring room. Every four hours the patient must be examined by a physician, who will make a judgement as to ending and substituting the restraint with less restrictive measures (Novak Grubič et al., 2018). The special protective measure of physical restraint should not last more than four hours. After four hours have elapsed, the physician then checks the justification for repeated use of SPM (»ZDZdr«, 2008). A set of belts and straps for SPM comprises (Bregar et al., 2012):

- body strap (abdominal strap) – 1 pc,
- cuff strap for hands with felt – 2 pcs,
- cuff strap for feet with felt – 2 pcs,
- strap for securing legs to the bed – 1 pc,
- magnetic lock buttons – 8 pcs, and
- magnet – 2 pcs (red).

The following details of carrying out the measure are summarised from the Protocol for Physical Restraint of Patients in Hospitals (Bregar et al., 2012).

Implementers:

- measure prescribed by physician,
- SPM may be applied by a graduate nurse, graduate midwife, healthcare technician or physician.

Number of implementers:

- at least two persons for a patient that is cooperating,

- for an aggressive patient, at least five persons (psychiatric practice specifies five persons – one at each extremity and the leader at the patient's head).

Materials and tools:

- standardised belts, which are always clean, ready and in a set,
- bed enclosure.

Preparation of patient:

- the need for the measure and the method of carrying it out must be explained to the patient.

Cause of implementing special protective measures:

- protection during the use of therapeutic tools,
- behavioural changes in the patient.

Execution of measure:

- selection of the appropriate size of the belt,
- preparation of selected equipment,
- the bed is raised to an appropriate height and prepared so that it can be accessed from all sides,
- removal from the patient's immediate environment of objects that could be a danger to them or their surroundings (e.g. lighter, knife, scissors, razor or other such items),
- the belts are then secured (Bregar et al., 2012).

c. Confinement within one space or room

Confinement within one space or room is defined as SPM by the »ZDZdr« (2008), but at present this measure is not applied in Slovenian psychiatric hospitals. This is the confinement of an individual patient in a small, safe space for the purpose of mitigating agitation and aggression (Novak Grubič et al., 2018). The measure is ordered and signed by a physician, except in urgent cases where a physician is not present when it can be imposed by another health worker or professional associate, who immediately notifies the physician, who in turn approves or terminates the measure. Such confinement may only last as long as needed, depending on the reason for imposing it, but in any case no longer than 12 hours. After that time has elapsed the physician must confirm the justification for repeated use of the measure (Zbornica zdravstvene in babiške nege Slovenije, 2018). This type of confinement involves being kept in a special space or room with padding made of pleasant, soft materials that can be easily sanitised. The space has visual and audio monitoring via a video system. A patient alone in such a space can still be contacted via a loudspeaker (Zbornica zdravstvene in babiške nege Slovenije, 2018).

1.3 Instruments of restraint of the police

The use of instruments of restraint is just one of several police powers with which police tasks are carried out. The »ZNPPol« (2013) states that police tasks are to be performed by observation, patrolling, intervention, ambush, heightened control,

and security action. Police officers are enabled to perform their official tasks by legally defined measures, i.e., police powers. These are measures defined by law that generally involve an encroachment on human rights and fundamental freedoms, and other rights of the individual. Since the execution of police powers involves encroachments on specific human rights or fundamental freedoms, the legislators have entrusted these powers solely to police officers. Other citizens must obey the demands of police officers, and they may not exercise police powers since they would thereby be committing a crime (Celestina & Hudrič, 2014). Police powers are a tool for successfully and effectively carrying out tasks specified in law and implementing regulations. They represent a mandate that the police require for successfully carrying out tasks and entitlements provided by law, and no other bodies or citizens have such tasks and entitlements. This does not just relate to the rights of police officers, but also to the duty whereby in legally specified cases they may carry out against persons certain measures in the manner laid down by law and implementing regulations (Žaberl, 2006). As already mentioned at the beginning, the use of instruments of restraint is one of a number of lawful police powers. Police officers employ them for physical coercion or in order to force someone to do something. There are various means of coercion, such as the use of one's own physical force or the force of animals (police dog, mounted police officer), and there are various implements that can be used in this context (baton, handcuffs and means of restraint, gas agents, means of forcing vehicles to stop, water cannon, special motor vehicles and firearms) (Žaberl, 2006). However, their use is resorted to only when a police officer cannot, through a warning, order or another exercise of authority, prevent or avert danger and, consequently, carry out a police task. Through their use, the individual is coerced into doing or not doing something. Means of coercion are set out in law and categorised by type, meaning that police officers may not use means other than those specified. Other means and methods, while not prescribed in law or categorised, may be used by police officers only for restraining and handcuffing persons, for forcible stopping of vehicles or when police officers' lives or the lives of others are directly threatened. These means and methods may be used if they are comparable and appropriate in terms of the expected consequences of their use (Celestina & Hudrič, 2014).

The use of instruments of restraint is regulated in point two of the third section of the »ZNPPol« (2013), and their manner of application is defined in the Rules on Police Powers. Given the topic in question, when we talk about instruments of restraint it is also essential to mention police assistance, as defined by the »ZNPPol« (2013). It is important precisely because it is a key link in cooperation between health workers and the police, most commonly in dealing with the very persons who are the subject of our study. Police assistance is defined in Article 12 of the »ZNPPol« (2013), where it states that the police shall provide help to state authorities and self-governing local communities and to the holders of public authorisation only when they are carrying out public authorisations based on legally defined tasks and competences, if in implementing their tasks they encounter resistance or threats or if these may be justifiably anticipated. The duty of the police to cooperate and offer assistance to health workers is also defined

and regulated by the »ZDZdr« (2008) and the Rules on the cooperation between medical staff and rescue service and police (»Pravilnik o načinu sodelovanja med zdravstvenim osebjem in reševalno službo ter policijo«, 2009), which lay down that in cases where violence is anticipated in advance from a patient, and it is likely that the health workers will not be able to control it, the physician may request in advance the assistance of the police. In this case, the police are bound to cooperate with the health workers and emergency medical services and offer them the necessary assistance for as long as medical measures cannot contain the person's threat. Equally, the police are bound to provide assistance in carrying out the holding of a person without their consent and in carrying out emergency transport in an ambulance without the person's consent.

As stated by the Rules on the cooperation between medical staff and rescue service and police (»Pravilnik o načinu sodelovanja med zdravstvenim osebjem in reševalno službo ter policijo«, 2009), the assistance of the police may be requested when, due to the nature of the mental disturbance of the person, it is essential for the person's movement or contact with their surroundings to be prevented even before the procedure is carried out for receiving treatment without consent, and if the legal conditions for receiving such treatment without consent are met. Upon fulfilment of the stated conditions, the physician may request the assistance of the police in holding the person and in ordering their transport to the hospital in an ambulance without their consent. Prior to receiving assistance, the physician must brief the police on all information that is important in the specific case. The physician is the one who assesses when police assistance is no longer needed, and the threat can be contained through medical measures.

1.4 Therapeutic process and proportionality in the use of force

As Gabrovec (2014) has found, the receiving and treatment of a psychiatric patient is a therapeutic process that begins with the reception or referral for reception. The successful treatment of mental disturbances requires that the individual cooperates and accepts the help of professional staff and their close family and friends (Fergola, 2007). Since the hospitalisation of a patient is usually urgent and is only rarely the patient's own wish, the hospitalisation of such a patient is fear-inducing and traumatic. However, the hospitalisation process can also be encouraging for the patient, something that depends on the institution itself, the family relations, friends, the reaction of health workers and the method of reception. Upon being received, patients are often frightened, untrusting, tense and even verbally and physically violent, which may be a consequence of their past experiences or ideas of what might happen next, which the patients create and are fuelled by the media (Komazec, 2000).

Nowadays, psychiatry applies ways of handling patients that are the most patient-friendly, non-traumatic and effective. Such handling must observe all the principles and laws with regard to not encroaching on human integrity and not violating human rights and freedoms. Account must always be taken of a patient's dangerous behaviour in the past, the diagnosis of the illness for which they are being treated, and their current behaviour. To foresee and prevent the

potentially dangerous behaviour of a patient, health workers need to be skilled in observing, with both theoretical and practical knowledge, and able to assess the situation correctly (Možgan, 2009). With sufficiently early recognition of the risk of aggressive behaviour and appropriate action, health workers can prevent later complications, including injuries to patients and staff (Groleger, 2009). To avoid the possible consequences of the patient's violent behaviour, it is all the more important to foresee well in advance such a development. To this end, a range of questionnaires and scales are in use, including the currently most revised, simplified and increasingly used around the world, the BVC – Brøset violence checklist (Perne, 2005). Equally, to prevent outbreaks of aggressiveness and ensure the safety of patients and employees, it is vital to be familiar with the procedures for managing aggressiveness, the best known of which are de-escalation techniques (Jambrošič & Bregar, 2015). Attention must also be paid to behaviour that points to the potential for aggression to arise (Andrejek Grabar, 2009). If heightened aggressiveness is recognised and efforts are made early enough to reduce it, it is often possible to avoid more restrictive measures that are unpleasant both for the patient and staff (Groleger, 2009). Nevertheless, it is often impossible to avoid a patient's dangerous behaviour, for which reason special protective measures must be employed, and these are stressful for everyone involved (Možgan, 2009). Since SPM are highly traumatic, special attention needs to be paid to the principle of proportionality, meaning that the measures must be in proportion to the risk level and may not be substituted for less coercive measures. Depending on the individual case, a decision needs to be made as to which measure for a given person is least traumatic, and an assessment must be made about whether the expected benefits outweigh the possible drawbacks. SPM must be selected based on the latest findings and adjusted in terms of duration to the circumstances. Equally, account must be taken that physical or psychological harm may be done during their application. The guiding principle must always be the protection of rights and dignity, and the selected SPM may not serve to shame the patient or give them the feeling that it is some form of punishment (Bregar et al., 2012). Even when health workers opt for police assistance, it is important that the scope of measures used to avert the threat posed by the person is not greater than absolutely necessary (»Pravilnik o načinu sodelovanja med zdravstvenim osebjem in reševalno službo ter policijo«, 2009).

2 METHOD USED, SAMPLE AND QUESTIONNAIRE

From 2 September to 2 November 2019, we surveyed male and female police officers employed at the Novo Mesto Police Administration. We used an adapted questionnaire developed by Gabrovec et al (2014), divided into seven sets of questions.

The questionnaire contained questions (a) on the frequency of encountering various forms of violence at work and how many times those surveyed had experienced such behaviour on the part of persons with health issues or under the influence of medications or drugs, followed by (b) a set of questions where we sought to identify what emotions the respondents encountered while carrying

out tasks with an aggressive person with health issues or under the influence of drugs. Respondents were offered nine different emotions, where they assessed to what extent they faced the described emotion, using a scale from 1 (not at all) to 5 (very much); the rate of internal consistency of this part of the questionnaire, measured using Cronbach α , amounted to .941. This was followed by seven statements with which we measured the level of empowerment of respondents from the organisation (police force) to effectively face situations where they had to carry out tasks with an aggressive person with health issues or under the influence of drugs; the responses were measured by means of a scale from 1 (not at all) to 5 (very much); the rate of internal consistency of this part of the questionnaire, measured using Cronbach α , amounted to .973. In the next set, we used eight statements to measure the influence of certain factors on the safety and quality of handling of the user upon an outbreak of violent behaviour; a five-level scale from 1 (not at all) to 5 (very much) was used; the rate of internal consistency of this part of the questionnaire, measured using Cronbach α , amounted to .949. In the final set of questions, we used four statements to measure the assessment of respondents about the education or training provided to police officers for working with aggressive persons with health issues or under the influence of drugs. A five-level scale from 1 (not at all) to 5 (very much) was used; the rate of internal consistency of this part of the questionnaire, measured using Cronbach α , amounted to .959. For all the substantive sets used in the questionnaire, we may conclude that they are internally highly consistent and useful for further analysis.

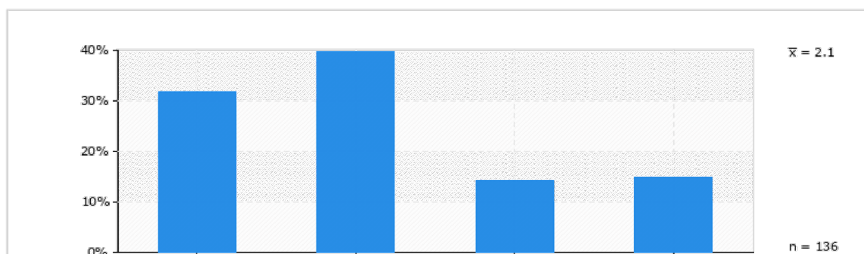
We conducted the survey by placing the questionnaire in the web environment 1ka, and we invited the participation of police officers from the Novo Mesto Administration who perform work in the field and may be sent on an intervention assignment where they could encounter aggressive persons with health or drug issues.

In total, the questionnaire was correctly completed by 281 police officers performing field or intervention work, although 20 did not answer all the items. Of the 261 respondents who answered the questions used to gather their demographic data, 81% of the officers were male and 19% female, with an average age of 40.7 years and an average length of service of 18.8 years. The largest number of respondents had a secondary education (41%), followed by those with post-secondary education (30%), one fifth had a higher education and one-tenth had an academic university education. Participation in the survey was voluntary, with respondents being guaranteed anonymity and confidentiality for their responses.

3 RESULTS

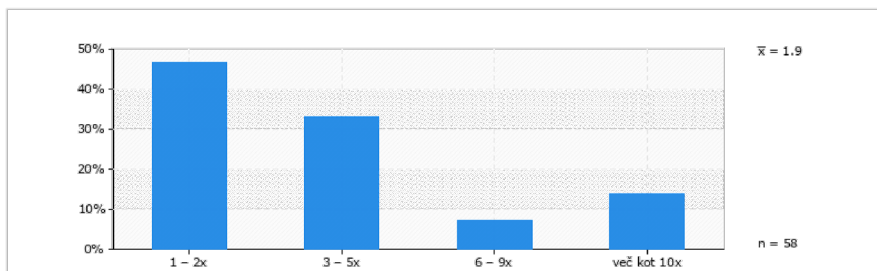
The respondents were first asked if and how frequently they had encountered verbal and physical violence in the past year at work and if they had ever been injured at work. Out of 278 respondents, 136 (49%) answered in the affirmative, meaning that nearly half of them had faced verbal violence in the past year. Of these, 43 (32%) had encountered verbal violence at work once or twice, 54 (40%) had encountered it three to five times, 19 (14%) six to nine times and 20 (15%) respondents had encountered it more than ten times.

Figure 1:
Frequency
of police
encountering
verbal
violence at
work in the
past year



In the past year, 58 out of 276 respondents (or 21%) encountered physical violence at work. The largest number of respondents encountered physical violence at work in the past year once or twice (27 or 47%), 19 (33%) had encountered this three to five times, 4 (7%) six to nine times, and eight (14%) respondents had encountered this more than ten times. Injuries at work had already been suffered by 110 (40%) of the respondents, of which 37 had suffered such injuries once, 35 twice, 24 three times, eight four times and six as many as five times.

Figure 2:
Frequency
of police
encountering
physical
violence at
work in the
past year



We then sought to find out if and how many times respondents had encountered verbal and physical violence in the past year at work from persons with health issues or under the influence of drugs/medications, and how many times such persons at work had injured them. Out of 277 respondents, this form of violence was encountered by 110 (40%) in the past year. Those who answered yes to this question were then asked how many times this had happened. Half of them (55, or 50%) responded that they had encountered verbal violence from such persons once or twice in the past year. Slightly fewer (39, or 35%) responded that they had encountered this form of violence three to five times in the past year. Then eight (7%) responded that they had encountered verbal violence from such persons six to nine times or more than ten times in the past year. Physical violence from persons with health issues or under the influence of drugs/medications was encountered at work in the past year by 49 (18%) out of 274 respondents, of whom more than half (28, or 57%) experienced this one or two times. Slightly fewer (18, or 37%) had encountered this form of violence three to five times, two respondents (4%) six to nine times, and one respondent (2%) had encountered this more than ten times in the past year. Injuries caused by persons with health issues or under the influence of drugs/medications were suffered at work by 35 (13%) respondents, of whom 28 suffered injuries once, four twice, two suffered them three times and one four times.

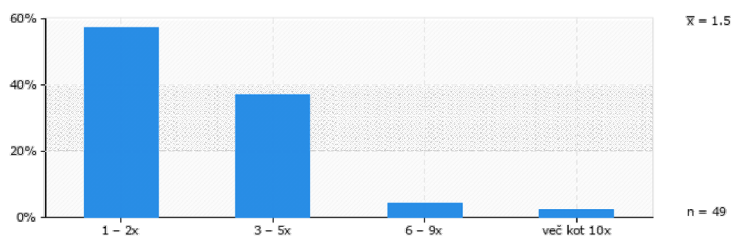


Figure 3:
Frequency of police encountering physical violence at work in the past year from persons with health issues or under the influence of drugs/medications

We also wished to know what emotions and states are experienced by the respondents when encountering an aggressive person. Emotions and states foreseen in advance, such as fear, uncertainty, impotence, lack of knowledge, anger, despair, a feeling of threat, and a lack of understanding from colleagues and superiors, were assessed by respondents using a five-level scale from 1 (completely disagree) to 5 (agree very much). The responses are shown in Table 1 below.

	N	Average	Standard deviation	Difference between male/female police officers
Feeling of threat	268	3.04	1.04	none
Fear	269	2.85	.98	none
Uncertainty	269	2.80	.99	$t = -2.12; p = .035$
Anger	267	2.55	1.07	none
Lack of understanding from superiors	270	2.55	1.03	none
Lack of understanding from colleagues	266	2.26	.98	none
Impotence	269	2.16	.90	none
Lack of knowledge	268	2.04	.91	$t = -2.42; p = .016$
Despair	266	1.85	.80	none

from 1 – completely disagree to 5 – agree very much

Table 1: Level of agreement or disagreement with the statement: “When you encounter a person who is aggressive, you experience the following emotions and states”

The results show that it is hard to pinpoint a specific emotion or state that the respondents experience more distinctly upon encountering an aggressive person. Most commonly, they experience feelings of threat, fear, and uncertainty. A total of 7% agreed very much that they experienced a feeling of threat, 25% agreed and 41% of respondents agreed partly. A total of 4% agreed very much with the feeling of fear, 18% agreed and 45% of respondents agreed partly. A total of 3% agreed very much with the feeling of uncertainty, 20% agreed and 40% of respondents agreed partly. The respondents least frequent experiences are feelings of despair, lack of knowledge and impotence. A total of 43% did not agree with the feeling of despair, and 38% of respondents did not agree at all. A total of 43% did not agree that they experienced a feeling of lack of knowledge, and 31% of respondents did

not agree at all with this statement. A total of 44% did not agree with the feeling of impotence, and 25% of respondents did not agree at all. We then used a t-test to verify whether these feelings are differentiated between male and female police officers. We found statistically significant differences in the sensing of uncertainty and lack of knowledge; female officers reported that they experienced both these emotions more frequently than male officers. We also checked the link between these emotions and the level of education, and determined that education has no statistically significant link with any of the emotions described. Younger respondents more frequently feel threatened ($r = -.115$; $p = .010$), while for the other emotions the participants' age or length of work experience had no statistically significant links (measured using the Pearson correlation coefficient).

In the next set of questions, we sought to obtain from the police officers surveyed an assessment of whether they were provided with all the means for dealing with violent persons, if their chiefs had a clear picture of the risks regarding provisions for violent persons, if their chiefs were familiar with the errors that arise in the area of ensuring safety, if their chiefs work to ensure conditions that support the safety of users and staff, if the safety of employees and users has the greatest importance in the organisation, if the organisation responds to outbreaks of violence, and if the organisation ensures supervision over the subduing of a violent user.

Table 2:
Assessment
of empower-
ment from
the organ-
isation for
effective
handling of
persons with
health issues
or under the
influence of
drugs

	N	Average	Standard deviation
I have all means available for the safe handling of violent users.	266	3.31	.98
The work organisation responds to outbreaks of violence.	264	3.28	.93
The safety of employees and users is of the greatest importance in our organisation.	264	3.22	1.07
The heads of the work organisation are properly familiarised with the types of errors that actually arise in the area of ensuring safety.	264	3.12	.89
The work organisation ensures supervision over the subduing of a violent user.	265	3.11	.89
The heads of the work organisation work to ensure conditions that support the safety of users and staff.	264	3.09	.88
The heads of the work organisation have a clear picture of the risks regarding provisions for violent persons and safety of staff.	265	2.98	.89

from 1 – completely disagree to 5 – agree very much

We found that the respondents have all means available for the safe handling of violent users, that the work organisation responds to outbreaks of violence and that the safety of employees and users is of the greatest importance in the organisation. A total of 44% agreed (very much) with the first statement, and 38% of respondents agreed partly. A total of 41% agreed (very much) with the

second statement, and 44% of respondents agreed partly. A total of 36% agreed (very much) with the third statement, and 44% of respondents agreed partly. The lowest level of agreement was observed in the statement that the heads of the work organisation have a clear picture of the risks regarding provisions for violent persons and the safety of staff. A total of 27% agreed (very much) with the statement, and 46% of respondents agreed partly. Using a t-test, we sought to determine whether there were any statistically significant differences between male and female police officers in their assessments in the above table, but we found no such differences. The statement that the "Heads of the work organisation have a clear picture of the risks regarding provisions for violent persons and safety of staff" found more agreement among older ($r = .169$; $p = .006$) and more experienced ($r = .144$; $p = .019$) respondents, while we found no other correlations, measured using the Pearson correlation coefficient, with regard to the education, age or work experience of respondents.

In the next set of questions, we determined how certain factors affect the safety and quality of dealing with users upon the outbreak of violent behaviour. Respondents were given statements as set out in Table 3 below.

	N	Average	Standard deviation
Conflicts between members of the team affect the safety and quality of work with violent persons.	263	3.63	.96
A record is made of any unfortunate event (outbreak of violence, other incidents).	262	3.28	1.10
Employees have precise instructions and protocols for how to act upon an outbreak of violence (what to do, who to call, etc.)	261	3.07	.86
After an outbreak of violence or an incident, decisions are taken to improve work in the future.	262	2.89	.970
In your work you rely on "luck" for everything to be OK, for nothing bad to happen.	263	2.73	1.08
After an outbreak of violence or an incident, we are offered team consideration and support.	261	2.67	.95
We are sufficiently motivated and rewarded for high quality and safe work.	263	2.51	.93
The number of employees in each shift is sufficient.	262	1.76	.90

from 1 – completely disagree to 5 – agree very much

Table 3: The effect of certain factors on the safety and quality of dealing with users upon the outbreak of violent behaviour

We found that respondents agree most with the statement that conflicts between team members affect the safety and quality of work with violent persons. A total of 55% agreed (very much) with this statement, and 34% of respondents agreed partly. There was also greater agreement with the statement that a record is kept of any unfortunate event, where a total of 43% agreed (very much)

with the statement, and 34% of respondents agreed partly. The highest level of disagreement was observed for the statement that the number of employees in each shift is sufficient, where nearly half of respondents (48%) did not agree at all, 32% did not agree and just 15% partly agreed. We also observed disagreement with the statement that respondents are sufficiently motivated and rewarded for high quality and safe work. A total of 48% did not agree (at all) with this statement, and 40% of respondents agreed partly. The gender of respondents did not have any statistical significance with regard to the responses shown in the table above, but older ($r = .146$; $p = 0.18$) and more experienced ($r = .130$; $p = .036$) respondents agree more with the statement that they are sufficiently motivated for high quality and safe work, while younger respondents rely more than their older colleagues on luck for everything to be OK and for nothing to happen to them ($r = -.123$; $p = .045$). We did not detect any other links, and we found that education was not linked to any differences in responses to the statements shown in the above table.

In the final set of questions we determined whether the respondents, in their opinion, have sufficient knowledge to control violent persons and violent persons with health issues or under the influence of medications/drugs, and if they can access appropriate training to deal with such persons. The results are shown in Table 4 below.

Table 4:
Training to
control violent
persons with
health issues

	N	Average	Standard deviation	Difference between male/female police officers
The knowledge I possess is sufficient for controlling violent persons.	263	3.18	.84	$t = 2.239$; $p = .017$
The knowledge I possess is sufficient for controlling violent persons with health issues or under the influence of medications/drugs.	263	2.88	.86	$t = 3.129$; $p = .002$
Adequate training is available to personnel for the safe care of violent persons.	263	2.69	.88	None
Adequate training is available to personnel for the safe care of violent persons with health issues or under the influence of medications/drugs.	263	2.44	.88	None

from 1 – completely disagree to 5 – agree very much

We can state that nearly half (48%) of respondents at least partly agree that their knowledge is sufficient for controlling violent persons. There was slightly more disagreement than agreement with the statement that the knowledge respondents possess is sufficient for controlling violent persons with health issues or under the influence of medications/drugs. A total of 30% did not agree

(at all) with this statement, 46% of respondents agreed partly, and 25% agreed. Disagreement was noted for the statement that adequate training is available to respondents for the safe care of violent persons. A total of 41% did not agree (at all) with this statement, and 42% of respondents agreed partly. The respondents disagreed most strongly with the statement that adequate training is available to personnel for the safe care of violent persons with health issues or under the influence of medications/drugs. A total of 54% did not agree (at all) with this statement, and 35% of respondents agreed partly. There was also a statistically significant higher frequency of agreement from male police officers than female officers with the statements that their knowledge of controlling violent persons is sufficient and that they are sufficiently skilled in controlling violent persons with health issues or under the influence of medications/drugs. Age, length of service or education had no statistically significant connection with the statements in the above table.

4 DISCUSSION

The results of the analysis point to a fair number of issues which should be considered in further work, particularly in terms of educating police officers. As is well known, police officers have standards for police procedures, but we can find no particular procedures in these standards for persons with health issues (in the health sector they would be termed patients). The fact is that acting against the stated categories of person is a specific field of action and cannot be equated with procedures for dealing with intoxicated persons. Although they are similar to a certain extent, especially in terms of the use of expert grips/holds, ultimately these procedures cannot be the same. Upon the first contact with the parties involved, police officers have a hard job identifying which category of person they are dealing with. Of the police officers who in the past year had encountered physical violence from persons who were suffering from health problems or were under the influence of drugs/medications (49, or 18% of respondents), most encountered this form of violence up to five times. The proportion of police officers who had encountered this form of violence in the past year represents as much as 94% of respondents. In dealing with and subduing such persons, police officers can make use of the same powers as when they deal with persons who do not have health issues. They have access to a wide variety of instruments of restraint to control them, depending on the intensity of resistance or attack, and these means can also be proportionally enhanced. At the same time, there are laws, guidelines and protocols setting out grips/holds and forms of cooperation between police officers and health professionals when they encounter such persons (Pravilnik o načinu sodelovanja med zdravstvenim osebjem in reševalno službo ter policijo, 2009).

The results of this study indicate that the total share of surveyed police officers who do not agree with the statement that they possess sufficient knowledge to control such persons is just under a third, which may later affect the course of treatment effectiveness (Gabrovec, 2014). Looking at the results, we can see that the share of those who agree that they have sufficient knowledge for these procedures is equal to the share of surveyed police officers who view that they do

not possess this knowledge. More than half of the surveyed police officers believe that there is not adequate training available for the controlling and safe care of violent persons with health issues or under the influence of medications/drugs. It should be especially noted that female police officers report that they lack such knowledge. We have found that most police officers believe that they lack appropriate knowledge for controlling such persons, and this lack is even greater in terms of adequate training. They do indeed have a more positive opinion regarding having sufficient knowledge and training to control violent persons without health issues, but they are also aware that dealing with and controlling such persons is a specific kind of activity that requires a different kind of approach. Given the awareness among police officers that they lack sufficient knowledge to control such persons, we may conclude that they would be willing to supplement this through appropriate training. Training should include health workers who are in regular contact with such persons and who could familiarise police officers with their methods and courses of action («Pravilnik o načinu sodelovanja med zdravstvenim osebjem in reševalno službo ter policijo», 2009; Žaberl, 2006). Even some basic knowledge would make it easier for police officers to deal with and control such persons, and thereby facilitate more effective treatment of the patient later on (Gabrovec, 2014). We also anticipate that with additional knowledge and the right approach both the number of times and intensity of using means of coercion against persons with health issues would diminish.

REFERENCES

- Andrejek Grabar, E. (2009). Terapevtski ukrepi pri agresivnem pacientu [Therapeutic measures toward a violent patient]. In S. Čelan Stropnik (Ed.), *Funkcionalno izobraževanje iz psihiatrične zdravstvene nege in psihiatrije* (pp. 119–128). Univerzitetni klinični center Maribor.
- Bregar, B., Kadivec, S., Kramar, Z., Marinšek, N., & Naka, S. (2012). *Protokol fizičnega oviranja s pasovi pacientov v bolnišnicah* [The protocol of usage of physical restraint over patients in hospitals using belts]. Zbornica zdravstvene in babiške nege Slovenije, Zveza strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije. <https://www.zbornica-zveza.si/wp-content/uploads/2019/09/Protokol-fizi%C4%8Dnega-oviranja-s-pasovi-pacientov-v-bolni%C5%A1nicah-.pdf>
- Celestina, I., & Hudrič, G. (2014). *Kaj moramo vedeti o policijskih postopkih?* [What we need to know about the police procedures]. Ministrstvo za notranje zadeve Republike Slovenije.
- Cvetežar, I. Š., & Pretnar Kunstek, V. (Eds.). (2005). *Okvirne smernice za obravnavanje nasilja na delovnem mestu v zdravstvu* [Framework guidelines for addressing workplace violence in the health sector]. Delovna skupina za nenasilje v zdravstveni negi, Zbornica zdravstvene in babiške nege Slovenije – Zveza društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije.
- Davison, S. E. (2005). The management of violence in general psychiatry. *Advances in Psychiatric Treatment*, 5(11), 362–370. <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/EF671B6513F53315E0B46A7656B064DA/>

S1355514600002509a.pdf/management_of_violence_in_general_psychiatry.pdf

- Dernovšek, M. Z., & Novak Grubič, V. (2001). *Priporočila in smernice za uporabo posebnih ukrepov v psihiatriji* [The recommendations and guidelines for the use of special measures in psychiatry]. Viceversa.
- Duxbury, J., & Whittington, R. (2005). Causes and management of patient aggression and violence: Staff and patient perspectives. *Journal of Advanced Nursing*, 50(5), 469–478. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.339&rep=rep1&type=pdf>
- Fergola, B. (2007). *Sprejem proti volji pri bolniku z duševno motnjo* [Diplomsko delo] [The admission against the will of the mental health disordered patient into the hospital [Diploma thesis]]. Fakulteta za zdravstvene vede.
- Gabrovec, B. (2014). *Organizacijski model zagotavljanja varnosti in kakovosti pri obravnavi psihiatričnega bolnika z vidika različnih deležnikov* [Doktorska disertacija] [Organizational model of safety and quality assurance in psychiatric patient treatment in terms of diverse participants [Doctoral dissertation]]. Fakulteta za organizacijske vede.
- Gabrovec, B. (2015). The prevalence of violence directed at paramedic services personnel. *Obzornik zdravstvene nege*, 49(4), 284–294. <https://doi.org/10.14528/snr.2015.49.4.60>
- Gabrovec, B. (2017). Violence towards nursing employees in Slovenia. *Varstvoslovje*, 19(2), 151–166.
- Gabrovec, B., & Eržen, I. (2016). Prevalence of violence towards nursing staff in Slovenian nursing homes. *Zdravstveno varstvo*, 55(3), 212–217.
- Gabrovec, B., & Lobnikar, B. (2015). The analysis of the role of an institution in providing safety and quality in psychiatric health care. *Anadolu Psikiyatri Dergisi*, 16(6), 420–425.
- Gabrovec, B., Eržen, I., & Lobnikar, B. (2014). The prevalence and the nature of violence directed at the medical staff in psychiatric health care in Slovenia. *HealthMed*, 8(2), 228–234.
- Groleger, U. (2009). Agresivnost [Aggressiveness]. In P. Pregelj, & R. Kobentar (Eds.), *Zdravstvena nega in zdravljenje motenj v duševnem zdravju* (pp. 288–294). Rokus Klett.
- Jambrošič, I., & Bregar, B. (2015). Nasilje pacientov do zaposlenih v zdravstveni negi [Aggressiveness of patients against health staff]. In S. Majcen Dvoršak, T. Štemberger Kolnik, & D. Klemenc (Eds.), *Z optimalnimi viri do učinkovite zdravstvene in babiške nege: Zbornik predavanj z recenzijo* (pp. 208–215). Zbornica zdravstvene in babiške nege Slovenije – Zveza strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije, Nacionalni center za strokovni, karierni in osebni razvoj medicinskih sester in babic.
- Kobal, M. F. (2009). *Psihopatologija za varnostno in pravno področje*. Fakulteta za varnostne vede.
- Komazec, S. (2000). Nasilje nad negovalnim timom [Violence against nursing teams]. In D. Klemenc, & M. Pahor (Eds.), *Nasilje in spolno nadlegovanje na delovnih mestih medicinskih sester v Sloveniji* (pp. 93–97). Društvo medicinskih sester in zdravstvenih tehnikov.

- Kores Plesničar, B. (2006). Pomen agresije v zdravstvenih ustanovah [The meaning of aggression in health care institutions]. In V. Čuk (Ed.), *Raziskovanje, izobraževanje in razvoj v psihiatrični zdravstveni negi: Pravice bolnikov in zaposlenih* (pp. 27–30). Zbornica zdravstvene in babiške nege – Zveza društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije, Sekcija medicinskih sester in zdravstvenih tehnikov v psihiatriji.
- Kores Plesničar, B. in Kordić Lasič, J. (2004). Nasilje bolnikov in njihovih svojcev v zdravstvenih ustanovah [Violent behaviour of patients and their relatives in health care institutions]. *Zdravstveno varstvo*, 43(3), 179–183.
- Marinič, M. (1999). Izolacija pacientov s pasovi Segufix [Isolation of patients with Segufix belts]. In B. Kogovšek, & R. Kobentar (Eds.), *Priročnik psihiatrične zdravstvene nege in psihiatrije* (pp. 169–175). Rokus Klett.
- Močnik, M. (2009). Zloraba in nasilje varovancev v posebnem socialnovarstvenem zavodu Lukavci z vidika dela medicinske sestre [Abuse and violence of protégés in the special social welfare institution Lukavci from the nurses point of view]. In U. Poček (Ed.), *Zbornik prispevkov: Nasilno vedenje v duhu novih praks* (pp. 17–25). Zbornica zdravstvene in babiške nege – Zveza društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije, Sekcija medicinskih sester in zdravstvenih tehnikov v psihiatriji.
- Možgan, B. (2009). Posebni varovalni ukrepi [Special precautionary measures]. In P. Pregelj, & R. Kobentar (Eds.), *Zdravstvena nega in zdravljenje motenj v duševnem razvoju* (pp. 439–443). Rokus Klett.
- Novak Grubič, V., Bon, J., & Novak Šarotar, B. (Eds.). (2018). *Priporočila in smernice za uporabo posebnih varovalnih ukrepov v psihiatriji* [Recommendations and guidelines for the use of special protective measures in psychiatry]. Viceversa. <http://www.zpsih.si/media/documents/PVU2018.pdf>
- Pačnik, T. (1989). Socialni vidiki agresivnosti [The social aspects of aggressiveness]. *Obzornik zdravstvene nege*, 23(1/2), 73–79. <https://obzornik.zbornica-zveza.si/index.php/ObzorZdravNeg/article/view/1809>
- Perne, D. (2005). Uporaba Brosetove lestvice za napoved nasilnega pacienta [Brøset violence checklist – presentation and practical use]. In A. Bručan, M. Gričar, & R. Vajd (Eds.), *Urgentna medicina: Izbrana poglavja* (pp. 67–72). Slovensko združenje za urgentno medicino.
- Pravilnik o načinu sodelovanja med zdravstvenim osebjem in reševalno službo ter policijo [Rules on the cooperation between medical staff and rescue service and police]. (2009). *Uradni list RS*, (44/09).
- Škrila Čuš, D. (2005). Alkohol, agresija in nasilje [Alcohol, aggression, and violence]. *Zdravniški vestnik*, 74(9), 535–537. <https://www.dlib.si/details/URN:NBN:SI:doc-RNQUXRG>
- Šolc, S. (2001). Agresija in nasilje [Aggression and violence]. *Utrip*, 9(1), 32–35.
- Zakon o duševnem zdravju (ZDZdr) [Mental Health Act]. (2008, 2015, 2019). *Uradni list RS*, (77/08, 46/15, 44/2019).
- Zakon o nalogah in pooblastilih policije (ZNPPol) [Police Tasks and Powers Act]. (2013, 2015, 2017, 2019, 2021). *Uradni list RS*, (15/13, 23/15, 10/17, 46/19, 47/19, 153/21).
- Zbornica zdravstvene in babiške nege Slovenije. (2018). *Nacionalni protokoli*

aktivnosti zdravstvene in babiške nege: Posebni varovalni ukrep – omejitev gibanja znotraj enega prostora na področju psihiatrije [National protocols of nursing and midwives activities: Special protective measure – restriction of movement within one place in psychiatry]. <https://www.zbornica-zveza.si/wp-content/uploads/2019/09/NP-omejitev-gibanja-znotraj-enega-prostora.pdf>

Zeller, A., Hahn, S., Needham, I., Kok, G., Dassen, T., & Halfens, R. J. G. (2009). Aggressive behavior of nursing home residents toward caregivers: a systematic literature review. *Geriatric Nursing*, 30(3), 174–187.

Žaberl, M. (2006). *Temelji policijskih pooblastil* [Legal foundations of police powers]. Fakulteta za policijsko – varnostne vede.

ABOUT THE AUTHORS:

Branko Gabrovec, PhD, assist. professor in public health at the University of Ljubljana, National Institute of Public Health and Faculty of Health Sciences at the University of Maribor. E-mail: branko.gabrovec@nijz.si

Tilen Zupan, BA in security sciences, employed at the Novo Mesto Police Administration. E-mail: tilen.zupan@policija.si

Srečko Felix Krobe, PhD, assist. professor of security studies at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: srecko.krobe@siol.net

Branko Lobnikar, PhD, professor of security studies at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: branko.lobnikar@fvv.uni-mb.si

Adoption of Advanced Technological Solutions in Slovenian Private Security Companies

Miha Dvojmoč, Patricija Lunežnik, Kaja Prislan

Purpose:

The use of advanced technological solutions in security is one of the current development trends in the private security industry. It represents an opportunity for upgrading security services and for resolving human resources issues that private security companies face. The aim of the article is to present the potentials of modern technological solutions for upgrading security services and overcoming contemporary challenges in the field of private security.

Design/Methods/Approach:

For the purpose of the study, we conducted interviews with representatives of the Slovenian private security profession to determine the current challenges in the private security industry, their positions on modern technologies and their feasibility in practice. Interviews were conducted at the head offices of respondents' companies in summer 2019. In total, four interviews were conducted.

Findings:

The results show that general problems on the labour market have a significant impact on private security services in Slovenia, while the lack of competent personnel leads to unregulated working conditions and the inability to provide quality security services. The implementation of advanced technological solutions could address key operational challenges and optimise financial and human resources.

Research Limitations/Implications:

One of the limitations of the study is the small number of interviews. We tried to overcome this limitation by carefully selecting the interviewees and by conducting a thorough, in-depth interview.

Originality/Value:

The study addresses current and important issues and connects with the concepts of digitalisation of companies. This is a topic that is important in both public policing and private policing. The paper thus upgrades and complements existing knowledge in this field.

Keywords: private security companies, development trends, advanced technological solutions, technical security, human resources issues

UDC: 351.746.2

Prevzem naprednih tehnoloških rešitev v slovenskih zasebnih varnostnih podjetjih

Namen prispevka:

Uporaba naprednih tehnoloških rešitev v varovanju je eden od aktualnih razvojnih trendov v sektorju zasebnega varovanja. Predstavlja priložnost za nadgradnjo varnostnih storitev in reševanje kadrovskih težav, s katerimi se soočajo zasebna varnostna podjetja. Namen prispevka je predstaviti potencialne sodobnih tehnoloških rešitev za nadgradnjo varnostnih storitev in premagovanje sodobnih izzivov na področju zasebnega varovanja.

Metode:

Za namen študije smo opravili intervjuje s predstavniki slovenske stroke zasebnega varovanja, da bi ugotovili aktualne izzive v sektorju zasebnega varovanja, njihova stališča do sodobnih tehnologij in njihovo izvedljivost v praksi. Intervjuji so bili opravljeni na sedežih podjetij anketirancev poleti 2019. Skupno so bili opravljeni štirje intervjuji.

Ugotovitve:

Rezultati kažejo, da splošne težave na trgu dela pomembno vplivajo na zasebne varnostne službe v Sloveniji, pomanjkanje kompetentnega kadra pa vodi v neurejene delovne pogoje in nezmožnost zagotavljanja kakovostnih storitev varovanja. Z uvedbo naprednih tehnoloških rešitev bi lahko rešili ključne operativne izzive ter optimizirali finančne in kadrovske vire.

Omejitve/uporabnost raziskave:

Ena od omejitev študije je majhno število intervjujev. To omejitev smo poskušali preseči s skrbno izbiro intervjuvancev in s temeljitim, poglobljenim intervjujem.

Izvirnost/pomembnost prispevka:

Študija obravnava aktualna in pomembna vprašanja ter se povezuje s koncepti digitalizacije podjetij. To je tema, ki je pomembna tako v javni kot zasebni policiji. Prispevek tako nadgrajuje in dopolnjuje obstoječa znanja s tega področja.

Ključne besede: zasebna varnostna podjetja, trendi razvoja, napredne tehnološke rešitve, tehnično varovanje, kadrovska vprašanja

UDK: 351.746.2

1 INTRODUCTION

In recent years, the private security industry has been facing various changes that affect the restructuring of security methods, as well as approaches to corporate governance and management of private security companies. The most notable trends are related to the digitalisation and automation of business (security) operations, technological innovations, and, consequently, the changes in required competencies and reorganisation of human resources structures (Servoz, 2019). In this respect, advanced technological solutions in technical security certainly represent the more current progressions in private security industry development (El Dorado, 2017). The pursuit of innovation in the security industry is important, as it contributes to more effective implementation of security and exceeds the capacity of traditional technical security systems (Pistorius, 2018).

Although technological development of private security is proceeding rapidly globally, the use of modern technological solutions is not yet an established practice in many European countries. The fact that most private security companies are staunchly relying on traditional approaches is hampering technological development that could contribute to the greater effectiveness of private security services. Therefore, it is important to promote greater flexibility and innovation in private security services. An additional problem in this regard is the regulation that is often lagging behind technological development. New technologies can cause gaps in existing regulation or conflicts with current rules (Leenes et al., 2017). Therefore, law-making and rule-making must become more proactive, dynamic and responsive (Fenwick et al., 2017). Technological advances in the private security industry are also important because they represent an opportunity to reduce human resources issues, which is also one of the fundamental challenges companies have been facing in recent years. The lack of security staff has a negative impact on working conditions, leading to overburdening of employees (Pavšič, 2014), which also affects the quality of security services. In the future, a comprehensive approach will be needed to solve the human resources problem, which is reflected in the introduction of advanced technological solutions that fill the personnel gap and the training of existing personnel in the use and operation of new technologies.

The article thus includes an overview of the current state of human resources problems in (Slovenian) private security companies and a proposal for a solution using advanced technologies, considering the need to adapt the legislation. The findings address existing challenges in the private security industry and promote new security approaches.

The structure of the article is as follows. The next chapter presents the key development challenges that arise in private security and the potentials for using advanced technological solutions to advance private security and solve human resources problems. We compared traditional and modern approaches to security in the private security industry and determined whether advanced technological solutions could help reduce human resources problems. The third chapter presents the study of development trends, challenges and opportunities in private security, which examined how global challenges are reflected in the Slovenian security environment. The fourth chapter presents a discussion of the study

results, whereas the last chapter presents the conclusion with a view towards the future development of private security.

2 ANALYSIS OF CURRENT CHALLENGES AND TRENDS IN THE PRIVATE SECURITY INDUSTRY

Among the many trends influencing the development of the private security industry, digital transformation and technological innovations are certainly the most prominent. Technological advances include the creation of new or improvement of existing work methods, support of innovation and introduction of new approaches to business, which in turn affects reductions in costs and workload, improvements of existing products and advancements in the organisation (Radonjič, 2013). Many modern technologies, such as the Internet of Things (IoT) and related sensor technologies, as well as robotics, are already present and, to some extent, established in the private security market (Ludwig, 2018). Trends introducing innovations in technical security include ICT-related technologies, in particular, next-generation mobile devices (such as 5G connectivity) and cloud solutions, augmented reality (AR) and virtual reality (VR), which enable improved communications, data management, and security personnel training, in which realistic scenarios can be developed (Pistorius, 2018).

In line with the abovementioned technological development on the international market, there are various other examples of modern technical means applicable in the field of security: high-definition cameras with built-in high-quality sound, which allow complete documentation of the controlled area (El Dorado, 2017); smart applications for communication between security guards and security control centres, task management, document sharing and tracking (Madakam & Date, 2016); microwave intrusion detection alarms for monitoring open areas, runways, fuel storage areas and other secured facilities (Fiber SenSys, 2012); secure Internet identity with biometric smart cards that only work in conjunction with a specific body; security equipment with electronic chips within the product or coding that only works at a specific location (Davis & Pease, 2000), and AI security cameras that detect suspicious behaviour (Vincent, 2018). In addition to the solutions mentioned, automation and robotics are increasingly being introduced in private security services. Two such examples are security robots and drones, which can be equipped with high-resolution cameras, sensors, automatic recognition systems, access control systems, etc., representing a comprehensive technical security system (Kyung-hoon et al., 2010).

Although the dynamics of technological change can bring new opportunities and strengthen the development of technical security, many private security companies are not yet taking advantage of these new technologies. Some advanced solutions are already noticeable and are becoming a common practice (for example, digital event reports (Sintal Konzern, 2017), electronic alarm security systems (Stinger Security, 2020), SMP automatic patrolling security robot, advanced video surveillance systems (Protect, 2020), however, private security companies in practice still rely on traditional approaches in most cases (video and audio surveillance, sensors, motion detectors and security alarms). Such a situation

is noticeable, for example, in Slovenia. Thus, in the following, when analysing the challenges and investigating the implementation of new technological solutions in practice, we focus in more detail on the experiences from Slovenia. Although certain challenges are country-specific, these problems can be generalised to other comparable European countries.

Technological development and advances depend on many factors, with legal regulation being one of the most significant. In the field of technical security regulation, it is common that legal norms are general in nature and merely stipulate that provision of private security may include the use of technical security systems. These are usually defined as video and audio surveillance systems, technical and mechanical security devices, entry control systems, devices for inspection of luggage or cargo, control systems of the secured areas, and detection and prevention of unauthorised entry. In addition to the general definitions of security systems, legal regulation does not explicitly mention the use of technological innovations or instructions for their safe use. Such a definition of private security measures is established in most European countries, including Slovenia. While on the other hand, for example, the introduction of new technologies and procedures in the field of public security requires a precise risk assessment and definition of their use. This indicates that legal regulations of private security are not modernised and does not address issues related to technological development or the feasibility of using new technologies.

Whether innovations represent completely new technologies or new combinations of existing technologies, it is important to define regulations in the field of legislation further and set minimum standards for their use. Therefore, in the future, legislators will be forced to examine the need for harmonisation and further definition of new approaches to private security provision (Celestina, 2013).

In order to adapt to digital and technological development, it is necessary to develop human resources through continuous education and training and modernising legislation. Although advanced technological solutions are only in the initial stages of use, personnel will need to have appropriate expertise in handling such technology in the future (El Dorado, 2019). Advanced technologies require operators who understand how they work (Bughin et al., 2018), so continuous professional training – which is already not conducted in a sufficient manner – will be required for the new generation of security personnel (Cobbina et al., 2016). However, recruitment, retention and training of security personnel at all levels is currently extremely difficult, as private security companies face major human resources problems (SSI Staff, 2018). This is a global problem that is also evident in Slovenia. A survey conducted by the Employment Service of Slovenia shows that the demand for security personnel is high; for example, a need for almost 700 security guards was observed in 2019 (Zavod RS za zaposlovanje, 2020). The lack of security guards is also observed elsewhere in Europe. In Spain, for example, several private security companies are in bankruptcy proceedings due to human resources problems (González, 2019); in Croatia, companies face an excessive brain drain of specialised personnel abroad (Pavlic, 2016); there is also the high-profile case of the security at the 2012 Olympic Games in Great Britain,

where the military was also involved, due to the inability to provide adequate numbers of security guards (Adams, 2012). These problems can also be observed outside EU member states. In 2018, Japan reported that more than 90 per cent of private security companies face human resources problems. The greatest need is observable for crowd control personnel and security guards, airport security guards and security personnel for facilities protection (Kyodo, 2018). Considering the growing needs and demands for private security services (Nalla & Cobbina, 2017), the lack of security personnel often means that the demand for security is greater than the available workforce. Hence, private security companies are forced to do more with fewer people.

Consequently, there have been several publications in the media in the last several years of security personnel warning of unregulated working conditions, low salaries, poor reputation (G. C., 2013), excessive overtime, disregard for their complexity of work, and overburdened employees (Pavšič, 2014). For example, a survey from Singapore found that about two-thirds of security guards were dissatisfied with their salaries (Lim & Nalla, 2014). Overall, the shortage of security personnel has a negative impact on the private security industry, private security companies, working conditions of security personnel, the quality of security services and, finally, according to Button and Lalonde (2014), on general community safety and crime prevention performance. This situation further exacerbates the unstable private security market. Private security companies often accept orders for security services below standard prices in the private security market, which leads to unfair competition.¹ The consequences of unfair competition are widespread and are reflected in salaries below minimum wage, personnel's dissatisfaction with employment, difficulties in recruiting new personnel, a negative public image, and undermined efforts to improve the quality of services (Savski, 2013).

Due to the growing market demands and limited resources, private security companies need new approaches for providing security services. Solutions can be found in advanced technologies, which enable more efficient allocation of human resources in critical situations, facilitate regular work procedures (SMP Robotics, 2019), reduces working hours of security personnel, reduce costs, and ensure a higher quality of security services (Sunstates Security, 2020). Thus, modern technologies can positively affect jobs and personnel needs in the short and long term. Most notably, the need for recruitment can drop, and the quality of jobs can be improved (Pfeiffer, 2016). However, in achieving such synergies, we must consider that the right approach to introducing digital and technological development in the private security industry inevitably requires many changes in the field of security organisation, human resource structure, and security services.

Hikvision Digital Technology (HDT, 2022) and Ridenhour (2022) anticipate trends in the private security industry in 2022. Advances in security-related technology have made it a viable option for reducing labor costs while improving the level of protection and service provided (Ridenhour, 2022). By all appearances, the private security industry is in a stage of redefining itself (HDT,

¹ *Unfair competition means »that the action of the company is contrary to good business practice and which causes or is likely to cause harm to other market participants« (»Zakon o preprečevanju omejevanja konkurence [ZPOmK-1G]«, 2017).*

2022). Artificial Intelligence (AI) has been one of the fundamental technologies to reshape the security industry. Currently AI technologies are being used for wider applications, like personal protective equipment detection, automated event alerts, fall detection. In the future Artificial Intelligence of Things (AIoT) will bring more possibilities to the industry, with expanding applications for security devices and systems, moreover cloud-based solutions and services will also become essential (HDT, 2022).

An overview of the general development trends and most significant challenges in private security shows that the advanced technological solutions may be most efficient in the provision of private security services. Two questions arise in this regard. First, what is the contribution of such solutions to work efficiency, and second, can the implementation of such solutions solve current challenges? In order to clarify these issues, we compared the traditional approaches to the provision of security services (i.e. provision of security with security guards) with modern ones (i.e. provision of security supported by advanced technological solutions), and analysed their advantages and disadvantages.

2.1 Comparison of traditional and modern approaches to the provision of security in the private security industry

The evaluation parameters used for the comparison of traditional and modern approaches were as follows.

1. *Degree of autonomy and continuity*, where we analysed the levels of independence and overall capabilities of analysed approaches.
2. *Surveillance of secured area*, where we reviewed the surveillance capabilities provided by a particular approach to security.
3. *Threats to security*, where we analysed the risks associated with both approaches.
4. *Costs of security services*, where we investigated which approach to the provision of security is more favourable for a private security company.

The first evaluation parameter is the *degree of autonomy and continuity*. Technological solutions do not have the same operational requirements and needs as human resources (e.g. rest, lunch breaks, vacations) (SMP Robotics, 2019) to ensure effectiveness, so they can constantly operate without interruptions (Turner, 2015). Security guards' working hours are regulated and significantly more limited than operating hours of advanced technological solutions. This reduces the need for personnel, as constant patrols of numerous security guards can be replaced by modern cameras, security robots, drones, or other advanced technological solutions (Marriott, 2020). Unlike human resources, however, surveillance technologies require human supervision. Automation and operation of advanced technological solutions can also cause unexpected problems, such as misinterpretation of sensors, plug-in malfunction, or software errors, leading to severe consequences for residents (Pfeiffer, 2016), especially in the field of security. Furthermore, security guards can resolve a crisis situation appropriately without additional aid (e.g. with proper communication to calm an upset guest) (El Dorado, 2019) or provide first aid (Hill, 2019). Although learning-based programming

can ensure that modern technologies respond to situations according to learned patterns; however, from a security perspective, this is difficult, as it is impossible to predict all possible events (Lin et al., 2009).

The second evaluation parameter is *surveillance of secured area*. A security guard can oversee a limited secured area, whereas larger facilities and areas require additional mechanisms and means, such as security cameras, which also do not provide full surveillance in their traditional form. However, advanced technological solutions with built-in control systems, such as security robots and drones, can provide a 360-degree overview, which is more convenient and high-quality than installing multiple surveillance cameras in one area. Furthermore, they provide more reliable information on events and circumstances, which can be used as evidence in the event of security incidents and criminal offences. Instead of the standard detailed visitor records, advanced technological solutions with more advanced functionalities can provide a record of car registrations or entry of unauthorised persons (Knightscope, n. d.). However, if used inappropriately, such data collection can pose a significant risk of misuse of personal data and excessive invasion of privacy (Papademetriou, 2016), which means that such measures must be properly regulated by law.

The third evaluation parameter is *threats in security*. The work of security guards involves many dangers that can arise when performing this type of work. Examples include burglaries, physical clashes between groups on the streets or rescuing people from danger (Theodoridis & Huosheng, 2012). Security guards patrolling in critical industrial environments may also be exposed to hazardous chemicals, gases or radiation. Such security requires specialised training for security guards and personal protective equipment, such as respirators, high visibility jackets and protective clothing (Button & Lalonde, 2014). In these cases, advanced technological solutions, such as security robots and drones, serve as a substitute for physical presence in the problematic area or as an aid to ensure security guard's readiness and appropriate intervention according to the situation. Nevertheless, the use of advanced technological means also poses certain dangers associated with threats to information and cyber security. The prevalence of digital technology means that we depend on information systems that may be exposed to criminal elements (Grabosky, 2007). Advanced technological solutions can be wirelessly connected to the Internet, which means that they depend on the connection, while various cyber threats can compromise communications and sensitive data security. In addition to intercepting or stealing data, hackers can take control of modern technology, weaken the frequency of connection to the operator or use it for malicious acts (Ludwig, 2018). Because of the complexity of the use of modern technologies, it will cause increased difficulties in investigations and presenting evidence (Davis & Pease, 2000). For digital evidence to be legally admissible in court, it must be credible, accurate, complete and conclusive. However, this is made difficult due to the lack of a robust legal framework for cybercrime and a reliable digital forensic investigation (Yeboah-Ofori & Brown, 2020).

The fourth evaluation parameter is *costs of security services*. The purchase of advanced technological solutions as a one-time expense is a very high investment

but generates economic savings in the long run (Joh, 2017). The traditional approach to the provision of security requires not only human resources (i.e., security guards) but additional technical means, such as video cameras, to provide 24-hour security, which represents additional costs. However, advanced technological solutions can replace the constant patrolling of numerous security guards. Nevertheless, it is important to keep in mind that advanced technological solutions require constant system updates, checks and repairs, resulting in additional operating costs. Management of such technologies also requires personnel with appropriate IT expertise (Bendis, 2016). The cost comparison is therefore not simple; however, practical experience has shown that using advanced technological solutions is a cost-effective decision in the long run. A change in the mentality of security service customers is also needed, which is often the biggest obstacle in introducing advanced technological solutions (Marriott, 2020).

In summary, a comparison of traditional and modern approaches to the provision of security has shown that advanced technological solutions cannot yet operate independently, so human resources are nevertheless needed to control the technology and ensure uninterrupted operations. Both traditional and modern approaches are constrained by regulatory frameworks and guidelines, with the autonomy of people being greater. People can exercise discretion, while technologies are managed by people. Advanced technological solutions are more reliable in terms of surveillance, which can be useful for large facilities or institutions and the protection of critical areas that would pose a life-threatening situation to a security guard. However, the use of advanced technological solutions requires special care in the collection of personal data, in the form of integrated mechanisms that prevent misuse and ensure the implementation of fundamental principles from the perspective of information/cyber security and data/privacy protection. Nevertheless, practice examples show that implementing advanced technological solutions helps address key operational challenges and optimise financial and human resources. Even though modern technologies seem more efficient and perhaps even more reliable according to the conducted analysis, the costs of equipment maintenance must be taken into account and all the advantages. Based on the above, we can conclude that while the use of advanced technological solutions could help reduce human resources problems and contribute to problem-solving, this involves additional costs and creates certain reorganisation needs. Nonetheless, combining advanced technical security systems with physical security, will undoubtedly result in the above-standard quality of security.

Based on the overview of the challenges facing the private security industry, we conducted a study of development trends, challenges and opportunities in private security in Slovenia. The purpose of the study was to determine how companies perceive and address these challenges, and what are their views and plans regarding the use of advanced technological solutions in the future.

3 DESCRIPTION OF METHOD, QUESTIONNAIRE, AND SAMPLE

3.1 Method

We conducted a qualitative study, which included in-depth semi-structured interviews with representatives of the private security sector in Slovenia.

The target population were private security companies in Slovenia. In order to obtain the best possible data regarding the experience in Slovenian practice, we determined three other specific (inclusion) criteria for the selection of companies, specifically:

- a. location (companies based in different regions of Slovenia);
- b. type of services (the company provides services of physical and technical security); and
- c. size of the company (the company employs at least 150 employees).

To obtain the sample, we used targeted sampling, i.e. we selected a specific group of companies that is as representative as possible in terms of target population and inclusion criteria. To obtain a comprehensive understanding of the challenges facing the private security industry, we also aimed to conduct an interview with a representative of the private security sector on a national strategic level.

3.2 Questionnaire and data collection procedure

Interviews were conducted at the head offices of respondents' companies from 31 July to 8 August 2019. Before conducting the study, we sent invitations for participation to respondents, and they were also informed that the collected data will be used for research purposes. Audio recordings were made of all interviews to be used for transcripts.

For the purpose of interviews, we prepared two different questionnaires: one for interviewing representatives of private security companies, and the other for the representative of the private security sector on a national strategic level, i.e. the president of the Chamber for the Development of Slovenian Private Security (president of the Chamber). The thematic sections of the two questionnaires were aligned, with questions differing according to the purpose of the interview. Interviews with respondents from private security companies were aimed at gaining insight into the challenges faced by Slovenian private security companies, while the interview with the president of the Chamber was aimed at examining the general state of development of the private security industry and market.

Both questionnaires were divided into six sections, followed by open-ended questions and, if necessary, sub-questions. The first questionnaire (Q1) for representatives of private security companies included 53 questions in total, while the second questionnaire (Q2) for the president of the Chamber included 33 questions in total. The questions were developed based on findings from the literature review on human resources problems, modern technologies in the private security market, and the challenges related to the use of advanced technologies. The questionnaire for the president of the Chamber did not include

questions related to the operations of private security companies and instead focused on the state of the Slovenian private security market and the development of the private security industry.

The main sections of the questionnaire were as follows.

1. *Human resources problems*: This section included questions (11 main questions in Q1; seven main questions in Q2) regarding the human resources situation in private security companies and how these human resources problems are being resolved (e.g., Do you think that the lack of staff and the employment of unskilled people for work are noticeably present?; In what way could we address this issue, from the political and sectoral view?; In your opinion, what is the most significant cause of staff shortage?; In what way do you attract new staff to your team?).
2. *Development of employees' competencies and activities*: This section included questions (seven main questions and one sub-question in Q1; five main questions and one sub-question in Q2) about employee training and development of new technical competencies in human resources (e.g., What are the most desirable/sought-after characteristics and knowledge of the employee when performing work in your company?; Considering technological developments, do you plan to develop new technical competencies of human resources in the next two years?; Do you think that any changes are needed at the systemic, state-level regarding the training of security personnel?).
3. *Advanced technological solutions*: This section included questions (six main questions and nine sub-questions in Q1; six main questions and five sub-questions in Q2) regarding respondents' views on the advantages and disadvantages of security provision using advanced technological solutions and the possibility of their integration into current security services (e.g., If you compare the efficiency of advanced technological solutions with the physical protection, what are the advantages and the disadvantages of both means of ensuring security?; What are the potential improvements and dangers of introducing advanced technological solutions in your work?; Do you think that the use of advanced technological solutions could contribute to solving personnel issues?; Are you planning to introduce new technological solutions in your work and services in the next two years?).
4. *Adequacy of legislation*: This section included questions (five main questions and one sub-question in Q1; three main questions in Q2) about respondents' views on the adequacy of the current legislation and proposals for changes (e.g., What are the limitations of Slovenian legislation in introducing innovations in private security in terms of development and staffing?; What changes are needed to make the development of the private security industry faster?).
5. *Future trends*: This section included questions (three main questions in Q1 and Q2) about respondents' views on the challenges that the private security industry will face in the future (e.g., Do you think that private security companies are flexible enough to keep up with developments?;

What do you think are the most important challenges and trends in the future, and what will be the most topical in the field of private security in the future - where will the development of the private security industry go?).

In addition to substantive questions, the questionnaire included questions on respondents' characteristics. Demographic characteristics in Q1 were determined using ten questions related to both the respondent and their private security company (respondent's education and work experience, time frame of the company's existence, number of employees in the company, types of security services provided by the company, types of technical means used in provision of security, types of company clients, and the company's international operations). In Q2, three questions related to demographic characteristics were included (education, years of experience in the field, and professional achievements in the field).

The data obtained was processed using the content analysis method. First, we transcribed the audio recordings. We then analysed the respondents' answers in detail and performed a comparison of data. We performed a cross-analysis of respondents' answers, identified differences in their reported opinions, and studied the diversity of answers to each question. We then interpreted the results to summarise the findings of the analysis.

3.3 Sample

Based on the selected target population, 156 private security companies operated in Slovenia at the time of the study. Using the targeted sampling method and considering the selection criteria, we invited six (3.8%) private security companies, and three (50%) companies responded to the invitation. Thus, interviews were conducted with representatives of three private security companies in Slovenia. We also conducted an interview with a representative of the Chamber for the Development of Slovenian Private Security, Mr Branko Slak. In total, we conducted four interviews. The demographic characteristics of the respondents and general data about their companies are presented below.

- The first respondent (R1) from company A is a Bachelor of Law graduate in law with a completed bar examination, who has been in the management position (Head of the legal department) for five years. Company A has been operating for more than 20 years, has more than 150 employees, with security services clients from both the public and private sectors, and operates exclusively in Slovenia.
- The second respondent (R2) from company B is an economic technician by education, and has been the Director of the security company for 10 years; previously he worked as a security guard in the same company. Company B has been operating on the market for more than 30 years, has more than 180 employees, with security services client from both the public and private sectors, and operates exclusively in Slovenia.
- The third respondent (R3), who is a procurator of company C, has the sixth level of education, has been in a managerial position for 15 years,

and has previously performed various jobs in private security. Company C has recently undergone restructuring and has been in business for four years, operates in three different countries and employs 900 people, with security services clients from both the public and private sectors.

- Mr Branko Slak has been working in the field of private security for 12 years and has been the president of the Chamber for nine years.

All three companies included in the study employ all types of security personnel: security guards, guards, technical security guards, security operators, security managers and security supervisors. They provide all forms of security services, except protection of persons and design of technical security systems.

4 RESULTS

In the following, we present the findings of the study, which show the current challenges facing the Slovenian private security companies, their future development plans, and feasibility of advanced technological solutions, taking into account legislative frameworks and their effectiveness in solving human resources problems. The results are combined and presented in a summarised form by individual sections, as presented in the methodological section of the article.

The first section relates to human resources problems in Slovenian private security companies. Respondents confirmed that the lack of human resources is a significant problem. This is reflected mainly in the competition between private security companies and the inability to provide sufficient numbers of security guards for certain security orders. According to the respondents, the causes for the lack of human resources can be divided into internal and external. Internal causes are working hours, overtime, and low pay of security guards considering the complexity of work, while external causes are a lack of interest of young people in the work of security guards, young personnel leaving the industry, excessive additional training, and legal restrictions for immigrants to obtain service cards without the appropriate citizenship.

On the other hand, the president of the Chamber believes that the causes are primarily external and a consequence of the economic situation, as the shortage of personnel is noticeable in all industries, not only in private security companies. Respondents from private security companies believe that the human resources problem requires a multi-level approach. They primarily highlighted the problem of competition and inconsistent prices in the private security market, and the consequent provision of security services without any emphasis on quality. They note that private security services clients often do not have adequate knowledge of security services and do not realise that the quality of services also depends on the price. Because of these challenges, private security companies are unable to offer fair pay to security guards. Secondly, they also acknowledged the regulative challenges, specifically the legislative issues and inflexible employment procedures. Private security companies try to solve human resources problems by providing a positive working environment, effective internal communication, and assistance in solving employees' issues. In order to meet the quantitative

needs of security orders, private security companies attract new personnel through public networks and rely on indirect recruitment. Respondent R1 stated that they are affiliated with the Secondary School for Security Education and are actively cooperating with the Chamber for the Development of Slovenian Private Security. We asked the president of Chamber about how, if at all, private security companies strive to improve the social situation of security guards. The respondent believes that it is first necessary to sort out the relationship between private security companies and state bodies, finding ways to improve the private security market, which would, in turn, contribute to the growth of the minimum wage of security guards.

The following section covers the development of employees' competencies. Respondents consider education and training of employees to be important, and therefore actively participate in public tenders for additional education of security guards, projects organised by the Chamber for the Development of Slovenian Private Security, ASI – Comprehensive support for companies for active ageing of the workforce, and in English language school centres, in addition to the mandatory education and training required for the work of security guards. The president of the Chamber agrees on the importance of continuing education in employment, stating that the success of a private security company is contingent on qualified personnel that can offer quality security services. Given the exponential technological developments that also characterise the security sector, respondents R1 and R3 confirmed the planning for the development of new technical competencies in human resources over the next two years, while respondent R2 believes that they already provide employees with the training needed for technical security, so they do not plan to develop new technical competencies in the next two years.

The third section relates to advanced technological solutions. The respondents recognise the benefits of using advanced technological solutions and strive to implement existing security services. They believe that the main advantages of using modern technologies are related to lower demands for human resources, greater effectiveness in the provision of security, and overall improved surveillance capabilities. Furthermore, they represent a good complement to video surveillance and allow to exceed the limitations of traditional approaches to security, and at the same time represent a solution to the described human resources problems. Advanced modern technologies thus represent a good upgrade of security services; however, the respondents point out that the effectiveness of using advanced technologies is contingent on the appropriate integration of technology and human resources. They consider the digitisation of administrative procedures (reporting), which coincides with the GDPR, smart applications for communication between security guards and security control centres, task management, document sharing and tracking applications, modern video surveillance systems and modern anti-theft systems to be the most useful for their work. They also state that they plan to use new technological solutions in their work and provision of services in the next two years. In addition to the listed advanced technological solutions, respondents also recognise the effectiveness of security robots and drones. They believe a security robot is an effective example

for patrolling larger areas and critical infrastructures, while a drone is effective for surveillance of public gatherings. The president of the Chamber added that the combination of the two abovementioned security solutions would represent an even more effective security system. The respondents were also asked about the potential risks that may arise when using advanced technological solutions. They recognise excessive invasion of privacy and violation of human rights as the most important risks. They believe that preparation for their use is important, as legislation has not defined them yet (2020).

The fourth section relates to the adequacy of Slovenian legislation. The respondents from private security companies highlighted the challenges of Slovenian legislation, which are reflected in their work and the development of the private security industry. They believe that legislation (1) excessively interferes with staffing, thereby exacerbating the problem of inflexible employment; (2) does not include a collective agreement that could regulate employment in more detail; (3) excessively interferes with the economic activity. Respondent R2 believes that the state should regulate only the general regulations while leaving economic aspects and procedures to the private security market. He adds that by meeting the conditions set by the regulator, private security companies cannot adapt to the market, which in his opinion limits the development of the private security industry. Respondent R1 states that the regulator imposes requirements, guidelines and instructions for security services but does not provide relief for compliance. Respondent R1 explains the excessive interference in the company with the example of required equipment for the transport of cash – such equipment must be provided according to the prescribed standards, but they must procure it entirely themselves. Lastly, they add that (4) the regulator does not oversee unfair competition in the private security market and the grey economy. On the other hand, the president of the Chamber believes that Slovenian legislation on private security is flexible enough and allows for the possibility of development. However, it should be supplemented accordingly, thus eliminating the shortcomings manifesting in the professional field of private security.

The last section relates to future trends. The respondents from private security companies believe that the development of the Slovenian private security industry, compared to other countries, sufficiently follows current trends. However, they do not share opinions on the flexibility of companies. Two respondents (R2 and R3) from private security companies believe that companies are not flexible enough, as they are overburdened with meeting the requirements of the legislation. On the other hand, respondent R1 believes that the flexibility of private security companies is appropriate, as it is necessary for survival in the private security market. The president of the Chamber explained that the flexibility of private security companies depends on the client's demands. The more demanding the client, the more private security companies will strive to meet their demands, as this is how they get business. If the clients do not have the appropriate knowledge of security services, the private security company will provide only basic security. The respondents from private security companies believe that future challenges will be primarily related to meeting the growing market demands for the provision of security in general, growing complexity of

managing private security tasks, providing appropriate security personnel and appropriate training, continuous upgrading of security services by implementing advanced technological solutions, and strengthening information security. The president of the Chamber anticipates that in the future, the challenges will be related to meeting the legal restrictions set by the regulator, clients' demands, technological development and the consequent training of security personnel. He believes that private security companies will strive to replace physical security by using advanced technological solutions in conjunction with human resources, which could be offered as value-added security on the market.

5 DISCUSSION

The results of the conducted interviews indicate that the human resources problem represents a great challenge to Slovenian private security companies and that a multi-level approach to the solution is necessary. During times of a stable economy, when there is a high demand for skilled security personnel, young people opt for other industries or leave the private security industry in a few years, leaving behind an increasingly ageing workforce that is less adaptable to new technologies. In addition, the decision to look for another job is also influenced by unfavourable working hours, overtime and below-average salaries of security guards considering the complexity of their work.

In order to solve the human resources problem, a stable private security market is needed, which properly regulates the system of employees' salaries. According to the study's findings, one of the most important solutions is to ascribe greater value to security services and consequent improvement of the pricing policy, which will enable companies to provide higher salaries to employees (Savski, 2013). Low salaries of employees with unfavourable working conditions increase their dissatisfaction, leading to other forms of human resources problems. Therefore, it is important to make clients, especially from the public sector, aware of the need to change their attitude towards the quality of private security and pricing of services. This means that clients should choose providers based on their references and strive for high-quality services rather than the lowest price offer (Celestina, 2013). After all, private security companies that adopt advanced technological solutions will offer such services at a higher price. This raises the question of whether clients will favour such developments and whether they will be willing to accept pricing policy changes (Marriott, 2020).

Based on the survey results, we found that according to the respondents' experience Slovenian legislation, which regulates private security, over-excessively interferes with said activity, especially in the area of human resources. Therefore, they propose a change in legislation that would positively impact employee recruitment. They view regulation of economic activity as a restriction of companies' flexibility and, consequently, their development. On the other hand, the president of the Chamber believes that the progression of private security activities requires more regulated mechanisms that will set proper guidelines for the safe usage of advanced technological solutions. The importance of legislation and regulation of technological development in security was also highlighted by

other respondents, who believe that the use of advanced technological solutions could excessively invade privacy and thus violate human rights. According to the respondents, the basic legislation in the field of private security is quite general in the part where it defines technical security systems and does not define aspects such as integration of information systems, digitalisation, advanced or smart technologies and applications. Quality implementation of private security activities requires well-organised mechanisms that would set guidelines for safe use for users of advanced technological solutions.

The study results also showed that Slovenian private security companies are aware of the importance of personnel education and training, so their employees regularly attend education and training courses. They also participate in public tenders for further training of security guards and work with secondary schools. Respondents also emphasised that technical skills and competencies will become increasingly important for working with advanced technologies.

By comparing traditional and modern approaches to security, we found that the use of advanced technological solutions could reduce human resources problems (for example, various solutions, including security robots and drones, can to some extent replace or facilitate traditional approaches to security, which in turn reduces the consumption of financial and human resources), but their use involves certain challenges related to their implementation in practice. Such challenges include: a) unexpected technical problems related to the use of advanced technological solutions, which in turn may pose a threat to residents; b) risks of misuse of personal data and excessive invasion of privacy; c) risks related to information and cybersecurity threats; d) changes in the required competencies of personnel and the set of education and training courses; and e) operating costs associated with the constant updating of systems, inspection and repair of technologies. In discussing the advantages and benefits of modern approaches to security provision, it is important to acknowledge that advanced technological solutions require constant human control (Sintal Koncern, 2017). These findings are also in line with the views of various authors, who agree that it is impossible to predict all possible events and that unexpected automation problems can lead to serious consequences in terms of safety (Hill, 2019). Nevertheless, modern technological solutions offer constant surveillance, filling the gap in traditional security and facilitating the work of security guards. The respondents also confirmed the effectiveness of solving human resources problems with the implementation of advanced technological solutions. The usefulness of advanced technological solutions is recognised mainly in the surveillance of larger areas and critical infrastructures. They also see the advantages of using advanced technologies in a smaller share of staff needed to perform tasks, greater security efficiency and tighter surveillance at night. Digital incident reports, smart applications for security guards, modern video surveillance systems and modern anti-burglary systems were emphasised as the most effective solutions that are currently most needed. Security robots and unmanned aerial vehicles are not yet included in the priorities, and even in such technologies, they recognise the usefulness for security activities. We can conclude that companies have needs for modernisation and digitisation of existing systems. In this respect, the respondents

emphasised that appropriate integration of technology and the human factor is needed to achieve higher quality.

In summary, the study results indicate that Slovenian private security companies are affected by numerous challenges, with technological advances and human resources problems being one of the most significant. Among others, pricing policy on the private security market was also highlighted as an important issue, since it hinders the development of private security companies and negatively affects their business success. At the same time, certain shortcomings of Slovenian legislation have been observed, especially in personnel recruitment. According to the respondents, the current legal regulation affects the flexibility of companies by excessive interference in their economic activity. Therefore, it seems that more efficient execution or implementation of advanced technological solutions in practice first requires the formation of strong foundations, which include efforts to achieve a stable private security market, improvements to working conditions for employees, and creation of regulation that will address management of security risks of advanced technological solutions.

Overall, we can deduce that if companies want to adapt to technological progress and respond appropriately to the challenges presented, they will have to upgrade traditional safety and work organisation approaches and resort to modern methods. Such changes depend not only on changes in legislation but also on internal measures in companies. Therefore, the management of private security companies is recommended to assess the quality of their security services and identify opportunities for improvement. It is also important that they strive to promote the motivation and commitment of employees and, accordingly, provide a positive organisational climate, a stronger organisational culture and offer existing staff an appropriate working environment.

5.1 Implications, limitations and future work

The theoretical contribution of the presented research is wide, as no in-depth research has been conducted on human resources issues and technological development in the Slovenian private security industry. Accordingly, qualitative research was conducted, which enabled an in-depth insight into the situation in practice, and the findings can be used to plan future research. Most of the literature on the topic of advanced technological solutions in security is in the form of expert discussions, so the article is generally a rare scientific contribution on the potential of advanced technological solutions in the private security industry. However, the main limitation of the research is related to sampling. As a research sample is not random and representative, special care in interpreting the results is needed.

The results are primarily helpful for private security companies. They represent the advantages and challenges of a modern approach to security and the circumstances that need to be considered when planning the implementation of advanced technological solutions in practice. The findings of the analysis of regulatory frameworks, which highlight the key challenges facing private security companies in practice, are also important for planning regulatory improvements in the future. The results are also intended for other stakeholders in private

security, especially in planning optimisation and development of activities in the future.

Based on the results of the research, certain aspects that would be worth exploring in the future have also emerged. Although we presented certain possibilities of technological development of private security activity, in order to develop comprehensive recommendations for the introduction of technological development in the private security industry in the future, it would be necessary to study good practices and analyse areas of protection in which it would make sense to implement advanced technological solutions. It would also be necessary to specify the types of technologies for each security service. In order to determine the cost-effectiveness of different approaches to security, it would be necessary to examine the solutions in more detail with appropriate financial benchmarking, as well as to make proposals for appropriate amendments to the legislation to address the identified challenges.

6 CONCLUSION

Technological development and innovations are important in the private security industry for several reasons, mainly because they contribute to greater competitiveness, reduction of human resources problems, and greater work quality and efficiency. Although technological development in the economy is inevitable, it is hampered in the private security industry by an unstable market and a lack of financial resources, the absence of regulation, and a lack of qualified security personnel. To ensure appropriate further development of the private security market, it is important to establish an adequate legal basis and political culture that will ascribe higher value to private security services and encourage clients to understand the importance of quality in providing security services. Based on the described technological changes, the development of the private security industry also requires proactive operation of private security companies. This means that companies should constantly monitor development trends, be familiar with the needs of their customers and the market in which they operate, and properly assess which solutions are most suitable for them. All of the above requires flexibility and innovation of companies and the ability to respond quickly to unexpected challenges. Considering the constant technological advances and current social trends, the demands for a safer environment and consequent demand for private security will increase in the future, resulting in the need for the private security industry to follow global trends if it wants to remain competitive. Since private security activity indirectly contributes to the common internal security and represents an important player in the system of plural policing, it is important that all key stakeholders are involved in the development of the field, including private security companies, legislators, clients and other entities associated with this economic activity.

REFERENCES

- Adams, W. L. (13. 7. 2012). British military to fill embarrassing security gap at the London olympics. *Time*. <http://olympics.time.com/2012/07/13/british-military-to-fill-embarrassing-security-gap-at-the-london-olympics/>
- Bendis, M. (27. 9. 2016). *Can security technology replace guard force?* Facility Executive. <https://facilityexecutive.com/2016/09/can-security-technology-replace-guard-force/>
- Bughin, J., Hazan, E., Lund, S., Dahlstrom, P., Wiesinger, A., & Subramaniam, A. (23. 5. 2018). *Skill shift: Automation in the future of the workforce*. McKinsey & Company. <https://www.mckinsey.com/featured-insights/future-of-work/skill-shift-automation-and-the-future-of-the-workforce>
- Button, M., & Lalonde, M. (2014). *State regulation concerning civilian private security services in their contribution to crime prevention in community safety*. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/justice-and-prison-reform/Civilian_Private_Security_Services_Ebook.pdf
- Celestina, I. (2013). Spoznanja in izzivi na področju zasebnega varovanja v Republiki Sloveniji [Findings and challenges in the field of private security in the Republic of Slovenia]. In *Zasebno varovanje v luči uporabnikov zasebno varnostnih storitev: Zbornik prispevkov*, (pp. 13–20). Zbornica za razvoj slovenskega zasebnega varovanja.
- Cobbina, J., Nalla, M., & Bender, K. (2016). Security officers' attitudes towards training in their work environment. *Security Journal*, 29, 385–399. <https://doi.org/10.1057/sj.2013.34>
- Davis, R., & Pease, K. (2000). Crime, technology in the future. *Security Journal*, 13, 59–64. <https://doi.org/10.1057/palgrave.sj.8340050>
- El Dorado. (28. 2. 2017). *Relying on technology in the security industry*. El Dorado Insurance Agency, Inc. <https://www.eldoradoinsurance.com/security-industry-news/relying-on-technology-security-industry/>
- El Dorado. (28. 9. 2019). *Changing of the guards: How the private security industry is evolving*. El Dorado Insurance Agency, Inc. <https://www.eldoradoinsurance.com/el-dorado-news/changing-of-the-guards-how-the-private-security-industry-is-evolving/>
- Fenwick, M., Kaal, W. A., & Vermeulen, E. M. P. (2017). Regulation tomorrow: What happens when technology is faster than the law?. *American University Business Law Review*, 6(3), 16–23. <https://doi.org/10.2139/ssrn.2834531>
- Fiber SenSys. (2012). *Microwave perimeter security*. FiberSenSys.com <https://fibersensys.com/product-information/download-file?path=A+and+E+Documents%2FAApplication+Notes+-+PDF%2FAN-SM-011+Microwave+Perimeter+Security+Application+Note+-+Rev+A.+6-12.pdf>
- G. C. (23. 4. 2013). Večina varnostnikov prejema zgolj minimalne plače [Most security guards on minimum salary]. MMC RTV SLO. <https://www.rtvlo.si/gospodarstvo/vecina-varnostnikov-prejema-zgolj-minimalne-place/307323>
- González, F. (14. 2. 2019). *A la baja empresas de seguridad privada por falta de personal*. El Sol de Salamanca. <http://www.elsoldesalamanca.com.mx/local/a-la-baja-empresas-de-seguridad-privada-por-falta-de-personal-3062159.html>
- Grabosky, P. (2007). Security in the 21st century. *Security Journal*, 20, 9–11. <http://>

- doi.org/10.1057/palgrave.sj.8350036
- Hikvision Digital Technology (HDT). (18. 3. 2022). *Top 8 trends for the security industry in 2022*. CISION PR newswire. <https://www.prnewswire.com/news-releases/top-8-trends-for-the-security-industry-in-2022-301461128.html>
- Hill, R. (20. 5. 2019). *What role do robots have as security guards?* Colocation America. <https://www.colocationamerica.com/blog/robot-security-guards>
- Joh, E. E. (2017). A certain dangerous engine: Private security robots, artificial intelligence, in deadly force. *UC Davis Literature Review*, 51(1), 569–587. <https://ssrn.com/abstract=3048394>
- Knightscope. (n. d.). *Knightscope credited for reducing crime*. <https://www.knightscope.com/crime>
- Kyodo. (19. 4. 2018). *Over 90% of security companies suffering staff shortages, police survey shows*. The Japan Times. <https://www.japantimes.co.jp/news/2018/04/19/national/90-security-companies-suffering-staff-shortages-police-survey-shows/#.XJ5Nz5hKjIV>
- Kyung-Hoon, K, Soonil, B., & Kwanghak, H. (2010). Intelligent surveillance in security robot systems. In *IEEE Workshop on Advanced Robotics in its Social Impacts*, (pp.70–73). IEEE. <https://ieeexplore.ieee.org/abstract/document/5679624>
- Leenes, R., Palmerini, E., Koops, B., Bertolini, I., Salvini, P., & Lucivero, R. (2017). Regulatory challenges of robotics: Some guidelines for addressing legal in ethical issues. *Law, Innovation in Technology*, 9(1), 1–44. <https://doi.org/10.1080/17579961.2017.1304921>
- Lim, S. L., & Nalla, M. K. (2014). Attitudes of private security officers in Singapore toward their work environment. *Journal of Applied Security Research*, 9(1), 41–56. <https://doi.org/10.1080/19361610.2014.851579>
- Lin, P., Bekey, G. A., & Abney, K. (2009). Robots in war: Issues of risk in ethics. In R. Capurro, M. Nagenborg & G. Tamburinni (Eds.), *Ethics and robotics*, (pp. 83–103). IOS Press.
- Ludwig, S. (9. 3. 2018). *Drones: A security tool, threat and challenge*. *Securitymagazine.com*. <https://www.securitymagazine.com/articles/88803-drones-a-security-tool-threat-and-challenge>
- Madakam, S., & Date, H. (2016). Security mechanisms for connectivity of smart devices in the internet of things. In Z. Mahmood (Ed.), *Connectivity frameworks for smart devices*. Springer. https://doi.org/10.1007/978-3-319-33124-9_2
- Marriott, M. (14. 5. 2020). *How to reduce security guard expenditure despite the increasing labour: Property management in procurement*. Pegaxis. com. <https://www.pegaxis.com/blog/how-to-reduce-security-guard-expenditure-despite-the-increasing-labour-costs>
- Nalla, M. K., & Cobbina, J. E. (2017). Environmental factors in job satisfaction: The case of private security guards. *Security Journal*, 30, 215–226. <https://doi.org/10.1057/sj.2016.12>
- Papademetriou, T. (2016). European union. In *Regulation of drones*, (pp. 122-132). The Law Library of Congress, Global Legal Research Center. https://irp.fas.org/congress/2016_rpt/lloc-drones.pdf
- Pavlic, V. (30. 4. 2016). *Private security companies in Croatia faced with lack of staff*.

- Totalcroatiannews.com. <https://www.total-croatia-news.com/business/11646-private-security-companies-in-croatia-faced-with-lack-of-staff>
- Pavšič, G. (23. 6. 2014). *Varnostne službe v Sloveniji z dobički, za varnostnike slaba plača* [Security services in Slovenia with profits, security guards on low salaries]. Siol.net. <https://siol.net/novice/slovenija/varnostne-sluzbe-v-sloveniji-z-dobicki-za-varnostnike-slaba-placa-111822>
- Pfeiffer, S. (2016). Robots, industry 4.0 in humans, or why assembly work is more than routine work. *Societies*, 6(2), 1–26. <http://dx.doi.org/10.3390/soc6020016>
- Pistorius, C. (2018). *The impact of emerging technologies on the private security industry*. Delta Hedron. <https://deltahedron.co.uk/the-impact-of-emerging-technologies-on-the-private-security-industry/>
- Protect. (20. 5. 2020). *Sodobne varnostne rešitve* [Modern security solutions]. PROTECT – Infra varnostni inženiring. <https://www.protect.si/za-vas-posel/sodobne-varnostne-resitve/>
- Radonjič, G. (2013). *Tehnološki sistemi in integrirano varstvo okolja* [Technological systems and integrated environmental protection]. Ekonomsko-poslovna fakulteta.
- Ridenhour, J. (18. 3. 2022). *New technology in the security industry 2022*. Dsisecurity.com. <https://www.dsisecurity.com/2022/01/13/new-technology-in-the-security-industry-2022/>
- Savski, S. (2013). Izbira ponudnika zasebnega varovanja v javnem sektorju – Kaj lahko za izboljšanje stanja storijo izvajalci? [Selection of private security provider in the public sector – What can providers do to improve the situation?] In *Zasebno varovanje v luči uporabnikov zasebnih varnostnih storitev: Zbornik prispevkov*, (pp. 38–43). Zbornica za razvoj slovenskega zasebnega varovanja.
- Servoz, M. (2019) *The future of work? Work of the future! On how artificial intelligence, robotics in automation are transforming jobs and the economy in Europe*. European Commission. https://ec.europa.eu/epsc/sites/epsc/files/ai-report_online-version.pdf
- Sintal Concern. (2017). Roboti v varovanju. *Sintalček*, 75, 6–10.
- SMP Robotics. (25. 7. 2019). *Security robots outdoor patrolling, video & thermal surveillance for security service companies*. SMP Robotics. https://smprobotics.com/security_robot/
- SSI Staff. (18. 12. 2018). *Experts share their top 5 challenges facing the security industry in 2019*. Security Sales & Integration. <https://www.securitysales.com/business/challenges-security-industry-2019/>
- Stinger Security. (12. 5. 2020). *Tehnično varovanje* [Technical security]. Stinger.si. <https://stinger.si/tehnico-varovanje>
- Sunstates Security. (12. 5. 2020). *How technology is transforming the security industry*. Sunstatesecurity.com. <https://www.sunstatesecurity.com/technology-transforming-security-industry/>
- Theodoridis, T., & Huosheng, H. (2012). Toward intelligent security robots: A survey. *IEEE Transactions on Systems in Cybernetics*, 42(6), 1219–1230. <https://ieeexplore.ieee.org/document/6392475>
- Turner, B. (15. 12. 2015). *Drones for private security*. American Security Force. <https://>

- www.americansecurityforce.com/drones-for-the-private-security
Vincent, J. (26. 6. 2018). *This Japanese AI security camera shows the future of surveillance will be automated*. The Verge. <https://www.theverge.com/2018/6/26/17479068/ai-guardman-security-camera-shoplifter-japan-automated-surveillance>
- Yeboah-Ofori, A, & Brown, AD. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Journal of Forensic Legal & Investigative Sciences*, 6. <http://dx.doi.org/10.24966/FLIS-733X/100045>
- Zakon o spremembah in dopolnitvah Zakona o preprečevanju omejevanja konkurence (ZPOMK-1G) [Act Amending the Prevention of Restriction of Competition Act]. (2017). *Uradni list RS*, (23/17).
- Zavod RS za zaposlovanje. (2019). *Napovednik zaposlovanja 2019/II – Kaj delodajalci napovedujejo za slovenski trg dela za prvo polovico leta 2020?* [Employment forecast 2019/II – What do employers predict for the slovenian labour market for the first half of 2020?]. https://www.ess.gov.si/_files/12836/Porocilo_napovednik_zaposlovanja_2019_II.pdf

ABOUT THE AUTHORS:

Miha Dvojmoč, PhD, Assistant Professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: miha.dvojmoc@fvv.uni-mb.si

Patricija Lunežnik, M.A. in Criminal Justice and Security. E-mail: patricija.luneznik@student.um.si

Kaja Prislan, PhD, Assistant Professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor. E-mail: kaja.prislan@fvv.uni-mb.si

The Use of Tools for Obtaining Data From Publicly Accessible Sources for the Purpose of Competitive Intelligence in Enterprises

VARSTVOSLOVJE
*Journal of Criminal
Justice and Security*
year 23
no. 4
pp. 425–446

Žiga Primc

Purpose:

Article seeks to determine the state of affairs of research in using tools to obtain data from public sources for competitive intelligence activities. The author wishes to offer an overview of what already exists and shed light on areas that merit further research efforts.

Design/Methods/Approach:

A systematic literature review was made using the PRISMA method in the Scopus and IEEE Xplore databases. The review included 23 articles published between 2011 and 2021.

Findings:

Over the past decade, the practice of obtaining data from publicly accessible sources has developed extremely rapidly, and this can be attributed mainly to the rapid advances in technology, the digitalisation the operations of organisations, and to the immeasurable quantities of data that appear every day on the internet. New fields are emerging in obtaining data from publicly accessible sources, and more effective tools are being developed to automate processes. Existing studies highlight the importance of competitive intelligence activities by means of obtaining data from publicly accessible sources for organisations. At the same time, they identify a lack of trained personnel and adequate software systems for optimal business use.

Practical Implications:

The findings of this article offer an insight into research of competitive intelligence activities and highlights the research gaps and formulates starting points for future research.

Originality/Value:

The article is the first systematic literature review in obtaining data from publicly accessible sources for the purpose of competitive intelligence activities to support better decision-making in business environments.

Keywords: Open Source Intelligence, competitive intelligence, systematic literature review, tools, public sources.

UDC: 004.6

Uporaba orodij za pridobivanje podatkov iz javno dostopnih virov v okviru konkurenčne obveščevalne dejavnosti v podjetjih

Namen prispevka:

Namen prispevka je s pomočjo sistematičnega pregleda literature ugotoviti uporabnost orodij za pridobivanje podatkov iz javnih virov v okviru konkurenčne obveščevalne dejavnosti v podjetjih. Na podlagi analize obstoječega stanja želimo izpostaviti vsebine za nadaljnje raziskovanje.

Metode:

Narejen je bil sistematični pregled literature po metodi PRISMA v bazah podatkov Scopus in IEEE Xplore. V končni pregled je bilo vključenih 23 prispevkov, ki so bili objavljeni med letoma 2011 in 2021.

Ugotovitve:

Področje pridobivanja podatkov iz javno dostopnih virov se v zadnjem desetletju razvija izjemno hitro, kar gre pripisat predvsem hitremu tehnološkemu razvoju, digitalizaciji poslovanja organizacij ter neizmerljivim količinam podatkov, ki se vsakodnevno znajdejo na internetu. Odkrivajo se nova področja uporabe pridobivanja podatkov iz javno dostopnih virov, razvijajo se učinkovitejša orodja za avtomatizacijo procesov. Obstoječe študije izpostavljajo pomembnost konkurenčne obveščevalne dejavnosti z uporabo pridobivanja podatkov iz javno dostopnih virov za organizacije, hkrati pa ugotavljajo pomanjkanje usposobljenega kadra in programskih rešitev za optimalno poslovno uporabo.

Uporabnost raziskave:

Ugotovitve prispevka nudijo vpogled v raziskovalno dejavnost na področju konkurenčne obveščevalne dejavnosti ter lahko služijo kot osnova za raziskovanje tega področja. V prispevku so izpostavljene raziskovalne vrzeli in oblikovana izhodišča za prihodnje raziskave.

Izvirnost/pomembnost prispevka:

Gre za prvi sistematični pregled literature na področju uporabe pridobivanja podatkov iz javno dostopnih virov za namen konkurenčne obveščevalne dejavnosti kot podpore za boljše odločanje v poslovnih okoljih.

Ključne besede: pridobivanje podatkov iz javno dostopnih virov, konkurenčna obveščevalna dejavnost, sistematični pregled literature, orodja, javni viri

UDK: 004.6

1 INTRODUCTION

Obtaining data from publicly accessible sources for competitive intelligence activities is a field in which not much has yet been written. Despite this, the field has been gaining attention in recent years. When we speak of obtaining data from publicly accessible sources, we usually encounter the better-known term Open-Source Intelligence or OSINT. This is an expression that dates back more than 70 years, and in comparison, with its beginnings, up to the present day – especially in terms of the method of obtaining information due to technological advances – a lot has changed. Credit for this can be claimed principally by the significant advances in information technology and the digitalisation of everyday life and business. In the review of works dealing with obtaining data from publicly accessible sources, we can quickly see businesses, for the most part, focus on cybersecurity and preventing threats. Open sources of data are excellent for obtaining the majority of information that the state, armed forces or a company might need. Competitive intelligence is the process and forward-looking practices used in producing knowledge about the competitive environment to improve organisational performance (Madureira et al., 2021) and involves systematic collection and analysis of information from multiple sources. It can be described as the action of defining, gathering, analysing, and distributing intelligence about products, customers, competitors, and any aspect of the environment needed to support executives and managers in strategic decision making for an organisation. When we speak of competitive intelligence, we can see that much has been researched and written in terms of preventive measures (cybersecurity, other threats to organisations). For instance, online social networks are used to obtain information about the competition, and they can also be used to identify threats and for taking timely action (Ansari et al., 2013; Al-khateeb & Agarwal, 2020; Yaboah-Ofori & Brimicombe, 2017) as well as for detecting potential outbreaks of disease (Bernard et al., 2018). More recent fields of interest include artificial intelligence (AI) in connection with obtaining data from publicly accessible sources (Gonçalves Evangelista et al., 2020), which in the future could also be used in competitive intelligence or for identifying threats to an organisation, based on the identification of specific topics in texts that are freely available (Li et al., 2020).

This article focuses on a review of those sources that relate exclusively to competitive intelligence activities in connection with obtaining data from publicly accessible sources.

2 METHOD

The systematic review of the literature in the field of using tools for obtaining information from publicly accessible sources (open-source intelligence - OSINT) for the purpose of competitive intelligence was conducted in the international bibliographical databases Scopus and IEEE Xplore. The search string used to find articles contained various key words: ((OSINT OR »public sources« OR »corporate intelligence« OR »private *intelligence« OR »competitive intelligence« OR »threat intelligence« OR »cyber intelligence«)). We searched for a combination of selected keywords in titles, summaries and keywords of articles. The review

of the literature was performed on 12 August 2021. Our inclusion criteria covered articles published in 2011 or later and articles written in Slovenian or English. As the field of tools for the use of OSINT in the context of competitive intelligence is developing rapidly technologically, it made sense to include only contributions that are not more than a decade old in the analysis. The use of the specific databases stems from the fact that IEEE Xplore is one of the most important databases linked to information technology, and Scopus is an exceptionally broad and abundant collection of articles. The reason for the absence of the Web of Science database, which would otherwise have been used in our article, is that at the time of searching for material and writing the article that database was experiencing technical difficulties, which prevented us from exporting a list of articles for analysis. We then excluded from the array of articles duplicated articles, those that were not open-source and those that do not relate to obtaining data from publicly accessible sources and competitive intelligence. In reviewing the full text of articles, in the final stage, we excluded irrelevant research and those articles that do not include the basic search terms. The inclusion and exclusion criteria are presented in Table 1.

Table 1: The inclusion and exclusion criteria for systematic literature review

Inclusion criteria	Exclusion criteria
Articles published in scientific journals or conference papers	Books, chapters in books, early accesses, discussions, introductions, reviews.
Articles published between 2011 and 2021	Articles published before 2011
Articles in Slovenian and English	Articles in other languages
Free access to the article	Inaccessibility of the full article
Thematic relevance of the article	Articles that do not relate to the use of public sources, obtaining data from publicly accessible sources and competitive intelligence.

The process of collecting and identifying appropriate articles is presented through a PRISMA diagram in Figure 1.

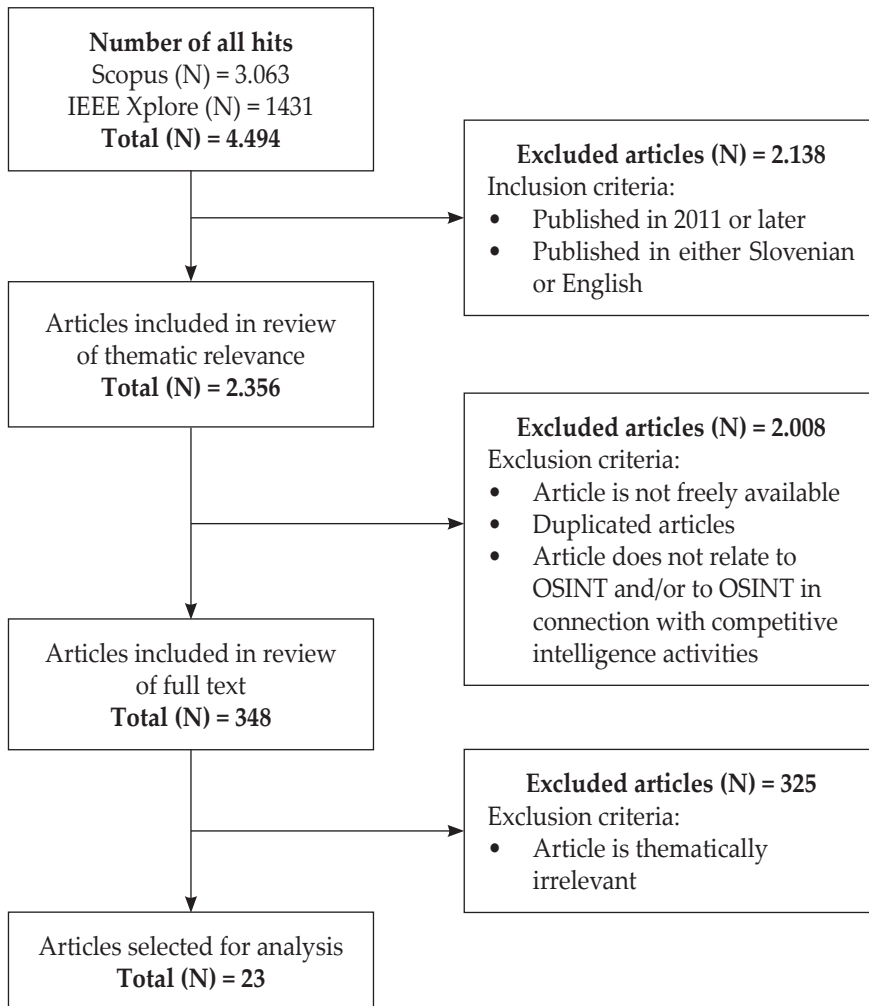


Figure 1:
The flow of
searching
and selecting
literature

Based on the criteria presented in Table 1, we can conclude that only a small number of articles are useful for in-depth analysis. Although we initially detected many contributions in both databases, we excluded most of them because they do not analyse the use of the OSINT method in relation to competitive intelligence.

3 RESULTS

The first search for articles with the described search string yielded 4,495 results. Taking into account the inclusion and exclusion criteria, and after excluding duplicates, 23 articles remained for the final analysis. A description of the articles included in the systematic review of the literature is shown in Table 2.

The Use of Tools for Obtaining Data ...

Author and title of article	Type of article and predominant method	Purpose of the article	Key findings of the article
[Anand et al., 2020] PeopleXploit- A hybrid tool to collect public data	review article; presentation of tools	Presents an approach that illustrates the OSINT concept as an important application in profiling individuals.	The PeopleXploit approach makes use of a hybrid tool that aids in the public gathering of available information that is reliable and important for the data searcher.
[Benes, 2013] OSINT, New technologies, education: expanding opportunities and threats. a new paradigm	review article	Analyses how rapidly advanced technology is changing information and consequently the obtaining of data from publicly accessible sources.	The development of new technologies and education in this area are essential for an adequate understanding and use of various OSINT tools. These tools represent the future of obtaining digital intelligence data.
[Best, 2011] Challenges in open source intelligence	review article	Identification of the future challenges regarding tools for obtaining data from publicly accessible sources	Nowadays access itself to gather information using OSINT no longer represents a challenge, it is the analysis of the obtained data that is problematic.
[Buccafurri et al., 2020] Implementing multiple-social-network meta-APIs to support OSINT programming	review article; presentation of model	Points out that despite the availability of tools and platforms for OSINT, gaps exist in terms of software engineering.	Social networks today represent an important source of information and are frequently a basis for OSINT research. In this article the authors present the approach of user-centred social networks programming, whereby pieces of information can be merged and linked, and for OSINT research this is consequently more systematic.

[Černya et al. 2019] Using open data and Google search data for competitive intelligence analysis	review article; presentation of model	Analysis of the competitive environment using OSINT in the health sector.	The analysis of the competitive environment is set out in a reliable time frame, and obtains all the necessary competitive data important for determining the competitiveness of a company.
[Chae et al., 2019] A system approach for evaluating current and emerging army open-source intelligence tools	review article; presentation of model	An assessment of the current situation and examination of emerging OSINT tools and technology.	In the military OSINT is a tool that offers useful information and is used principally for obtaining competitive data and potential threats. At the same time OSINT improves both privacy and protection against threats. Through systemic analysis the authors concluded that certain OSINT tools do not fully meet the requirements of the military, since new tools have been developed on the market that could be more effective.
[Chi & Chen, 2013] Collaborative competitive intelligence: A knowledge base system approach	review article; presentation of model	A definition of the development and presentation of a decision-making platform for boosting the competitive intelligence activities of a company.	The knowledge base system has achieved the aim of targeted competitive intelligence activities and has proven to be successful and reliable. Companies can use these data in formulating strategic objectives.
[Di et al., 2014] Research on enterprise competitive intelligence development and strategies in the big data era	original science article; quantitative research	Presents the development and importance of competitive intelligence activities in the age of digitalisation.	The development of competitive intelligence activities has recently been reaching new heights, since enterprises and organisations are aware of their importance. The digitalisation of data enables the development of various OSINT tools that can comprehensively gather all the necessary information for formulating a competitive strategy based on data about competing enterprises in a completely legal way.

The Use of Tools for Obtaining Data ...

[Dorton et al., 2019] A theoretical model for assessing information validity from multiple observers	original science article; qualitative research and presentation of model	Presentation of a model/approach for assessing the validity of information obtained from HUMINT and OSINT.	In the authors' assessment the approach is appropriate and good, but gaps remain particularly in terms of programming, and these need to be addressed. The focus should be on obtaining information that is not just relevant but also valid.
[Goujon, 2011] Text mining for opinion target detection	review article; presentation of model	Presentation of a model for automated gathering of opinions on a specific topic.	Using text mining it is possible to obtain information on opinions linked to a given topic, for the purpose of competitive intelligence activities. Going forward, a more comprehensive review of sources is needed to confirm the relevance of these opinions for the end user.
[Hribar et al., 2014] OSINT: A "Grey Zone"?	review article	Presentation of elements of intelligence activities and the use of <i>fuzzy logic</i> in OSINT.	OSINT is an excellent way of gathering intelligence data that does not violate human rights and is also lawful. OSINT is also a formal tool and means of analytical support in the work of intelligence services –this can also at times be questionable and creates a grey zone in its use.
[Hu & Zhu, 2013] Competitive intelligence acquisition from websites	review article; case study	Analysis of the area of obtaining information from company websites.	Use of competitive intelligence activities is an important method of obtaining information about the competition in the information age. Publicly accessible information on websites offers an excellent insight into information about a company, though this needs to be enhanced by an analysis of data from other publicly accessible databases.

[Pais & Ciobanu, 2014] OSINT for B2B platforms	review article; presentation of software	Determines the possibility of including OSINT via the application Cloud.ro in B2B platforms.	The applicability of OSINT in a B2B platform has been shown to be good and very useful, especially in terms of obtaining information about companies, information on company activities, information on employees and information on business partners.
[Pastor-Galindo et al., 2020] The not yet exploited goldmine of OSINT: opportunities, open challenges and future trend	review article;	Analysis and review of the current state of development of OSINT and a comprehensive overview of the paradigm, with emphasis on technology and services.	OSINT is developing rapidly, and innovative applications are being designed for use in various fields. The authors see the greatest potential for its use as lying in proactive use to detect cyber threats and in the public sphere (especially state authorities), where OSINT represents an ideal tool for obtaining diverse information, including about competitors.
[Rai et al., 2021] Using open source intelligence as a tool for reliable web searching	review article; presentation of model	Analysis of OSINT tools and formulation of a proposed possible new development.	OSINT gathers and obtains data from web servers or sources that are freely accessible. OSINT provides a more rapid means of searching for and filtering data.
[Ranjan & Foropon, 2020] Big data analytics in building the competitive intelligence of organisations	original science article; qualitative research	A study of data in a competitive environment and presentation of the context of the development of competitive intelligence in the future.	Monitoring competitors by means of OSINT has already become an everyday practice, since it enables a determination of the competitiveness of companies. For the most part, companies have a highly centralised, informal process of gathering such data, and development must be oriented towards advanced machine learning based on targeted methods.

The Use of Tools for Obtaining Data ...

[Rasekh, 2015] A new competitive intelligence-based strategy for web page search	review article; presentation of model	Presents a model for searching higher-quality websites, based on competitive intelligence.	The proposed system combines the ICA algorithm and the scheme of classification based on links. The aim of the model is to improve search results, but additional work is needed for the model to be adapted to the web.
[Schaurer & Störger, 2013] The evolution of open source intelligence (OSINT)	review article	Presentation of the development of OSINT.	They define OSINT as a collection, processing, analysis and classification of information obtained from sources in a way that is open and legally accessible. In essence, OSINT emerged as an intelligence discipline in the domain of the state, which in recent times has contributed to the integrated process of managing sources also in the private sector.
[Semerkova et al., 2017] Application of information technologies in competitive intelligence	review article	Presents the concept of competitive intelligence, the intelligence cycle and competitive intelligence tools on the internet.	By means of competitive intelligence, an enterprise can create a competitive advantage, so this is an important strategic orientation for the enterprise. An analysis of the weaknesses and vulnerabilities of competitors is therefore essential, and using OSINT tools can aid in this.
[Sharma et al., 2013] Big data – competitive intelligence	review article; presentation of model	Presents a model for tackling the challenges of organisations adapting to a competitive market by means of obtaining competitive data.	Nowadays obtaining data is no longer as complicated as it once was, due to the availability of various OSINT tools. All the more important data can be obtained from publicly accessible sources, but a systematic review of the data remains the challenge.

[Sondrava et al., 2021] Prevention to sensitive information disclosure via OSINT	review article	A description of OSINT tools and approaches for searching sensitive information online.	The best protection against sensitive information is provided by automated and payable OSINT tools, while at the same time many OSINT tools represent potential 'weapons', since they enable individuals to access information and data which they can use for malicious purposes.
[Wang et al., 2011] Construction and operation of cultivation model for enterprise competitive intelligence competence	review article; presentation of model	Design of a cultivation model for competitive intelligence	This represents an additional value of competitive intelligence, and is regarded as an effective means of raising the competitiveness of a company, if that company has the skills to use it. This plays an important part in shaping business processes and strategies, and competitive must be built both upon internal and external factors.
[Yang & Lee, 2012] Mining open source text documents for intelligence gathering	review article; presentation of model	Formulates an approach for OSINT with the aim of automating the gathering of intelligence data	The gathering and analysis of intelligence data plays an important part in the growth of a company. OSINT is the main approach for gathering and analysing intelligence data, but this is hampered by a lack of automation. The authors have developed a tool that fills this gap and is applicable especially in the area of business intelligence and personal management.

In the use of keywords, we had to set out the search string more broadly since there are too few actual works containing the term OSINT in the title for conducting a systematic review of the literature. For this reason, we spent more time on the actual review of all sources, and consequently obtained better results. In terms of content, we divided the articles into four groups, specifically 1) those that generally address actual OSINT, 2) those that present a specific solution, 3) those that present a model for obtaining and analysing OSINT data, and 4) those that present a model for evaluating the data obtained. We did not include the Web of Science database in our selection of literature because, at the time of gathering articles for review, that website was experiencing technical difficulties that prevented the export of results.

3.1 Review of the field of obtaining data from publicly accessible sources

The best-known definition of Open-Source Intelligence (OSINT) is that this is intelligence data “produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement”. The term was defined by both the U.S. Director of National Intelligence (DNI) and U.S. Department of Defense (DoD). Schaurer and Störger (2013) expand the concept somewhat into the “collection, processing, analysis, production, classification, and dissemination of information derived from sources and by means openly available to and legally accessible and employable by the public in response to official national security requirements.”

The first signs of efforts to gather data from publicly accessible sources appeared with the establishing of the Foreign Broadcast Monitoring Service (FBMS) in 1941, which was originally intended to monitor foreign (printed and spoken) media. Later on, after the Japanese attack on Pearl Harbour the area of obtaining information from public media gained in importance. After the war, in 1947, this was placed under the administration of the U.S. Central Intelligence Agency (CIA), with the title Foreign Broadcast Intelligence Service (FBIS) (Shaurer & Störger, 2013).

Over decades this field was modified and adapted to changes, and this can be seen most prominently in the last decade, during the period of accelerated digitalisation. While it started out monitoring printed media, radio and later television, today the area of OSINT is focused for the most part on digital media. Pastor-Galindo et al. (2020) state that the quantity of data generated by today’s extraordinarily connected world is immeasurable. These data are for the most part accessible to the public and available whenever and wherever. The main sources they mention are the mass media, online social networks, blogs, forums, public administration data, commercial data and publications.

Rai et al. (2021) see obtaining data from publicly accessible sources as a process comprising the following steps: 1) identification of the source, 2) obtaining data, 3) integration and processing of data, 4) analysis of data and 5) delivery of the final result to the relevant recipient. The steps involved in the competitive intelligence cycle were set out in a similar way by Semerkova et al. (2017), who state that

the cycle is made up of defining the objectives, gathering data, analysing data, delivering information to the final recipient and use of the information obtained. Pastor-Galindo et al. (2020) described the process more simply, involving three steps of gathering, analysis and acquiring knowledge. In their article the authors for the most part are concerned with cybersecurity and use of data acquisition from publicly accessible sources for this purpose.

Analysis of the literature has shown *inter alia* that authors focus on two approaches in using data acquisition from publicly accessible sources: offensive and defensive. The first approach can be more easily placed in the framework of competitive intelligence, i.e., obtaining information on one's competitors on the market, while the second, which is much more prominent, serves to obtain information from public sources through open-source data acquisition for a timely response to cyber and other threats, which ultimately affords organisations a competitive advantage. The timely reaction to an unexpected scenario, for instance a cyber-attack, can in certain cases mean life or death for an organisation.

While obtaining publicly accessible data can have major benefits for an organisation, on the other hand this area is still in a very early stage of development, and the question is, can the development of new technologies catch up in terms of effective use of tools and models for gathering public data. Pastor-Galindo et al. (2020) strikingly delineate the advantages and weaknesses of obtaining data from publicly accessible sources. Among the advantages they list the huge quantity of available information, the massive computer power (when we speak of gathering/searching information), the concept of *big data*¹ and machine learning, the complementarity of data, flexibility of use and the wide selection, while they highlight the weaknesses of complexity and data management, non-structured information, erroneous or false information, reliability of the actual sources of information and ethical or legal reservations. This last factor has been a topic of numerous debates for some time. The grey zone of obtaining data from publicly accessible sources and how this issue can be resolved was written about by Hribar, et al. (2014), who are focused on traditional intelligence activities, although here we can clearly draw parallels with competitive intelligence activities. They state that obtaining data from publicly accessible sources in the majority of cases is accepted, since it involves legal form of information gathering, up until a human right is violated. The personal data of individuals can generate a legal conflict in obtaining data from public sources, so there is a need to respect the legislation governing human rights and privacy (Schaurer & Störger, 2013).

Using tools to obtain data from publicly accessible sources, it is easy to obtain information, and anyone can do it if they decide to acquire these tools, but the harder part is the actual analysis of data, which requires a trained and experienced expert, if you want to achieve optimal results (Hribar et al., 2014). Raw data obtained from public sources can only be assembled into a meaningful whole by someone who requires the legal and technical knowledge, analytical skills and powerful tech support for this (Schaurer & Störger, 2013). The challenge today is no longer how to obtain information, but how to whittle down the

¹ In the opinion of Saša Mojsilović, a court expert for big data at IBM, in 2020 some 40 (Dolenc, 2014) or 44 zettabytes (Microsoft, 2019) of data will be generated in the world (one zettabyte is 44 billion gigabytes). Today the average personal computer has one or two terabytes of memory.

information obtained to what is relevant. For this reason, there is also a need to further develop the tools that will offer appropriate technical support (Best, 2011). Legitimate use of tools for data acquisition from publicly accessible sources will be possible in the long term through the proper education and training of those who will be involved in it, be it in an organisation or for organisations as a service on demand. Benes (2013) notes that what is needed for an outstanding analyst, alongside excellent theoretical and practical training, is a mindset that espouses lifelong learning. The area of data acquisition from publicly accessible sources is one of the most rapidly developing areas, and the development of personnel here will also require outstanding teachers, schools and training programmes, a general awareness in the public about the opportunities that await in this field and the development of technical support that will deal with the problem of the quantity of information.

Competitive intelligence using big data is an enhanced form of using data acquisition from publicly accessible sources. As determined by Ranjan and Foropon (2020), competitive intelligence using big data involves a complex approach that can offer greater value for practical application. Difficulties arise in analysis, in a way that is similar to obtaining data from publicly accessible sources, except that the quantity of data is significantly greater. In their empirical research they have found that for the most part companies do not see any rational need to implement the big data approach in their competitive intelligence procedure, since they are convinced that they know the market and their competitors well. They also highlight the problems in recruiting appropriate personnel, for as they have found, operatives lack the essential advanced analytical abilities to process, interpret and present results to support decision-making.

3.3 Presentation of systems/tools

In the review of articles over the past ten years we have seen that there have been initiatives and actual development of (software) systems for use in competitive intelligence. Pais and Ciobanu (2014) talk of a purpose-built platform resulted from their development and serves for obtaining data on competitor companies, specifically information on the company, information on activities in their domain, employee data and information on the main business partners. As the authors assert, the system itself can be included in existing platforms.

To obtain data from publicly accessible sources or competitive intelligence, online social networks are a rich source of data, but due to their closed nature, they do not enable free browsing of content in one place. Searching for information can consequently be time-consuming. Buccafurri et al. (2020) propose programming a *meta-API*, which will enable user-centred searching through various social networks. The software itself could enable the developers to create a dedicated tool that could search on various social networks for the location of an individual, their friends or contacts, the use of hashtags and so on. Simultaneous searching by user profiles on different social networks offers us a more complete picture of their activities, since in this way we can merge together information on their leisure

time (e.g. Facebook, Instagram and Twitter) and from the business environment (e.g. LinkedIn).

Checking out individuals is also pursued more broadly in practice, outside the online social networks. Here we can speak of information gathering for competitive intelligence purposes, and background-checking an individual before employment. A very important factor in acquiring publicly accessible information is the already mentioned protection of personal data, i.e. encroachment on privacy. It is always essential to have a legal basis for this kind of searching in such cases. *PeopleXploit* is a tool created for the purpose of increasing the relevance score in profiling, according Anand et al. (2020). This is a hybrid tool that aids in collecting publicly available information that is reliable and relevant to the given input, such as name, surname, e-mail address, telephone number, and so forth, in other words, the user's digital footprints. Once the search is complete, the tool offers an analysis, which differs depending on the purpose of the search.

The majority of the information gathered by means of data acquisition from publicly accessible sources is analysed today manually, since the market does not yet offer sufficient applicable tools that could perform this reliably, or rather such tools have not username yet been perfected. Since analysis is time-consuming, Yang and Lee (2012) and their associates developed an approach for automatic data processing based on text mining techniques. The authors assert that the approach can automatically identify important events, whereby it is able to see from different angles. Actual awareness of such events would offer companies benefits in their decision-making. Text mining techniques can be applicable in the areas of national security and e-learning and also in competitive intelligence.

A similar approach to text mining was taken by Goujon (2011), in connection with obtaining public opinions regarding a specific target. His text mining technique is based on linguistic knowledge and linguistic patterns that automatically identify the target opinions being sought, for the purpose of competitive intelligence. The author tested the tool in specific cases. The results have shown potential in the application of the method, but also deficiencies and indications for further work. Searching opinions and terms can be an extremely complex task due to the dynamics of language and the consequences of dialects and multilingualism. The success of the method therefore depends on a large database of terms through which text is mined and opinions found.

Open-source tools and others that are freely available or available against payment can be found very quickly on the internet. Some tools are extremely powerful, while others are very niche-oriented. In their article, Pastor-Galindo et al. (2020) analyse well the majority of relevant automated data acquisition tools that are currently available and applicable. These tools are divided up by purpose or field of searching:

1. Tools that serve for obtaining information on identity, network information and information on files: FOCA, Maltego, Recon-NG;
2. Tools that serve for obtaining network information and information on files: Metagoofil;
3. Tools that serve for obtaining network information: Shodan, Spiderfoot;

4. Tools that serve for obtaining network information and information on identity: The Harvester, IntelTechniques (limited functioning).

3.3 Models/methods of obtaining data for decision-making purposes

With the aim of improving information searches using data acquisition from publicly accessible sources, numerous authors have presented a method of obtaining data or have set out a model that takes the user through the process.

A simple but effective way of obtaining and analysing data has been presented by Černý et al. (2019) in their attempt to use publicly accessible data in the pharmaceutical sector. They have found that using publicly accessible user data on the use of tablets is possible to obtain a legitimate picture of the state of health trend in the population, which can be used very effectively in terms of competitive advantage. In their experiment the skill level of the analysts was crucial, along with an actual knowledge of where to obtain the data.

Obtaining data from publicly accessible sources can be applied in a broader sense, and we can search for all publicly available information, and be more targeted, for instance to a company's website. Company websites contain some vital information that can be used to gain a competitive advantage, since the data can provide a knowledge of the advantages and weaknesses of competitors (Hu & Zhu, 2013). A review of websites, web applications, and competitors' network can reveal their vulnerabilities and possible sensitive (personal) data, which is made public (Sondrava et al., 2021). In the opinion of Hu and Zhu (2013), the following information is relevant for competitive intelligence: the popularity of the website, age of the domain, appearance in search engine results, number of single device visits (meaning a visit using a certain device, although the same device has visited a website multiple times), the number of visited pages, links to pages, response time and website ranking. The information obtained must be set in the right context and correctly interpreted for an organisation to derive value from it.

Just as we can obtain data on turnover from a website, using tools to obtain data from publicly accessible sources we can rapidly gain information on the vulnerability of a specific website or application. These vulnerabilities appear in the form of leaks of sensitive data, such as account access information, open ports on a network, unprotected web services, outmoded software and an operating system running in the background (Sondrava et al., 2021). Such data are useful for potential attackers or for organisations that search for this information in themselves in the case of a penetration test. Were such data to be used or exploited for the purpose of a competitive advantage, this would constitute a crime, regardless of the fact that the data were freely accessible.

Actual searching on websites can also be time-consuming, since a first search can yield a lot of hits that need to be looked at. Resolving the questionable quality of results and gaining higher quality searches using web browsers is also addressed by Rasekh (2015), who designed a new search system based on competitive intelligence activity with the implementation of a high-quality browser. The proposed system is a combination of an ICA algorithm and a system

of ranking based on links. The described system needs a few more adjustments for use on the internet.

In recent years the concept of big data has of course been a major topic, and researchers are aware that the use of such data can offer value. Di et al. (2014) have identified the importance of competitive intelligence in the increasingly digitalised world and highlight the vast quantities of data generated every day and available on the web for use in conducting in-depth analysis that can signify an extraordinary competitive advantage. Through effective analysis organisations can recognise trends and also dangers, and because of this information they possess, they can make higher quality decisions, or decisions that are better than those of competitors. A similar conclusion was drawn by Sharma et al. (2013), who take the view that older approaches (before the arrival of the big data age) have major deficiencies in obtaining data for the purpose of competitive. Organisations can now obtain information on a dynamic business environment and markets and analyse consumers' responses and opinions in various social networks, forums, and blogs. For the actual analysis of data they present a technical solution for structuring and visualisation of large quantities of unstructured data with a user interface for easier use. They define data analysis steps as follows: posing questions, gathering data, analysis of data, and proposed reactions to the findings.

The added value of competitive intelligence is also recognised by Wang et al. (2011), who take the view that competitive intelligence offer the necessary support for managing companies, along with strategic support. Their article presents a model for acquiring competencies to successfully implementing competitive intelligence, emphasising an organisational culture and other internal and external factors. They have found that competitive intelligence play an important part in the long-term development of a company, including the setting up and operation of various groups and departments within the organisation. A system can be effective if the organisation has set up good training mechanisms to maintain and develop a lasting competitive advantage.

Chi and Chen (2013) researched the area of collaborative competitive intelligence, where they have found that modern organisations, due to their complexity, often require cooperation among various departments, or rather inter-functional cooperation, as they call it. They designed a model for competitive intelligence based on a knowledge base system approach. The system is composed of domain ontology, task ontology and semantic rules. The aim of the system is to deliver to various departments in an organisation news relating to competitive intelligence, depending on the weighting or relevance of the news for the individual department. With a test sample of 512 news entries, the system carried out an average 78% level of recall and 85% accuracy in delivering news. The decision-making model had a correctness level of 99%, and with department weighting 96%. In general they assess the knowledge base system as successful, since it achieves the objective of steering news through the decision-making channels in a company.

3.3 Models for evaluating obtained data and tools

In using OSINT tools and techniques, the seriousness and quality of information can be problematic. It is no surprise that researchers started dealing with this area and designing models for evaluating obtained data and tools. Chae et al. (2019) developed a systemic approach to assessing the appropriateness of current and future tools for obtaining data from publicly accessible sources for military use. The model itself is not oriented towards competitive intelligence, but it is at least partly applicable in assessing the appropriateness of the tool (and consequently also the information obtained with these tools) in the commercial sector. In the qualitative model, which is part of the developed approach, in the assessment they touch upon the actual suitability of the tool in terms of military policy (disclosing data on users of the tool), system decision-making in the final results (quality of information is important), the time needed for training personnel and the limitations of the tool (e.g. necessary internet connection speed, possible false positive results and so on). All the main criteria are in the interest of every slightly larger organisation that has in its ranks a department for competitive intelligence activities.

It is harder to assess the validity of data from multiple sources than to assess tools for using data acquisition from publicly accessible sources. Dorton et al. (2019) developed an approach based on the principles of social sciences, and this enables the mass gathering of opinions and validation of certain information in a quantitative way, in other words a rapid quantitative definition of the validity of information or multiple pieces of information from several observers. Theoretical research is important for conducting qualitative research as well as for analysing information obtained by means of data acquisition from publicly accessible sources and for obtaining data from human sources (Human Intelligence or HUMINT). At this level there are several more limitations to the research. One limitation is that there needs to be empirical research that would confirm or reject the theoretical assertions. Checking assertions is based on axioms which people do not observe consistently, moreover it is assumed that each observer has the same credibility, which is not true in practice. The model also needs to be assessed in a larger group of observers (in the case of theoretical research there were 15 observers). It is also questionable that the model relies on the memory or capacity to recall of individuals, which can cause errors in the validity of the information, since people can remember an event mistakenly.

4 DISCUSSION AND CONCLUSION: WHAT DO WE KNOW AND WHAT NEEDS TO BE FURTHER RESEARCHED?

Using data acquisition from publicly accessible sources is a topical subject that has recently attracted considerable attention, especially in terms of modern technology. For the most part, research related to the use of tools for data acquisition from publicly accessible sources refers to information technology and digital information, which are freely available on the internet. More recent works on this subject no longer talk about classical approaches to obtaining information from people or from print media, although obtaining information

from people is still an important part of competitive intelligence, when we speak of decision-making over important matters. There are a few available tools for obtaining information from public sources, but the majority are problematic since they also capture irrelevant information, and consequently for the general public the acquisition of data from publicly accessible sources can be time-consuming and analytically demanding. For this reason, the majority of companies do not conduct competitive intelligence, or conduct them in a limited scope, since they lack, or else cannot afford, technical and analytical staff that could cover this area.

Researchers write about obtaining data from publicly accessible sources and competitive intelligence, but there has still not been any extensive empirical research in this field. In the review of the literature, we had to set the search parameters very broadly, in order to capture all relevant sources, since the industry uses a variety of expressions for similar approaches and fields. Researchers are not always in unison in their use of terminology, which probably lies in the fact that the field of data acquisition from publicly accessible sources is developing very rapidly, and consequently new sub-fields are emerging that attempt to define in greater detail or analyse the activity itself. It is possible to trace in the work of researchers an inclination towards and recognition of the importance of obtaining data from publicly accessible sources also in competitive intelligence, while at the same time they are unanimous that a great number of unanswered questions remain in relation to the immeasurable quantities of data and the necessary technical support for processing and analysing the data. One obvious obstacle is a lack of personnel, who are often inadequately trained to obtain data, or lack analytical abilities to correctly interpret the data obtained and deliver this to management in the form of useful information in support of decision-making processes.

We see numerous possibilities for further work, including greater empirical research in the field of using tools to obtain data from publicly accessible sources and to obtain data from publicly accessible sources for the purpose of competitive intelligence. Research would need to be conducted in organisational environments, involving work on real (decision-making) cases, where the real value of such use could be measured. One possibility is working on the design of an approach model for conducting competitive intelligence using data acquisition from publicly accessible sources, which would serve as a framework in the business environment and whose implementation would offer added value. It would be designed in such a way that in addition to an organisational approach, it would resolve the issue of training for employees and those conducting data acquisition from publicly accessible sources for clients.

The systematic literature review has shown that in the area of obtaining data from publicly accessible sources and competitive intelligence, there is still a lot of room for development, since the distance between where we are and where we would like to be is huge. The path to effective use of obtaining data from publicly accessible sources in organisational environments still faces some obstacles, which can be removed in the coming years, but of course the entire process must have proper IT support and must enable both organisational and technical implementation in various commercial environments.

REFERENCES

- Anand, A., Buvanasi, A. K., Meenakshi, R., Karthika, S., & Mohan, A. K. (2020). PeopleXploit- A hybrid tool to collect public data. In *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*. IEEE. <https://doi.org/10.1109/ICCCSP49186.2020.9315266>
- Al-khateeb, S., & Agarwal, N. (2020). Social cyber forensics: Leveraging open source information and social network analysis to advance cyber security informatics. *Journal of Computational and Mathematical Organization Theory*, 23, 412–430. <https://doi.org/10.1007/s10588-019-09296-3>
- Ansari, F., Akhlaq, M., & Rauf, A. (2013). Social networks and web security: Implications on open source intelligence. In *2013 2nd National Conference on Information Assurance (NCIA)*, (pp. 79–82). IEEE. <https://doi.org/10.1109/NCIA.2013.6725328>
- Benes, L. (2013). OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm. *Journal of Strategic Security*, 6(3), 22–37. <http://dx.doi.org/10.5038/1944-0472.6.3S.3>
- Bernard, R., Bowsher, G., Milner, C., Boyle, P., Patel, P., & Sullivan, R. (2018). Intelligence and global health: Assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. *Journal of Public Health*, 26, 509–514. <https://doi.org/10.1007/s10389-018-0899-3>
- Best, C. (2011). Challenges in open source intelligence. In *2011 European Intelligence and Security Informatics Conference*, 58–62. IEEE. <https://doi.org/10.1109/EISIC.2011.41>
- Buccafurri, F., De Angelis, V., & Idone, M. F. (2020). Implementing multiple-social-network meta-APIs to support OSINT programming. In *2020 12th International Conference on Advanced Infocomm Technology (ICAIT)*, (pp. 124–128). IEEE. <https://doi.org/10.1109/ICAIT51223.2020.9315457>
- Černýa, J., Potančoka, M., & Molnára, Z. (2019) Using open data and Google search data for competitive intelligence analysis. *Journal of Intelligence Studies in Business*, 9(2), 72–81. <https://doi.org/10.37380/jisib.v9i2.470>
- Chae, J., Graham, D., Henderson, A., Matthews, M., Orcutt, J., & Song, S. (2019). A system approach for evaluating current and emerging army open-source intelligence tools. In *2019 IEEE International Systems Conference*, (pp. 1–5). IEEE. <https://doi.org/10.1109/SYSCON.2019.8836885>
- Chi, Y. L., & Chen, T. T. (2013). Collaborative competitive intelligence: A knowledge base system approach. In *2013 8th Iberian Conference on Information Systems and Technologies (CISTI)*, (pp. 1–4). IEEE. <https://ieeexplore.ieee.org/document/6615735>
- Di, J., He, B., & Li, W. (2014). Research on enterprise competitive intelligence development and strategies in the big data era. In *2014 IEEE International Conference on Computer and Information Technology*, (pp. 658–663). IEEE. <https://doi.org/10.1109/CIT.2014.119>
- Dolenc, S. (2014). Kaj je Big Data? Kvarkadabra. <https://kvarkadabra.net/2014/09/kaj-je-big-data/>
- Goujon, B. (2011). Text mining for opinion target detection. In *2011 European Intelligence and Security Informatics Conference*, (pp. 322–326). IEEE. <https://doi.org/10.1109/EISIC.2011.41>

[org/10.1109/EISIC.2011.45](https://doi.org/10.1109/EISIC.2011.45)

- Dorton, S. L., Frommer, I. D., & Garrison, T. M. (2019). A theoretical model for assessing information validity from multiple observers. In *2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, (pp. 52–58). IEEE. <https://doi.org/10.1109/COGSIMA.2019.8724242>
- Gonçalves Evangelista, J. R., Sassi, R. J., Romero, M., & Napolitano, D. (2020). Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. *Journal of Applied Security Research*, 16(3), 345–369. <https://doi.org/10.1080/19361610.2020.1761737>
- Hribar, G., Podbregar, I., & Ivanuša, T. (2014). OSINT: A »Grey Zone«? *International Journal of Intelligence and Counter Intelligence*, 27(3), 529–549. <https://doi.org/10.1080/08850607.2014.900295>
- Hu, L., & Zhu, M. (2013). Competitive intelligence acquisition from websites. In *2013 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, (pp. 858–862). <https://doi.org/10.1109/FSKD.2013.6816314>
- Li, D., Zhou, X., & Xue, A. (2020). Open source threat intelligence discovery based on topic detection. In *2020 29th International Conference on Computer Communications and Networks*, (pp. 1–4). IEEE. <https://doi.org/10.1109/ICCCN49398.2020.9209602>
- Madureira, L., Popovič, A., & Castelli, M. (2021). Competitive intelligence: A unified view and modular definition. *Technological Forecasting and Social Change*, 173, 121086. <https://doi.org/10.1016/j.techfore.2021.121086>
- Microsoft. (2019). Načrtovanje varne prihodnosti za podjetja [Planning a secure future for your company]. <https://www.microsoft.com/sl-si/microsoft-365/business-insights-ideas/resources/planning-a-secure-future-for-your-company>
- Pais, V. F., & Ciobanu, D. S. (2014). OSINT for B2B platforms. In *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, (p.p. 720–723). IEEE. <https://doi.org/10.1109/ASONAM.2014.6921665>
- Pastor-Galindo, J., Nespoli, P., Gomez-Marmol, F., & Martinez Perez, G. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trend. *IEEE Access*, 8, 10282–10304. <https://doi.org/10.1109/ACCESS.2020.2965257>
- Rai, B. K., Verma, R., & Tiwari, S. (2021). Using open source intelligence as a tool for reliable web searching. *Journal of Computer Science*, 2(402). <https://doi.org/10.1007/s42979-021-00777-4>
- Ranjan, J., & Foropon, C. (2020). Big data analytics in building the competitive intelligence of organisations. *International Journal of Information Management*, 56. <https://doi.org/10.1016/j.ijinfomgt.2020.102231>
- Rasekh, I. (2015). A new competitive intelligence-based strategy for web page search. In *2015 Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015)*, (pp. 120–126). IEEE. <https://doi.org/10.1109/ICOSC.2015.7050789>
- Schaurer, F., & Störger, J. (2013). The evolution of open source intelligence (OSINT). *Journal of U.S. Intelligence Studies*, 19(3), 53–56. https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013

[pdf](#)

- Semerikova, L. N., Zaretskiy, A. P., Divnenko, Z. A., Grosheva, E. S., & Vishnevskaya, G. V. (2017). Application of information technologies in competitive intelligence. In *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*, (pp. 804–807). IEEE. <https://doi.org/10.1109/SCM.2017.7970730>
- Sharma, D., Chaudhary, K., Vaidya, P., & Jora, K. (2013). Big data – competitive intelligence. In *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 684–689). IEEE. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7100336>
- Sondrava, S., Sharma, P., & Dholariya, D. (2021). Prevention to sensitive information disclosure via OSINT. *International Journal of Scientific Research in Science, Engineering and Technology*, 8(3), 109–114. <https://doi.org/10.32628/IJSRSET218317>
- Wang, Y., Zhao, X., & Zhang, X. (2011). Construction and operation of cultivation model for enterprise competitive intelligence competence. In *International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, (pp. 2004–2007). IEEE. <https://doi.org/10.1109/AIMSEC.2011.6010955>
- Yaboah-Ofori, A., & Brimicome, A. (2017). Cyber intelligence & OSINT: Developing mitigation techniques against cybercrime threats on social media. *International Journal of Cyber-Security and Digital Forensics*, 7(1), 87–98. <http://dx.doi.org/10.17781/P002378>
- Yang, H. C., & Lee, C. H. (2012). Mining open source text documents for intelligence gathering. In *2012 International Symposium on Information Technologies in Medicine and Education*, (pp. 969–973). <https://doi.org/10.1109/ITIME.2012.6291464>

About the author:

Žiga Primc holds a bachelor's degree in information security and a master's degree in criminal justice from the Faculty of Criminal Justice and Security, University of Maribor. He is a private detective, licensed as an ethical hacker. E-mail: ziga.primc@student.um.si



Anica Ferlin

Criminal liability and prosecution of Islamic State fighters in Iraq

Branko Gabrovec, Tilen Zupan, Srečko Felix Krope, Branko Lobnikar

Police Instruments of Restraint against Persons with Health Problems –
Analysis of the Use of Expert Grips and Holds as Forms of Physical Force

Miha Dvojmoč, Patricija Lunežnik, Kaja Prislan

Adoption of Advanced Technological Solutions in Slovenian Private Security
Companies

Žiga Primec

The Use of Tools for Obtaining Data From Publicly Accessible Sources for
the Purpose of Competitive Intelligence in Enterprises