Editorial

This issue of the Journal of Criminal Justice and Security contains six quite diverse scientific analyses of content important for the field of criminal justice. In-depth studies in the areas of private security and security studies, criminology, criminal investigation, information security and police activities are presented.

László Christián and **Andrej Sotlar** in the first paper *Private Security Regulation in Hungary and Slovenia – A Comparative Study Based on Legislation and Societal Foundations* compare how private security is regulated in Hungary and Slovenia using Button-Stiernstedt's evaluation model, which includes legislation and societal criteria. Slovenian private security regulation received 94 points, making it equal to Belgium in first place among 27 EU countries, while Hungary received 74 points that would rank it seventh, with the same number of points as Ireland. When discussing use of Button-Stiernstedt's evaluation model, the authors suggest that in the future certain criteria should be more flexibly applied.

Jaroš Britovšek in the paper *Comparing Counterintelligence and Counterterrorism – Similarities, Issues and Solutions* discusses and compares counterintelligence and counterterrorism, particularly following the Cold War and the rise of new forms of non-state terrorism. The author critically examines the tendency of Western liberal democracies to assign counterterrorism tasks to services traditionally involved in counterintelligence. Counterintelligence and counterterrorism seem very similar at first glance, but differ substantially when dealing with risks, time sensitivity and the sharing of information. In the paper, several solutions for policymakers are presented that derive from the principle of the separation of counterintelligence and counterterrorism, while also calling for the establishment of sharing and coordination bodies.

Monika Klun and **Matevž Bren** in the third paper *Male Sex Work in Slovenia* analyse the nature of male sex work in Slovenia. The study results suggest that male sex workers in Slovenia generally define themselves as homosexuals or bisexuals. Among male sex workers and men who do not engage in this type of activity, there are no significant differences in their socialisation process.

Saša Kuhar contributed the paper *Art crime and preventive measures for museums, churches and sacred objects.* In her study, she presents art crime and preventive measures that reduce crime involving art in museums, churches and sacred objects in Slovenia. Art thefts from private premises, galleries, churches and sacred objects prevail, but thefts from museums remain the art crime most covered by the media. The author concludes that the greatest difficulty is the concealed true level of crime involving art because many cases go unreported, especially when they happen in museums. A combination of security measures is urgently needed, namely, physical and technical protection as well as forensic marking.

Smart cars and information security, a topical paper by **Gašper Školc** and **Blaž Markelj**, covers the issue of users' data security in smart cars. The paper provides an insight into the level of general knowledge regarding such issues among those who drive smart cars. The study results show that the use of mobile devices and their various applications that connect to a smart car represent one of the biggest risks to information security in smart cars. While drivers are aware of these risks, many consider them not to be so important.

In the last paper, **Srečko Felix Krope** and **Vladimir Ilić** present the results of the study *Assaults on Police Officers in Slovenia between 2007 and 2017.* The highest number of assaults on police officers was reported from 2009 to 2013, with a steady decline being registered since 2013. The study results can help predict the trend of assaults on police officers and identify ways to increase the safety of police officers and persons during police procedures.

We hope you find all of these articles interesting and a good source of new ideas. Since we intend to publish one more issue of the journal in the English language by the end of the year, we warmly invite scholars to submit papers on the results of their studies.

Assoc. Prof. Branko Lobnikar, PhD
Editor of English Issues

Uvodnik

V tokratni številki revije Varstvoslovje v angleškem jeziku objavljamo šest raznolikih prispevkov, ki vsi po vrsti naslavljajo pomembna varstvoslovna vprašanja. Tako smo v objavo sprejeli študije s področja zasebnega varovanja, varnostnih ved, kriminalistike, kriminologije, policijske dejavnosti in informacijske varnosti.

László Christián in **Andrej Sotlar** v prispevku z naslovom *Ureditev zasebnega varovanja na Madžarskem in v Sloveniji – primerjalna študija na podlagi zakonodaje in societalnih dejavnikov* primerjata ureditev zasebnega varovanja na Madžarskem in v Sloveniji z uporabo Button-Stiernstedtovega modela evalvacije, ki temelji na zakonodaji in societalnih dejavnikih. Slovenska ureditev zasebnega varovanja je z uporabo tega merskega inštumenta prejela 94 točk, kar jo postavlja ob bok Belgiji na prvem mestu med 27 državami EU. Madžarska je prejela 74 točk in bi se uvrstila na sedmo mesto, z enakim številom točk kot Irska. Avtorja ugotavljata, da je Button-Stiernstedtov model evalvacije ureditve zasebnega varovanja večinoma uporaben za mednarodne primerjave, v prispevku pa predlagata, da bi se v prihodnosti nekateri kriteriji uporabili bolj fleksibilno.

Jaroš Britovšek je v študiji *Primerjava protiobveščevalne in protiteroristične dejavnosti – podobnosti, dileme in rešitve* primerjal protiobveščevalne in protiteroristične dejavnosti, še posebej z vidika konca hladne vojne in pojava novih oblik terorizma. Avtor v prispevku kritično obravnava nagnjenja zahodnih liberalnih demokracij, ki vlogo protiteroristične dejavnosti potiskajo v institucije, ki so bile tradicionalno zadolžene za protiobveščevalno dejavnost. Protiobveščevalna in protiteroristična dejavnost se zdita na prvi pogled podobni, vendar obstajajo med njima pomembne razlike, neupoštevanje teh razlik pa ima lahko pomembne posledice za nacionalno varnost, ugotavlja avtor.

Monika Klun in **Matevž Bren** v svojem prispevku analizirata *Moško spolno delo v Sloveniji*. Cilj njune študije je bilo ugotoviti, ali moško spolno delo v Sloveniji obstaja, ali obstajajo statistično pomembne razlike v spolni usmerjenosti med moškimi spolnimi delavci v Sloveniji in moškimi, ki se s tovrstnimi aktivnostmi ne ukvarjajo, ter ali obstajajo dejavniki tveganja, ki ločujejo med preučevanima skupinama. Avtorja ugotavljata, da se moški spolni delavci po večini opredeljujejo kot homoseksualci ali biseksualci. Med moškimi spolnimi delavci in moškimi, ki se s tem ne ukvarjajo, pa ni bistvenih razlik v socializacijskem procesu.

Saša Kuhar v prispevku *Preventivni ukrepi na področju kriminalitete zoper umetnine v muzejih, cerkvah in sakralnih objektih* predstavlja kriminaliteto zoper umetnine in preventivne ukrepe, ki pripomorejo k zmanjševanju kaznivih dejanj zoper umetnine v muzejih, cerkvah in sakralnih objektih v Sloveniji. V študiji ugotavlja, da v Sloveniji prevladujejo tatvine umetnin iz zasebnih objektov, galerij, cerkva in sakralnih objektov, medijsko pa so najbolj izpostavljeni primeri tatvin iz muzejev. Avtorica opozori na dejstvo, da je varovanje umetnin v muzejih, cerkvah in sakralnih objektih zelo zahtevna naloga, saj je potrebno umetnine hraniti varno, hkrati pa morajo biti dostopne obiskovalcem. Zato je nujna kombinacija raznolikih varnostnih ukrepov, od fizičnega in tehničnega varovanja do forenzičnega označevanja. Vse to pa je treba nadgraditi z ozaveščanjem javnosti o pomenu umetnin za družbo.

Gašper Školc in **Blaž Markelj** predstavljata zelo aktualno študijo *Pametni avtomobili in informacijska varnost*. Pametni avtomobili danes za svoje delovanje namreč veliko bolj kot v preteklosti uporabljajo raznovrstne podatke, ki jih pridobivajo iz okolice s pomočjo senzorske tehnologije in ostalih dostopnih virov. Vozniki pametnih avtomobilov pa prenašajo raznovrstne podatke, ko svoje mobilne naprave povezujejo s sistemi pametnih avtomobilov, na primer z uporabo različnih aplikacij. Avtorja ravno slednje prepoznavata kot eno največjih tveganj informacijski varnosti pri rabi pametnih avtomobilov.

V zadnjem prispevku *Napadi na policiste v Sloveniji v obdobju 2007–2017* **Srečko Felix Krope** in **Vladimir Ilić** analizirata trend napadov na policiste v obdobju 2007–2017 na podlagi letnih poročil Generalne policijske uprave. Največ napadov na policiste je bilo v obdobju 2009–2013 in šele po tem letu gre za dejanski stalen padec. Izstopajoč podatek je tudi število poškodovanih policistov, zlasti v letih 2011 in 2012, kar avtorja pripisujeta množičnim demonstracijam v tistem obdobju.

V uredništvu upamo, da bodo prispevki za bralce zanimivi in poučni. Hkrati pa vse pisce vabimo k oddaji rezultatov svojih študij v recenzijski postopek, saj bomo do konca letošnjega leta pripravili še eno številko revije Varstvoslovje v angleškem jeziku.

Izr. prof. dr. Branko Lobnikar
Urednik številk v angleškem jeziku

VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 20
no. 2
pp. 143–162

Private Security Regulation in Hungary and Slovenia – A Comparative Study Based on Legislation and Societal Foundations

László Christián, Andrej Sotlar

Purpose:

The purpose of the article is to conduct a comparative study of private security regulation in Hungary and Slovenia using Button-Stiernstedt's evaluation model based on legislation and societal foundations and to find out where the two countries are in comparison with other EU member states.

Design/Methods/Approach:

First, the main characteristics of private security in Hungary and Slovenia are analysed and presented through a literature and legislation review. Second, Button-Stiernstedt's evaluation model using legislation and societal criteria is studied and explained. Third, this evaluation model is used to evaluate private security in both countries and, fourth, Hungarian and Slovenian private security regulations are ranked on a regulatory system scale of 27 EU member states.

Findings:

In this re-evaluation, Slovenian private security regulation received 94 points which makes it equal to Belgium that holds first place among 27 EU countries. Hungary received 74 points, ranking it seventh with the same number of points as Ireland. Although Hungary seems to score relatively highly in the survey, this does not mean the situation in practice is positive. Button-Stiernstedt's private security regulation evaluation model is mostly useful for international comparisons. However, we suggest that in the future some criteria be used more flexibly than the authors proposed in 2016.

Research Limitations:

Limitations of the research arise from the fact that the presented evaluation model of private security regulation is not yet fully developed and that not all data on private security in both countries were available.

Practical Implications:

The findings are useful for both further harmonising private security regulation within the EU and improving the presented evaluation model to make international comparisons more precise.

Originality/Value:

Hungarian private security regulation is evaluated for the first time using Button-Stiernstedt's evaluation model.

UDC: 351.746.2(439)(497.4)

Keywords: private security, regulation, legislation, societal foundations, Hungary, Slovenia

Ureditev zasebnega varovanja na Madžarskem in v Sloveniji – primerjalna študija na podlagi zakonodaje in societalnih dejavnikov

Namen prispevka:

Namen članka je s primerjalno študijo ureditve zasebnega varovanja na Madžarskem in v Sloveniji z uporabo Button-Stiernstedtovega modela evalvacije, ki temelji na zakonodaji in societalnih dejavnikih, ugotoviti, kje se državi nahajata v primerjavi z drugimi članicami EU.

Metode:

Na osnovi pregleda literature in zakonodaje so bile analizirane in predstavljene glavne značilnosti zasebnega varovanja na Madžarskem in v Sloveniji, zatem pa je bil pojasnjen Button-Stiernstedtov evalvacijski model, ki temelji na zakonodaji in societalnih dejavnikih. Evalvacijski model je bil uporabljen za vrednotenje ureditve zasebnega varovanja v obeh državah. Ureditvi sta bili nato umeščeni na lestvico regulatornih sistemov 27 držav članic EU.

Ugotovitve:

Slovenska ureditev zasebnega varovanja je v tej ponovni oceni prejela 94 točk, kar jo postavlja ob bok Belgiji na prvem mestu med 27 državami EU. Madžarska je prejela 74 točk in bi se uvrstila na sedmo mesto, z enakim številom točk kot Irska. Čeprav se zdi, da se je Madžarska v raziskavi uvrstila razmeroma visoko, to ne pomeni, da razmere v praksi odražajo to pozitivno podobo. Button-Stiernstedtov model evalvacije ureditve zasebnega varovanja je večinoma uporaben za mednarodne primerjave, vendar predlagamo, da se v prihodnosti nekateri kriteriji uporabijo bolj fleksibilno, kot pa sta avtorja predlagala leta 2016.

Omejitve raziskave:

Omejitve raziskave izhajajo iz dejstva, da predstavljeni model evalvacije ureditve zasebnega varovanja še ni povsem dodelan in da niso bili na voljo vsi podatki o zasebnem varovanju v obravnavanih državah.

Praktična uporabnost:

Ugotovitve so koristne tako z vidika nadaljnje harmonizacije regulacije zasebnega varovanja v EU kot z vidika izboljšanja predstavljenega modela evalvacije, ki omogoča natančnejše mednarodne primerjave.

Izvirnost/pomembnost prispevka:

Madžarska ureditev zasebnega varovanja je bila prvič ovrednotena z Button-Stiernstedtovim modelom evalvacije.

UDK: 351.746.2(439)(497.4)

Ključne besede: zasebno varovanje, regulacija, zakonodaja, societalni dejavniki, Madžarska, Slovenija

1 INTRODUCTION

Private security is an activity or service not provided by state or local public authorities but by private economic entities – private security firms and individuals. They offer and provide security on a demand/supply basis and as such are first and foremost aimed at business success. However, their success in terms of profit cannot be achieved without being good at providing security to either private clients or the state. As such, private security is an important addition security mechanism in society and, together with other public and private policing/ security organisations, forms part of contemporary plural policing family (Jones & Newburn, 2006).

Despite not being researched as much as its 'older brother' (the police), private security is attracting ever more academic attention. There have been many country and international comparative studies on private security in the last 25 years. A lot has been done so far to enable a better understanding of the following phenomena related to private security:

- the nature, functions and goals of the private security industry (for example Johnston, 1992; Meško, Nalla, & Sotlar, 2004; Nalla & Heraux, 2003; Nalla & Hwang, 2004; Nalla & Newman, 1990; Nalla, Meško, Sotlar, & Johnson, 2006);
- the source of the legitimacy of private security (for example Nalla & Meško, 2015; Sotlar, 2007);
- the relationship between police and private security officers (for example Nalla & Hummer, 1999a, 1999b; Nalla, Johnson, & Meško, 2009; Sotlar & Meško, 2009);
- citizens' perceptions of and satisfaction with private security officers (for example Moreira, Cardoso, & Nalla, 2015; Nalla & Lim, 2003; Nalla, Gurinskaya, & Rafailova, 2017; Nalla, Ommi, & Murthy, 2013; Van Steden & Nalla, 2010) etc.

However, despite being quite a developed industry, private security is far from being equally understood, treated and especially regulated in EU countries. It is thus no surprise that international comparative studies on private security regulation are relatively rare and lack a common methodology. The best known studies in this regard are those dealing with the regulation and growth of private security in European Union countries (for instance Button, 2007; Button, 2012; Button & Stiernstedt, 2016; De Ward, 1993, 1999; De Ward & Van De Hook, 1991; Van Steden & Sarre, 2007) or in broader Europe (CoESS, 2011, 2013; ECORYS, 2011; Gerasimoski & Sotlar, 2013; United Nations Office on Drugs and Crime, 2014; Van Steden, & Sarre, 2010).

Hungary and Slovenia share one very important characteristic concerning private security. They are both former socialist countries where private economic initiatives started developing upon the decline of socialism less than three decades ago. The 'rebirth' of private property also saw the birth of private security (Johnston, 1992; Meško et al., 2004). After almost 30 years of the development and regulation of private security in these two EU member states, it is interesting to see what level of development in the role, growth and especially regulation of the field of private security has so far been achieved. As mentioned, there are always questions of how to fairly compare, evaluate and assess different countries' regulations without having a single comprehensive methodology. For the purposes of this article, we use quite a new evaluation model based on legislation and societal foundations prepared by Mark Button and Peter Stiernstedt. The model was first presented in their article "Comparing private security regulation in the European Union" (Button & Stiernstedt, 2016). The model will also be described in this article since, in our opinion, it represents the most comprehensive attempt to evaluate private security regulation in the EU thus far. Thus, we have decided to call it "Button-Stiernstedt's evaluation model". While Slovenia was already evaluated along with other EU countries, unfortunately this is not the case with Hungary. Namely, Hungary was (together with Croatia, another EU member state) excluded from the final analysis and report »due to insufficient data« (Button & Stiernstedt, 2016, p. 8).

The purpose of the article is therefore to comparatively study private security regulation in Hungary and Slovenia using Button-Stiernstedt's evaluation model based on legislation and societal foundations and to establish where the two countries are, not only in relation to each other, but primarily in comparison with other EU member states. In addition, the evaluation of Slovenian private security regulation from 2016 will be challenged, along with the evaluation model itself.

2 THE MAIN CHARACTERISTICS OF PRIVATE SECURITY IN HUNGARY AND SLOVENIA

2.1 Private Security in Hungary

Public safety is a collective and cooperative product of society, and consists of the activities of individuals and communities, state organisations' official measures, citizens' capability to protect themselves, and services of the entrepreneur market (Finszter, 2001). Law enforcement is the broadest term in this area with maintenance of the public order being just one important segment of it. The relevant actors in Hungary are namely the public-order bodies (Police, Disaster Management, Civil National Security Service, Prison Service), organisations tasked with ensuring public order (Parliament Guard, National Tax and Customs Administration) and, finally, complementary law enforcement organisations (local government law enforcement (a state actor), civil volunteer security organisations, private security) (Christián, 2015, 2016, 2017). Private security is further explained below.

After the change in political regime in Hungary in 1989, state security entities were partially disbanded, thereby creating a security void. At the same time, as part of the transition to a free market economy opportunities for the security market were opened, with western private security providers expanding to ex-Soviet bloc countries. The early 1990s may also be called the period of 'low hanging fruit'. Many companies and actors entered the private security field without any genuine professional preparations. In this period, there was no legislation to regulate this branch of the economy. That allowed the sector to grow in the quantity but not in the quality of the service.

Prior to 1998, there was no law specifically governing the private security industry, except for government regulation 87/1995. The first rules on private security were introduced in the Law on the Police XXXIV of 1994 concerning the main requirements of the service and supervision of related activity. The earliest legislation as a separate law came in 1998: Law IV of 1998. The following Law CXXXIII of 2005 provides the current regulation that is effective today. Two other regulations connected to this activity are effective today, the first is Law CLIX of 1997 on armed security guards and the second is Law CXX of 2012 on special law enforcement personnel (Christián, 2014).

A few relevant figures concerning the Hungarian private security sector are worth considering. In June 2017, around 5,260 companies were dealing with private security (see Table 1).

Table 1: Number of private security company licences in Hungary (2010–2017)

Year	Licences issued	Licences cancelled	Valid licences
2010	1,851	1,258	13,064
2011	3,345	1,615	12,907
2012	1,941	446	9,205
2013	1,119	242	8,311
2014	1,103	1,292	7,330
2015	1,086	829	6,637
2016	1,693	718	5,452
2017 (June)	817	242	5,260

Source: Data obtained directly from the deputy chief of the Hungarian police.

There are nearly 100,000 certified security guards and, as shown in Table 2, the number of private security personnel dropped significantly between 2010 and 2017.

Table 2: Number of private security guard certificates issued (2010–2017)

Year	Certificates issued	Certificates cancelled	Valid certificates
2010	16,429	10,933	133,360
2011	36,570	10,994	141,698
2012	35,030	994	122,151
2013	20,125	521	127,338
2014	16,526	436	122,754
2015	11,530	453	118,495
2016	26,616	373	104,187
2017 (June)	12,374	121	98,261

Source: Data obtained directly from the deputy chief of the Hungarian police.

The minimum employment requirements to become a security guard are:

- to be older than 18 years;
- no criminal record;

- legal residence in the country; and
- passing a state-mandated examination.

To obtain a security guard certificate, one must complete a 320-hour course which is provided by training companies in the market. In reality, the courses are usually shorter and of questionable quality. Private security personnel hold no state authority whatsoever, but may facilitate the arrest of citizens and act on behalf of their clients (exercising their rights to property, legal self-defence etc.). Most procedures fall into the legal category of defence of property. A security guard is authorised to use force, but items legally categorised as weapons are restricted (no teasers, firearms, batons, no tear gas above 40 mg/unit).

Compared to other countries, the figures concerning Hungarian private security are outstandingly high, some of the highest in the EU. Despite that, Hungarian citizens are hardly aware of the area and there is also a paucity of scientific research on it. Undoubtedly, the private security sector is quite an important and relevant part of the economy. Private security is taking over more and more responsibilities from the state, also providing public security. One can clear distinguish these agents in terms of their authorisation (empowerment). While private security focuses on prevention, public law enforcement agents have a strong focus on reaction. In fact, citizens are hardly aware of the field and tend to hold quite negative opinions of private security guards due to their poor qualification and low pay. A recent research study concluded that before the turn of the millennium these agents considered each another as rivals. However, it is now evident that optimal security is only attainable if these agents actually cooperate as partners (Sotlar & Meško 2009).

The Hungarian Chamber of Bodyguards, Property Protection and Private Detectives is supposed to play an important role in private security as a professional representative organisation. Yet, since mandatory membership in the chamber was abolished (1 January 2012), membership in the Chamber plummeted by approximately 80%–90%. In such circumstances, the Chamber lost its financial backing and thus no longer holds any real power to represent the interests of the private security sector. The organisation has a dual-level structure, including a national council with a Chief Board and regional county associations. The Chamber's remaining duties are to ensure members follow an ethical procedure and to investigate complaints concerning private security activities (Christián, 2014).

The supervision of private security activity is a responsibility of the state police and refers to the issuing of private security guard/private detective certificates and private company licences, the official registration of private security guards and licensed companies, and the control of all these activities. The police may levy a fine, cancel a certificate or a licence in the event of violations. Practically speaking, due to the limited human resources, supervision is mainly confined to administrative rather than professional control.

It has become a global tendency in recent years for the role of private security actors to be increasing within the law enforcement system. The main reason for this is that they offer both specialised and comprehensive services at an equal professional level. Meanwhile, despite its growing importance, private security is relatively poorly treated in Hungary, with a number of anomalies making its lawful and effective operation almost impossible. The legislation regarding close protection, safeguarding, as well as private investigation suffers considerable drawbacks, rendering it difficult for those in the trade to fulfil their duty especially since mandatory membership in their professional chamber was abolished in 2012. So far, professional, theoretical and scientific foundations for the area have been missing, a deficiency the Department for Private Security and Local Governmental Law Enforcement at the National University of Public Services intends to ameliorate.

2.2 Private Security in Slovenia

The first modern private security firms in Slovenia were established in 1989. Prior to that, all activities in the private security sector were carried out by security firms based on 'social ownership' common to the socialist political and economic system of former Yugoslavia (Meško et al., 2004). In 1994, the Law on Private Security and on the Mandatory Organisation of Security Services was adopted. The law defined physical and technical security for the first time in Slovenia. It also introduced licences for private security and the Chamber of the Republic of Slovenia for Private Security (CRSPS) in which membership was compulsory for all private security firms. The CRSPS was responsible for granting licences. Over the next ten years, the private security industry grew significantly. A new Private Security Law was passed in 2003. The traditional division into physical and technical security was replaced by six forms (licences) of private security activities, while mandatory training of private security personnel before commencing employment in security firms and certain new job positions were also introduced. A special body within the Ministry of the Interior – the Inspectorate for Interior Affairs of the Republic of Slovenia – and the Police (to some extent) became responsible for oversight of private security firms with respect to the legality of their activities, whereas professional supervision of firms was left to the CRSPS. The Ministry of the Interior (MI) was tasked with granting, revising and revoking licences for performing private security activities (Sotlar, 2010). In 2007, amendments to the Private Security Act did away with mandatory membership of the CRSPS. The Chamber had to change its name and organisation and now works under the name of the Chamber for the Development of Slovenian Private Security. Since no other chamber or association was founded, in 2011 the Ministry of the Interior proclaimed the chamber a representative professional association with certain administrative responsibilities in the private security field (Sotlar & Čas, 2011).

Private security regulation in Slovenia is today characterised by a new Private Security Act (Zakon o zasebnem varovanju [ZZasV-1], 2011). Sotlar and Čas (2011) describe the main characteristics of the new regulation as follows:

- the powers and responsibilities of the Ministry of the Interior in the field of private security keep growing;
- there is too much regulation of the field of private security, which is an economic activity;

- the Chamber for the Development of Slovenian Private Security is gaining back some powers even though membership in it is not compulsory;
- the number of measures/powers and means of private security officers has increased;
- the conditions for the use of particular measures/powers have broadened;
- basic and advanced security personnel training is given special attention; and
- in-house security is introduced.

Since 2011, eight different licences (forms) of private security have been available. A private security firm can apply for one or more licence if it meets the conditions and standards prescribed by law. In February 2018, there were 142 registered private security firms which together held 427 licences (see Table 3).

Table 3: Private security licences in Slovenia

Licences	No. of issued licences	No. of private security firms
Protection of people and property	91	
Protection of persons	26	
Transportation and protection of currency and other valuables	42	
Security of public gatherings	71	
Security at events in catering establishments	53	
Operation of a security control centre	15	
Design of technical security systems	35	
Implementation of technical security systems	94	
Total	**427**	**142**

Source: Ministrstvo za notranje zadeve (2018)

The Private Security Act (ZZasV-1, 2011) defines jobs in the field of private security which are also licensed. Security personnel is a common name that covers security watchmen, security guards, security supervisors, security control centre operators, security bodyguards, security managers, security technicians and authorised security system engineers. The law prescribes for all these categories basic (for example, 102 hours for a security guard) and advanced training as well as an examination. Without having trained security personnel who hold official identity cards private security firms are unable to apply for particular licences. No official data are available but some estimations indicate there are already around 6,500 private security personnel in Slovenia, meaning that private security is gradually numerical catching up with the police and its some 7,170 uniformed and criminal police officers (Police, 2018). The ratio between the number of private security officers and police officers is 0.91:1 (see Table 4).

The Private Security Act (ZZasV-1, 2011) provides relatively extensive powers (in Slovenia defined as "measures") that a security guard can use "when performing tasks of private security, in case of a threat to life, personal safety or property or when order or public order are breached" (Article 45). Security guards may issue warnings, make verbal orders, ascertain identity, conduct superficial searches, prevent entry to or leaving from a protected area, detain a person, use physical force, and apply handcuffs or other means of restraint. They may also use other measures if so specified by the law governing a particular field (e.g. the protection of airports, casinos or nuclear facilities) as well as technical security systems in line with the relevant legislation. Security guards (except security watchmen) may carry and use firearms (handguns), incapacitating spray[1] and a service dog.[2]

It seems the biggest problems concerning private security in Slovenia do not relate to the legislation but to factors in society like the salaries and working conditions of private security personnel. Their salaries remain far below the average salary in Slovenia (see Table 2), but it is promising that a collective labour agreement for private security was finally signed in 2016, bringing some improvements in this regard.

2.3 Comparison of the Main Characteristics of Private Security in Hungary and Slovenia

In order to ensure an easier comparison of Hungarian and Slovenian private security, we systematised the most important characteristics, thus making the similarities and differences more evident. Data from Table 4 will be analysed and furtherly discussed in section 4.

Table 4: Comparison of the main characteristics of private security in Hungary and Slovenia

Characteristics	*Hungary*	*Slovenia*
Population	9,797,561 (2017)	2,065,890 (2018)
Gross Domestic Product (GDP)	EUR 113,723 million (2016)	EUR 40,418 million (2018)
GDP per capita	EUR 11,300 (2016)	EUR 19,576 (2018)
Ratio police force/ population	1/245	1/288
Ratio private security force/population	1/100	1/317
Ratio private security force/police force	2.46/1	0.91/1
Licensing for private security companies	Mandatory by law	Mandatory by law
Total no. of private security companies	5,260 (2017)	142 (2018)
Total no. of private security officers	98,261 (2017)	6,500 (est.) (2018)
Maximum no. of working hours in the private security industry (under national legislation)	8 hours/day 40 hours/week Overtime: 240 hours/year	8 hours/day 40 hours/week Overtime: 240 hours/year

[1] *A security guard can only use an incapacitating spray if there is no other way of preventing an immediate illegal assault on the security guard.*

[2] *A security guard may use a specially trained service dog and use its sense of smell or sight to determine the presence of a person or substance. The dog must be muzzled, on a leash and under the direct control of the security guard.*

Table 4: Continuation

Characteristics	*Hungary*	*Slovenia*
Collective labour agreements	None exist	Collective labour agreement for private security (2016)
Average monthly salary in the country in 2017	HUF 297,000 (EUR 958) gross HUF 197,500 (EUR 637) net	EUR 1,627 gross EUR 1,062 net
Average monthly salary of private security officer in 2017	HUF 200,000 (EUR 645) gross (est.) HUF 150,000 (EUR 483) net (est.)	EUR 1,000 gross (est.) EUR 750 net (est.)
Private security industry regulated by	The Private Security Act (CXXXIII/2005)	The Private Security Act (Official Gazette No. 17/11)
Competent national authority for drafting and amending legislation regulating the private security industry	Ministry of the Interior	Ministry of the Interior
Competent national authority for control and inspection of the private security industry	• The Police • Ministry of the Interior (via the Chamber of Private Security)	• Ministry of the Interior • Inspectorate for Interior Affairs • The Police
Entrance requirements and restrictions	Entrance requirements (vetting procedure) for the private security industry: *At company level* • General conditions: • Criminal record check • Have at least one licensed security person • The company is not prohibited from engaging in private security activity • The company must not have an unpaid supervisory fine concerning its private security activity • Liability insurance *At personal level* • Age above 18 years • No criminal record • Legal residence in the country • State-mandated examination Every 5 years, obligatory state-mandated refresher training	Entrance requirements (vetting procedure) for the private security industry: *At company level* Entrance requirements depend on the type of licence General conditions: • Criminal record check • Hold a valid guard licence • Have a full-time security manager employed on a permanent contract (not required for all licences) • Have security personnel who are professionally trained • Have its own security control centre or one guaranteed by contract • Have to own or rent business premises in Slovenia • Liability insurance *At personal level* • Minimum age of 18 • EU, EEA or Swiss Confederation citizenship • Minimum professional training • Criminal record check • Passed a physical and psychological health assessment • Have active command of the Slovenian language

Table 4: Continuation

Characteristics	*Hungary*	*Slovenia*
Powers of private security officers	A security guard holds no state authority. Use of force is authorised, but items legally categorised as weapons are restricted. In case of property defence except public spaces: • Stop, identity check, require information about the purpose and right of entry. If required, prohibit entry. • Ask a person to show their packages • Ask to cease a breach of law • Use of technical security systems • Prohibit the taking in of unsafe items To make arrests and act on behalf of clients (exercising their rights to property, legal self-defence) Use of other means (in case of lawful self-defence): • CS gas/pepper spray • Service dog • Baton • Use of physical force • Handgun: very limited	In the event of a threat to life, personal safety or property or when order or public order are breached, a security guard may apply the following measures: • Warning • Verbal order • Ascertain identity • Superficial search • Prevent entry to or leaving from a protected area • Detain a person • Use physical force • Use handcuffs and other means of restraint A security officer may also use other measures if so specified by the act governing a particular field (protection of airports, casinos or nuclear facilities). A security officer may use technical security systems. Use of other means: • Incapacitating spray • Service dog • Carrying and use of a firearm – handgun (except for a security watchman)
Training and related provisions	• Minimum no. of basic training hours for security officer: 320 • The training is provided by specialised training institutions licensed by the Ministry of the Interior • Every 5 years a refresher training programme is mandatory by law • The training is provided by an educational institution of the Chamber of Bodyguards, Property Protection and Private Detectives • Basic training and refresher training are usually low-quality courses • University-level education: • National University of Public Services, Faculty of Law Enforcement Course for private security and local governmental law enforcement (BA, full-time and correspondence)	• Training programme is mandatory by law • Minimum no. of basic training hours for security officer: 102 • Mandatory additional/advanced training for various security jobs • Mandatory refresher training • The training is provided by specialised institutions licensed by the Ministry of the Interior • The training is financed by the company and/or officer • Upon successfully completion of basic training, private security guards are issued with a certificate of competence

Sources for Hungary: CoESS (2013), Központi Statisztikai Hivatai (2017). Some data were obtained directly from the deputy chief of the Hungarian police.

Sources for Slovenia: CoESS (2013), Gerasimoski & Sotlar (2013), Sotlar & Čas (2011), Sotlar & Dvojmoč (2016), Private Security Act (ZZasV-1, 2011), Republic of Slovenia Statistical Office (2018).

3 EVALUATION OF THE REGULATION OF PRIVATE SECURITY IN THE TWO COUNTRIES BASED ON LEGISLATION AND SOCIETAL FOUNDATIONS

The characteristics of private security in Hungary and Slovenia presented above give us a solid basis to evaluate the extent and level of regulation of private security in both countries. In order to make the data from two countries comparable with the situation in other EU countries, an evaluation based on a common methodology will now be conducted.

3.1 Methods

Button-Stiernstedt's evaluation model

Button and Stiernstedt (2016, p. 16) wanted to "illustrate the current state of private security regulation in the Member States of the EU". In order to achieve that, they were looking for a comprehensive methodology to evaluate private security in different EU countries. They studied the most significant literature, academic research articles, reports, government websites and interviews with industry professionals on these topics etc. They mostly relied on findings from four sources: 1) *State regulation concerning the civilian private security services and their contribution to crime prevention and community safety* (United Nations Office on Drugs and Crime, 2014); 2) *Private security in Europe in Europe – CoESS Facts & Figures 2011* (CoESS, 2011); 3) *Security regulation, conformity assessment & certification. Final report (Vol. I: Main report)* (ECORYS, 2011); and 4) *Assessing the regulation of private security across Europe* (Button, 2007).

They realised that merely analysing the legislative side of private security would be insufficient and that the way legislation is actually implemented is almost equally important, which led them to consider societal foundations. They created an analytical tool consisting of: 1) Legislation ("those aspects pertaining directly or indirectly to the actual national legislative framework"); and 2) Societal Foundations ("as the direct or indirect consequences of that legislation upon its implementation into the society") (Button & Stiernstedt, 2016, p. 8).

Button and Stiernstedt (2016) divided Legislation into 3 sub-divisions (Regulation, Coverage and Licensing) with a total of 13 questions. Societal Foundations were also divided into 3 sub-divisions (Professional associations, Enforcement and Training) with a total of 9 questions. They arbitrarily allocated a maximum of 100 points to these 22 questions. Ten points were allocated to Regulation, 16 to Coverage and 30 to Licensing, which gives 56 points to Legislation. On the other hand, 44 points were allocated to Social Foundations of which 4 points were allocated to Professional associations, 8 to Enforcement and 32 to Training (Button & Stiernstedt, 2016). Tables 6 and 7 explain the further division of questions and allocation of points, while Table 5 presents a description of the criteria according to which the private security regulation of each country was evaluated upon the allocation of the appropriate number of points.

Table 5: Sub-divisions and questions of the league table

Criteria/questions (max. 100 points)	Descriptions of criteria
Legislation/Regulation type (max. 4)	• 4 points: regulation is specific to private security • 2 points: general legislation with specific amendments addressing private security issues • 0 points: general legislation
Regulatory body (max. 2)	• 2 points: a single regulatory body is effectively responsible for all or most private security concerns • 0 points: the responsibility for private security is divided or diffuse
Role of PSI in regulation (max. 4)	• 4 points: if formally and democratically established and run • 2 points: if informal but influential • 0 points: if having a dominating role, formal or informal, and if not holding a significant role in regulation
Scope of licensing regulation (max. 10)	• Up to 10 points: for scope going beyond general standards with 2 points for each area (this refers to regulated areas falling outside of general guarding, e.g. CIT, close protection, private investigators etc.)
Prohibitions/Restrictions (max. 2)	• 2 points: if regulation contains a "speciality principle" • 0 points: without a "speciality principle" **Speciality principle means that one single legal entity, officially recognised as a private security company, is only allowed to carry out private security services and not auxiliary or additional services*
In-house security personnel (max. 4)	• 2 points: in-house security personnel, i.e. privately managed staff providing security services is included in the regulation • 0 points: in-house is not included in the regulation
Licensing firms (max. 8)	• 8 points: regulation contains comprehensive criteria • 4 points: regulation contains partial criteria • 0 points: regulation contains no criteria **Criteria included but were not limited to a consideration of background checks, criminal records, financial viability, fees, age restrictions, minimum educational level, language proficiency etc.*
Licensing operatives (max. 8)	• 8 points: if the regulation contains comprehensive criteria • 4 points: if the regulation contains partial criteria • 0 points: if the regulation contains no criteria **Criteria included but were not limited to a consideration of physical and psychological evaluations, criminal records, training certificates, fees, age restrictions, minimum educational level, language proficiency etc.*
Types of licensing (max. 4)	• 4 points: different licences may be issued for different roles and whether such differences reflect a comprehensive licensing spectrum • 2 points: different licences may be issued for different roles and whether such differences reflect a partial licensing spectrum • 0 points: no types of licences **Licences included but were not limited to: aviation/ airport security, CCTV related, close protection, CIT, maritime security etc.*
Licence card (max. 4)	• 4 points: if a licence card meeting the official EU standard for ID cards is issued • 0 points: if not

Table 5: Continuation

Compulsory codes of conduct (max. 2)	• 2 points: if one exists • 0 points: if not existing
Special equipment & weapons (max. 2)	• 2 points: firearms in private security are regulated that consequently allow or disallow guards from being armed with firearms • 0 points: unregulated
Working conditions (max. 2)	• 2 points: in legislation that affects the PSI, i.e. not necessarily specific to the PSI, there are sector- specific binding agreements for working conditions • 0 points: no sector-specific binding agreements
Professional associations (max. 4)	• 4 points: there are professional associations assumed to promote higher, better and more effective standards than the statutory minimum • 0 points: no such professional associations
Complaints procedure (max. 4)	• 4 points: regulation provides specific provisions for making, managing and following up complaints against private security individuals and/or entities • 0 points: no such provisions in the regulation
Sanctions for transgressions (max. 4)	• 4 points: there is a possibility for the regulator to administer sanctions upon security industry or individuals under both criminal law and administrative law • 2 points: there is a possibility for the regulator to administer sanctions upon security industry or individuals under criminal law • 0 points: there is no such possibility
Licensing of trainers (max. 4)	• 4 points: a licence is required to provide security personnel training • 0 points: no licence is required to provide security personnel training
Mandatory training (max. 14)	Mandatory training is stipulated by the regulation. The range of hours: • 14 points: 121 + hours • 12 points: 100 to 120 hours • 10 points: 80 to 99 hours • 8 points: 60 to 79 hours • 6 points: 40 to 59 hours • 4 points: 20 to 39 hours • 2 points: 1 to 19 hours • 0 points: 0 hours
Exam (max. 2)	• 2 points: upon successfully completing the basic training there is a theoretical and/or practical pass/fail exam after which private security guards are issued with a certificate of competence • 0 points: no exam
Refresher training (max. 4)	• 4 points: mandatory refresher or follow-up training exists • 0 points: no mandatory refresher or follow-up training exists
Specialist training (max. 4)	• 4 points: mandatory specialist training is required for security roles other than general guarding • 0 points: no mandatory specialist training exists
Management/Supervisor training (max .4)	• 4 points: mandatory training is required for management and/or supervisory roles of private security • 0 points: no mandatory training for management and/or supervisory roles

Source: Button and Stiernstedt (2016)

3.2 Results

Evaluation of private security regulation in Hungary and Slovenia

Table 6 presents a comparison of the results of the evaluation of private security regulation in the two countries based on legislation. The first column presents the sub-divisions and questions with the maximum possible points, the second and third columns present the results for Hungary and Slovenia in 2018, while the fourth column presents the results for Slovenia from Button and Stiernstedt's study conducted in 2016.

Table 6: Comparison of the states based on Legislation

Sub-divisions/questions (Max. points – 56)	Hungary	Slovenia	Slovenia in Button and Stiernstedt's (2016) evaluation
I. Regulation (10)	***10***	***10***	***10***
Legislation/Regulation type (4)	4	4	4
Regulatory body (2)	2	2	2
Role of PSI in regulation (4)	4	4	4
II. Coverage (16)	***8***	***14***	***14***
Scope of licensing regulation (10)	6	10	10
Prohibitions/Restrictions (2)	2	0	0
In-house security personnel (4)	0	4	4
III. Licensing (30)	***18***	***28***	***22***
Licensing firms (8)	8	8	4
Licensing operatives (8)	4	8	8
Types of licensing (4)	2	4	4
Licence card (4)	0	4	4
Compulsory codes of conduct (2)	0	2	2
Special equipment & weapons (2)	2	2	0
Working conditions (2)	0	0	0
Total	**36**	**52**	**46**

Table 7 compares the results for the two countries based on societal foundations. The first column presents the sub-divisions and questions with the maximum possible points, the second and third columns present the results for Hungary and Slovenia in 2018, while the fourth column gives the results for Slovenia from Button and Stiernstedt's study in 2016.

Table 7: Comparison of the states based on Societal Foundations

Criteria/questions (Max. points – 44)	**Hungary**	**Slovenia**	**Slovenia in Button and Stiernstedt's (2016) evaluation**
I. Professional associations (4)	***4***	***4***	***4***
II. Enforcement (8)	***8***	***8***	***4***
Complaints procedure (4)	4	4	0
Sanctions for transgressions (4)	4	4	4
III. Training (32)	24	30	28
Licensing of trainers (4)	4	4	4
Mandatory training (14)	14	12	10
Exam (2)	2	2	2
Refresher training (4)	4	4	4
Specialist training (4)	0	4	4
Management/Supervisor training (4)	0	4	4
Total	**38**	**42**	**36**

When we combine the scores in Tables 6 and 7, we obtain the following results: Hungary: 74 points (36 for Legislation and 38 points for Societal Foundations); Slovenia: 94 points (52 points for Legislation and 42 for Societal Foundations) and Slovenia in the study from 2016: 82 points (46 points for Legislation and 36 points for Societal Foundations). Comparison of private security regulation in Hungary and Slovenia as well as the results given by the evaluation model using legislation and societal foundations are discussed in section 4.

4 DISCUSSION

Hungary and Slovenia share one common characteristic – they are both ex-socialist countries with a relatively short history of private security development and regulation. But here most of the similarities stop. Hungary outnumbers Slovenia in population terms by 4.5 times, but this is not reflected in the private security field. Hungary has 37 times more registered private security firms and 15 times more private security guards than Slovenia! If we consider another parameter, the number of private security guards per police officer, we realise there are almost 2.5 times more security guards than police officers in Hungary, while in Slovenia there are still slightly more police officers than security guards. The reason for this discrepancy between the two countries was not researched in this paper, but certainly deserves further analysis. A comparison of the powers held by security guards shows that Slovenian guards are more empowered than their Hungarian colleagues. On the other hand, according to legislation the latter have to complete up to 320 hours of training, three times more than in Slovenia. However, it seems that in reality this training obligation in Hungary is quite poor and does not meet the prescribed standards.

Button-Stiernstedt's evaluation model also enabled us to assess and compare private security regulation based on the legislation and societal foundations in the two countries. We allocated points to 22 criteria of which 13 were related to legislation and 9 to societal factors. Slovenia was ranked third after Belgium (94 points) and Spain (90 points) among 26 EU states in Button and Stiernstedt's evaluation in 2016.[3] In this new evaluation, Slovenia received 94 points, making it equal to Belgium that holds first place among 27 EU countries. What makes Slovenia's score 12 points better than the 2016 evaluation? We gave Slovenia 6 additional points for Legislation as well as 6 more points for Societal Foundations. Namely, we believe that the criteria "licensing firms", "special equipment & weapons", "complaints procedure" and "mandatory training" were not initially allocated enough points regarding the existing regulation in Slovenia.

On the other hand, Hungary with 74 points would be ranked 7th, with the same score as Ireland, behind Sweden and Portugal with 78 points and ahead of Romania with 68 points. Although Hungary seems to have scored relatively highly in the survey, this does not mean the situation in practice is positive. Several criteria are stipulated by law, but in reality only a small fraction of the conditions can actually be observed.

In this article, we strictly and accurately followed Button-Stiernstedt's private security regulation evaluation model because we wanted to put Hungarian private security on the "EU private security regulation map". The model mostly works, but we suggest that in the future some criteria should be used more flexibly than Button and Stiernstedt proposed in 2016. Thus, in cases where criteria consist of several sub-criteria and the total sum is 4 points (for example), we propose that 0, 1, 2, 3, or 4 points be allocated (and not just 0, 2 or 4 points) because countries can have very different levels of regulation of particular private security questions. Of course, a precondition for that is that each sub-criterion is clearly defined and elaborated.

REFERENCES

Button, M. (2007). Assessing the regulation of private security across Europe. *European Journal of Criminology*, *4*(1), 109–128.

Button, M. (2012). Optimising security through effective regulation: Lessons from around the globe. In T. Prenzler (Ed.), *Policing and security in practice* (pp. 220–240). Basingstoke: Palgrave.

Button, M., & Stiernstedt, P. (2016). Comparing private security regulation in the European Union. *Policing and Society.* Retrieved from http://dx.doi.org/10.1080/10439463.2016.1161624

Christián, L. (Ed.) (2014). *A magánbiztonság elméleti alapjai* [The theoretical basis of private security]. Budapest: National University of Public Service.

Christián, L. (2015). Law enforcement. In A. Varga Zs, A. Patyi, & B. Schanda (Eds.), *The basic (fundamental) law of Hungary: A commentary of the new Hungarian constitution* (2nd ed.) (pp. 278–288). Dublin: Clarus Press.

Christián, L. (2016). A rendőrség és rendészet [Law enforcement and the police]. In A. Jakab, & Gy. Gajduschek (Eds.), *A Magyar Jogrendszer Állapota* [Analysis

[3] *Please note that an error was discovered in the article by Button and Stiernstedt (2016). Namely, Spain could not receive 18 points for "Coverage" since the maximum number of points was 16. The total number of points for Spain was therefore 90 and not 92 as written in Table 3 on page 8 of the mentioned article. However, Spain remains second, after Belgium and in front of Slovenia. This error was discussed with Button and Stiernstedt who had also noticed their mistake.*

of Hungarian law system] (pp. 681–707). Budapest: MTA Társadalomtudományi Kutatóközpont. Retrieved from http://jog.tk.mta.hu/uploads/files/25_Christian_Laszlo.pdf

Christián, L. (2017). The role of complementary law enforcement institutions in Hungary: Efficient synergy in the field of complementary law enforcement – a new approach. *Public Security and Public Order*, (18), 132–139.

CoESS. (2011). *Private security in Europe – CoESS Facts & Figures 2011*. Brussels: CoESS. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

CoESS. (2013). *Private security in Europe - CoESS Facts & Figures 2013*. Brussels: CoESS. Retrieved from http://www.coess.org/newsroom.php?page=facts-and-figures

De Waard, J. (1993). The private security sector in fifteen European countries: Size, rules and legislation. *Security Journal, 4*(2), 58–62.

De Waard, J. (1999). The private security industry in international perspective. *European Journal of Criminal Policy and Research, 7*(2), 143–174.

De Waard, J., & Van De Hoek, J. (1991). *Private security size and legislation in the Netherlands and Europe*. The Hague: Dutch Ministry of Justice.

ECORYS. (2011). *Security regulation, conformity assessment & certification: Final report* (Vol. I: Main report). Brussels: European Commission, DG Enterprise & Industry. Reterived from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/secerca_final_report_volume__1_main_report_en.pdf

Finszter, G. (2001). The share of competence of state authorities within the sphere of public order and safety protection in Hungary. In J. Widaczki, M. Maczynski, & J. Czapska (Eds.). *Local community, public security: Central and Eastern European countries under transformation* (pp. 53–66). Warsaw: Institute of Public Affairs.

Gerasimoski, S., & Sotlar, A. (2013). Comparative analysis of private security in Macedonia and Slovenia – history, trends and challenges. In C. Mojanoski (Ed.), *International scientific conference The Balkans between past and future: Security, conflict resolution and Euro-Atlantic integration* (Vol. 2, pp. 425–445). Bitola: University "St. Kliment Ohridski"; Skopje: Faculty of Security.

Központi Statisztikai Hivatai. (2017*). Népesség, összesen (2006–2017)* [Population, total (2006–2017)]. Retreived from https://www.ksh.hu/docs/hun/eurostat_tablak/tabl/tps00001.html

Johnston, L. (1992). *The rebirth of private policing*. London: Routledge.

Jones, T., & Newburn, T. (Eds.) (2006). *Plural policing.* Abingdon: Routledge.

Meško, G., Nalla, M., & Sotlar, A. (2004). Youth perceptions of private security in Slovenia: Preliminary findings. In G. Meško, M. Pagon, & B. Dobovšek (Eds.), *Policing in Central and Eastern Europe, Dilemmas of contemporary criminal justice* (pp. 745–752). Ljubljana: Faculty of Criminal Justice and Security.

Ministrstvo za notranje zadeve. (2018). *Seznam imetnikov licenc*. [Licence's holders list] Retrived from http://www.mnz.gov.si/si/mnz_za_vas/zasebno_varovanje_detektivi/zasebno_varovanje/evidence_vloge_in_obrazci/

Moreira, S., Cardoso, C., & Nalla, M. K. (2015). Citizen confidence in private security guards in Portugal. *European Journal of Criminology*, *12*(2), 208–225.

Nalla, M. K., & Heraux, C. G. (2003). Assessing goals and functions of private security. *Journal of Criminal Justice*, *31*(3), 237–247.

Nalla, M. K., & Hummer, D. (1999a). Assessing strategies for improving law enforcement/security relationships: Implications for community policing. *International Journal of Comparative and Applied Criminal Justice*, *23*(2), 227–239.

Nalla, M. K., & Hummer, D. (1999b). Relations between police officers and security professionals: A study of perceptions. *Security Journal*, *12*(3), 31–40.

Nalla, M., & Hwang, E. (2004). Assessing professionalism, goals, images, and nature of private security in South Korea. *Asian Policing*, *2*(1), 104–121.

Nalla, M. K., & Lim, S. S. (2003). Students' perceptions of private police in Singapore. *Asian Policing*, *1*(1), 27–47

Nalla, M. K., & Meško, G. (2015). What shapes security guards' trust in police? The role of perceived obligation to obey, procedural fairness, distributive justice, and legal cynicism. *Journal of Criminal Investigation and Criminology*, *66*(4), 307–318.

Nalla, M., & Newman, G. (1990). *A primer in private security*. New York: Harrow and Heston.

Nalla, M. K., Gurinskaya, A., & Rafailova, D. (2017). Youth perceptions of private security guard industry in Russia. *Journal of Applied Security Research*, *12*(4), 543–556.

Nalla, M. K., Johnson, J. D., & Meško, G. (2009). Are police and security personnel warming up to each other? A comparison of officers' attitudes in developed, emerging, and transitional economies. *Policing: An International Journal of Police Strategies & Management*, *32*(3), 508–525.

Nalla M. K., Ommi, K., & Murthy, V. S. (2013). Nature of work, safety, and trust in private security in India: A study of citizen perceptions of security guards. In N. P. Unnithan (Ed.), *Crime and justice in India* (pp. 226–243). New Delhi: SAGE Publications India.

Nalla M. K, Meško, G., Sotlar, A., & Johnson, J. D. (2006). Professionalism, goals, and the nature of private police in Slovenia. *Varstvoslovje*, *8*(3–4), 309–322.

Police. (2018). *About the police*. Retreived from https://www.policija.si/eng/index.php/aboutthepolice

Republic of Slovenia Statistical Office. (2018). *Earnings and labor costs*. Retrieved from http://www.stat.si/StatWeb/en/Field/Index/15

Sotlar, A. (2007). Izvor legitimnosti zasebnega varovanja: Dobiček med zasebnim in javnim interesom? [The origin of the legitimacy of private security: Earnings between private and public interests]. In *IV. mednarodna konferenca, VIII. strokovni posvet Dnevi zasebnega varovanja* (pp. 13–25). Ljubljana: Zbornica Republike Slovenije za zasebno varovanje.

Sotlar, A. (2010). Private security in a plural policing environment in Slovenia. *Cahiers Politiestudies*, *3*(16), 335-353.

Sotlar, A., & Čas, T. (2011). Analiza dosedanjega razvoja zasebnega varovanja v Sloveniji: Med prakso, teorijo in empirijo [Analysis of the development of private security in Slovenia between practice, theory and empirical experience]. *Revija za kriminalistiko in kriminologijo*, *62*(3), 227–241.

Sotlar, A., & Dvojmoč, M. (2016). Private security in Slovenia: 25 years of experiences and challenges for the future. In B. Vankovska, & O. Bakreski (Eds.), *International scientific conference Private Security in the 21st Century* (pp. 15–39). Skopje: Chamber of Republic of Macedonia for Private Security.

Sotlar, A., & Meško, G. (2009). The relationship between the public and private security sectors in Slovenia – from coexistence towards partnership? *Varstvoslovje, 11*(2), 269–285.

United Nations Office on Drugs and Crime. (2014). *State regulation concerning the civilian private security services and their contribution to crime prevention and community safety.* Vienna: UNODC. Retrieved from https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Ebook0.pdf

Van Steden, R., & Nalla, M. K. (2010). Citizen satisfaction with private security guards in the Netherlands: Perception of an ambiguous occupation. *European Journal of Criminology*, *7*(3), 214–234.

Van Steden, R., & Sarre, R. (2007). The growth of private security: Trends in the European Union. *Security Journal, 20*(4), 222–235.

Van Steden, R., & Sarre, R. (2010). Private policing in the former Yugoslavia: A menace to society? *Varstvoslovje, 12*(4), 424–439.

Zakon o zasebnem varovanju (ZZasV-1) [Private Security Act]. (2011). *Uradni list RS,* (17/11).

About the Authors:

László Christián, PhD, associate professor, Faculty of Law Enforcement, National University of Public Service, Budapest, Hungary. E-mail: christian.laszlo@uni-nke.hu

Andrej Sotlar, PhD, associate professor, Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: andrej.sotlar@fvv.uni-mb.si

Comparing Counterintelligence and Counterterrorism – Similarities, Issues and Solutions

VARSTVOSLOVJE,
Journal of Criminal Justice and Security,
year 20
no. 2
pp. 163–181

Jaroš Britovšek

Purpose:

This paper aims to discuss and compare counterintelligence and counterterrorism, particularly in the aftermath of the Cold War and the rise of new forms of non-state terrorism, and critically examine the tendency of western liberal democracies to assign counterterrorism tasks to services traditionally involved in counterintelligence. The aim is therefore to identify similarities, differences and issues that arise between these two activities. In addition, some solutions to the issues presented are proposed.

Methods:

Models and concepts are developed and presented through analysis of primary and secondary sources. Several aspects are identified, leading to a comparative analysis being conducted.

Findings:

Counterintelligence and counterterrorism seem very similar at first glance, but differ from each other in certain important respects. They both lie on a spectrum between a 'law enforcement model' and an 'intelligence model', and can overlap when targeting state-sponsored terrorism or state and non-state actors' intelligence activities. Yet they vary substantially when dealing with risks, time sensitivity and the sharing of information, and ignoring them can have a significant impact on national security.

Research Limitations:

Besides the secret nature of intelligence and, therefore, limited access to information, the paper primarily focuses only on states' security apparatus and does not consider other political, societal or psychological actors or approaches.

Practical Implications:

In the paper, several solutions derived from the principle of the separation of counterintelligence and counterterrorism are presented for policymakers, while also calling for the establishing of sharing and coordination bodies.

Value:

This paper counters the prevailing paradigm that overemphasises the role of the traditional services involved in counterintelligence as part of the fight against modern terrorism. The findings and conclusions are intended for political, professional and wider public audiences.

UDC: 351.746.1:343.3

Keywords: counterintelligence, counterterrorism, intelligence and security services, law enforcement

Primerjava protiobveščevalne in protiteroristične dejavnosti – podobnosti, dileme in rešitve

Namen prispevka:

Namen prispevka je obravnavati ter primerjati protiobveščevalne in protiteroristične dejavnosti, še posebej z vidika konca hladne vojne in pojava novih oblik terorizma, ter kritično obravnavati nagnjenja zahodnih liberalnih demokracij, ki vlogo protiteroristične dejavnosti potiskajo v organizacije, ki so bile tradicionalno zadolžene za protiobveščevalno dejavnost. Cilj je torej predstaviti podobnosti, razlike ter dileme. Glede na identificirane dileme so predstavljene tudi nekatere rešitve.

Metode:

Za razvoj modelov in konceptov je bila uporabljena analiza primarnih in sekundarnih virov. Identificiranih je bilo več vidikov, na podlagi katerih je bila nato opravljena primerjalna analiza.

Ugotovitve:

Protiobveščevalna in protiteroristična dejavnost se zdita na prvi pogled podobni, vendar obstajajo med njima pomembne razlike. Obe ležita na spektru med 'modelom organov pregona' in 'obveščevalnim modelom' ter se na nekaterih področjih tudi prekrivata, kot je spremljanje državno-sponzoriranega terorizma ter terorističnih skupin, ki uporabljajo obveščevalno dejavnost. Dejavnosti se razlikujeta predvsem na področju tveganj, časovne občutljivosti ter uporabe informacij. Neupoštevanje teh razlik ima lahko pomembne posledice za nacionalno varnost.

Omejitve:

Poleg tajne narave obveščevalne dejavnosti in s tem omejenega dostopa do informacij se prispevek osredotoča predvsem na varnostni aparat države in se hkrati izogiba ostalim političnim, družbenim ter psihološkim akterjem in pristopom k tematiki.

Praktična uporabnost:

V prispevku je predstavljenih več rešitev za odločevalce, ki izhajajo iz načela delitve protiobveščevalne in protiteroristične funkcije. Izražena je tudi potreba po centru, ki bi omogočal koordinacijo in izmenjavo informacij.

Izvirnost/pomembnost prispevka:

Prispevek nasprotuje prevladujoči paradigmi, ki daje pretirano vlogo v boju proti modernemu terorizmu službam, ki so tradicionalno vpete v protiobveščevalno delo. Ugotovitve so namenjene politični, strokovni in širši javnosti.

UDK: 351.746.1:343.3

Ključne besede: protiobveščevalna dejavnost, protiteroristična dejavnost, obveščevalne in varnostne službe, organi pregona

1 INTRODUCTION

Counterintelligence and counterterrorism are both significant activities of any national security system, with each serving their particular purpose and goals. While authors are chiefly concerned with either counterintelligence (Podbregar & Ivanuša; 2016; Prunckun, 2012, 2014; Van Cleave, 2013) or counterterrorism (Crelinstein, 2014; Pedahzur, 2009), some (Gleghorn, 2003; Mobley, 2012) also promote the use of counterintelligence tradecraft against terrorism. Following the Cold War and the rise of new forms of threats such as non-state sponsored terrorism, the tendency of western liberal democracies has been to assign counterterrorism tasks and responsibilities to intelligence and security services traditionally involved in counterintelligence (Bauer, 2016). Although counterintelligence and counterterrorism sometimes overlap, confusing them may have a significant impact on national security as they essentially differ in their nature, purpose and goals. Both activities aim to neutralise specific threats. By definition, counterintelligence deals with countering a foreign intelligence threat, while counterterrorism deals with preventing a terrorist threat. Intelligence and terrorism are defined in a multitude of ways, with no firm consensus of what each constitutes (Warner, 2002; Weinberg, Pedahzur, & Hirsch-Hoefler, 2004).

Intelligence itself is an elusive concept, but at its core it is concerned with data and information. It consists of three fundamental elements: the collection of data and information, analysis of collected data and information, and counterintelligence, or preventing an adversary from collecting data and information about oneself. Counterintelligence is a vital activity for protecting secrets. It is therefore pitted against other entities' intelligence activities and usually also an integral part of a state's intelligence efforts (Britovšek, Sotlar, & Tičar, 2017). However, intelligence services are not only involved in intelligence gathering. Warner (2002, p. 21) defined intelligence as a "secret, state activity to understand or influence foreign entities", meaning that besides espionage some states use intelligence agencies to conduct covert action or special measures in order to influence other political entities. Counterintelligence therefore also includes countering activities of influence (covert actions), such as subversion, sabotage and even terrorism[1] (Van Cleave, 2013).

[1] *Counterintelligence tasks can also include counterpropaganda or countering 'fake news', to use a more fashionable term, or protecting a country's electoral process. Russian intelligence and propaganda interference in the 2016 presidential election in the United States is a recent example of this (Priest, 2017).*

In contrast, terrorism is difficult to define due to different, often opposing political interests, and to date there is no universally objective and internationally accepted definition of terrorism (Ramsay, 2015; Richards, 2014; Schmid, 2004). One reason for this, at least according to Bauer (2016), is that "nothing more resembles a terrorist than a resistance fighter". Yet some efforts have been made to identify certain key elements of terrorism that go some way to defining it. To distinguish it from other criminal acts, Hoffman (2006, p. 40) defined terrorism "as the deliberate creation and exploitation of fear through violence or the threat of violence in pursuit of political change". In addition, Weinberg et al. (2004, p. 782) stated that "terrorism is a politically motivated tactic involving the threat or use of force or violence in which the pursuit of publicity plays a significant role". Counterterrorism's main role is therefore to counter politically motivated illegal acts of violence.

Countries differ in their approaches to national security issues, which in turn depends significantly on how they perceive the threats they face. Intelligence tends to be divided into foreign intelligence and security intelligence. The former focuses on foreign governments and situations external to the service's home country, while the latter focus, but are not necessarily limited to, domestic or internal security threats (Herman, 1996). They are further divided into military and civilian counterparts. However, due to the hybridisation and overlapping nature of security threats in the contemporary international order, the lines between foreign and domestic, military and civilian, have been blurred considerably (Britovšek & Čretnik, 2016). Here, the differences between counterintelligence and counterterrorism may be explained and compared through two models of addressing the threats each is intended to neutralise: a 'law enforcement model' and an 'intelligence model'.

2 LAW ENFORCEMENT AND INTELLIGENCE MODELS

To better understand the frameworks and concepts according to which counterintelligence and counterterrorism operate, two models[2] have been developed to allow a more coherent analysis and comparison of the two activities; a 'law enforcement model' and an 'intelligence model' (see the simplified comparison of these models in Table 1). The 'law enforcement model' derives and is based on the legal feature or public law, while the 'intelligence model' originates and is based on political considerations, partly diplomatic and partly military, depending on the situation of a particular country. The models lie on a spectrum ranging from legal towards more political and military aspects, which will help us understand the issues and differences arising from counterintelligence and counterterrorism, and will also locate both activities on the spectrum these two models lie on.

[2] *The models have been derived, modified and adapted from already developed coercive models with regard to counterterrorism: the 'criminal justice model' and the 'war model'. The 'criminal justice model' perceives terrorism as a criminal act, using police to deal with it within the criminal justice system's restraints, while the 'war model' perceives terrorism as part of war, as revolutionary warfare, consequently using also hard force such as military action to eliminate or defeat terrorist threats (Crelinsten, 2014).*

The 'law enforcement model' presupposes a more stable operating environment of the 'rule of law', whereas the 'intelligence model' works in a more competitive, chaotic and hostile environment that is less constrained by a transparent framework or laws, rules and regulations. The main aspects of both models have been identified and compared and, with the support of each, counterintelligence and counterterrorism have been further compared and analysed with regard to several identified issues. The overlap and most significant differences have been identified and explained, leading to the conclusion that counterintelligence and counterterrorism should not be conflated, or perhaps even be conducted by the same organisational or institutional structures.

Table 1: Comparison of the 'law enforcement model' and 'intelligence model' in the context of counterintelligence and counter-terrorism

	Law enforcement model	**Intelligence model**
Main aspect	Perceiving and treating terrorism, espionage, subversion and sabotage as criminal acts	Perceiving and treating terrorism as a political or war tactic and intelligence as an auxiliary element of one's opponent
Environment	Legal environment with an emphasis on the rule of law	Competitive political environment, which in extreme cases can lead to war
Means and aim	To investigate, arrest and prosecute according to the rule of law	To gather and analyse intelligence on one's opponents' capabilities and intentions
Agents	Police and criminal justice system	Intelligence and security services
Information	Gathering evidence to be legally used in courts	Gathering intelligence with an emphasis on secrecy
Issues	Punishment not enough to deter politically motivated culprits Lack of knowledge before crimes are committed	Overemphasis and expansion of surveillance (delay of action) Ignoring or violating of basic human rights
Benefits	Delegitimises culprits as mere criminals	Preparation and possible prevention of threats

The models differ in several respects. These can be explained by their roots in different organisational cultures: one originating in law enforcement and the other from intelligence services (Hulnick, 1997). Starting with the main aspect, the 'law enforcement model' perceives terrorism as well as some intelligence activities such as espionage, sabotage and subversion as criminal acts, while the 'intelligence model' considers terrorism a political or military tactic and intelligence as an auxiliary element of an opponent's effort to achieve political or military goals. The 'law enforcement model' also assumes a stable legal framework and responds to criminal acts in compliance with the law and is subjected to constant judicial oversight. The means and aims are investigations, arrests and prosecutions according to the rule of law. Its primary agents are police agencies and the broader criminal justice system. The model perceives the world in a black-and-white manner of legal and illegal, while the 'intelligence model' sees the world more in shades of ambiguous grey (Gleghorn, 2003).

The 'intelligence model' functions in the more politically competitive international environment, which can – following Clausewitz's principles – in certain circumstances and extreme cases develop into war. The means and aims of the 'intelligence model' concentrate on gathering and analysing intelligence on one's opponents, assessing their capabilities and trying to understand their intentions (Vandepeer, 2011). Consequently, these activities are by nature much slower and more time-consuming than law enforcement investigations (Gleghorn, 2003). The main agents are intelligence services, or perhaps to be more precise in the context of counterintelligence and counterterrorism, security services. The latter depends on the countries' organisational framework; separated or combined foreign and security intelligence for example.

An important point of the distinction between the two models is the role of information in either's activities. The 'law enforcement model' focuses on gathering and establishing evidence, while the 'intelligence model' gathers data and information with the aim to produce intelligence reports for decision-makers regarding opponents' capabilities, plans and intentions. Information in the 'law enforcement model' refers to evidence, which has to satisfy specific legal standards or burdens of proof, such as 'probable cause' and 'beyond a reasonable doubt'. Its core objective is to prove that someone is guilty of a crime or not. On the other hand, information in the 'intelligence model' refers to intelligence, with a lower evidentiary standard and greater emphasis on assessments and prognosis. The latter derives from working in a more uncertain environment, trying to gain access to opponents' secrets, reveal their intent, and where they will likely try to counter one's own intelligence efforts. The main objective in the latter model is not to prove guilt as in the former, but to inform policymakers or military leaders (Berkowitz, 2003).

Both models have their advantages and disadvantages. In the 'intelligence model', the state receives intelligence reports on the current situation and possible future threats to form a clearer understanding of the opponent and, thus, take preventative actions by applying appropriate measures. But the nature of intelligence work makes agencies prone to the over classification of their products which are primarily meant for decision-makers, thus rendering it difficult to share with other relevant agencies (Goitein & Shapiro, 2011). The lower evidentiary standard and secrecy make it difficult to use intelligence (information) in courts and criminal justice proceedings (Bigo, Carrera, Hernanz, & Scherrer, 2015; Eijkman & van Ginkel, 2011). Moreover, overemphasising the role of intelligence can not only lead to overproduction and lack of action (Lutwak, 2015), but also to increased surveillance of ordinary citizens, which consequently risks ignoring basic human rights, especially without proper and effective oversight mechanisms (Lubin, 2017).

Conversely, the 'law enforcement model' follows a more legalistic and thus more legitimate process, utilising the 'rule of law' when dealing with suspects. Even if there was a political agenda, treating it as a mere crime can also have a delegitimising effect on the culprits' political ideology and goals. A deficiency of the model is too much emphasis and reliance on punishment, thus missing the point that highly politically motivated persons will not be deterred by the mere fear of punishment (Crelinsten, 2014). This reliance and focus on punishment risks law enforcement agencies becoming wilfully blind to any events occurring before a crime is prepared or carried out, thereby hindering the prevention of incidents (Treverton, 2009).

3 COUNTERINTELLIGENCE AND COUNTERTERRORISM

Counterintelligence and counterterrorism do not fall strictly into one model or the other. They usually lie on a spectrum between the 'intelligence model' and the 'law enforcement model', which depends on a state's institutions, organisations, history, culture and legislation. In general, counterintelligence lies closer to the 'intelligence model', working in a more politically competitive environment, while counterterrorism lies closer but is not strictly confined to the 'law enforcement model', with its greater emphasis on the legal framework and its attending constraints.

There is a reason the tasks of counterintelligence and counterterrorism are often perceived as being very similar, as they do overlap on some issues. This is especially seen in the 'intelligence model' because they both use surveillance techniques when monitoring their targets. Another common feature is the role of intelligence analysis, especially in risk[3] assessment, or assessing one's own vulnerabilities and identifying potential threats (Crelinsten, 2014; Prunckun, 2012; Vandepeer, 2011). In the 'law enforcement model', there is an overlap when criminal investigation is involved as both terrorism and some intelligence activities like espionage are considered criminal acts. Consequently, gathered information must fulfil certain evidentiary standards to allow its lawful and effective use in courts.

Another overlap between counterintelligence and counterterrorism are the threats themselves. On the one hand, states can be involved or otherwise support non-state groups that conduct terrorist acts. On the other, non-state groups, otherwise involved in terrorist attacks, can use intelligence gathering and espionage to support their main activities[4]. The interplay between states and non-state groups, as well as the rise of non-state groups' intelligence capabilities, is an area where counterintelligence and counterterrorism meet and cooperate. In order to enhance such cooperation, coordination and also the de-confliction of activities, states can and should establish coordination and information centres for these purposes (Britovšek & Čretnik, 2016).

Counterintelligence and counterterrorism are also dissimilar in their activities and functions, meaning there are significant differences when comparing the two activities on different organisational levels. Counterterrorism is a more independent activity, concentrating more or less on the obvious threat of terrorism, while counterintelligence is as an auxiliary element to other activities and depends on the organisation that employs it, that is, elements of counterintelligence can be used to protect the confidentiality of information, operations and sources in the police, intelligence, military or private sector (Britovšek et al., 2017; Prunckun, 2012). This difference means that counterintelligence can be more readily applied in the course of counterterrorism activities than vice versa.

[3] *As I explain later, imminent risks are more a feature in counterterrorism, where it is essential that intelligence analysis 'gets it right', connecting the right dots at the right time and finding the right targets (Bauer, 2016).*

[4] *For example, Hezbollah, a Shiite militant group from Lebanon with strong links to and support from Iranian intelligence, has been known to be involved in terrorist attacks (Azani, 2013). But through the years Hezbollah was also able to develop its own military and intelligence capabilities (Harber, 2009).*

Due to historical reasons and institutional evolution, the tasks of counterterrorism were pushed into the hands of agencies that knew how to conduct counterintelligence, but not how to counter the new forms of terrorism emerging after the Cold War. Terrorism during the Cold War was essentially part of the struggle between the two main antagonistic powers: the United States and the Soviet Union. Terrorist groups were active but were supported, managed or tolerated by the opposing states and their intelligence services (Bauer, 2016). Their biggest targets were foreign states and their intelligence services. The main reason counterintelligence played a major role in combating terrorism was due to this link to states as sponsors and targets. But the primary targets were always foreign intelligence activities. When communism/socialism collapsed, politically left-leaning terrorist groups practically disappeared[5]. The key point here is that countering terrorism was understood to be a function of and managed by states' intelligence services.

But as the environment changes and evolves, so does the threat. After the collapse of communism, the greatest threat, the Soviet Union and its allies, disappeared and western intelligence and security services started losing their *raison d'être*. From a historical point of view, intelligence and counterintelligence usually rise to prominence when there is a highly competitive or hostile environment, usually between religious, national or ideological blocs or coalitions. Such were the periods of the religious wars between Catholics and Protestants in Europe and the ideological rivalry between the United States and the Soviet Union during the Cold War (Liulevicius, 2011). The 'intelligence model' thrives in competitive environments. Yet, after the collapse of communism, the level of hostilities and competition fell drastically, and with it the foreign intelligence threat and the importance of counterintelligence[6].

However, the rise of non-state, Islamist extremism and terrorism, and the re-emergence of intelligence threats from countries such as Russia and China, returned the focus to intelligence and security services. The problem is that the task of counterterrorism has been assigned to agencies that were responsible for either counterintelligence or law enforcement. Bauer (2016) argues that most western counterterrorism activities are today being conducted by agencies that traditionally worked in the field of counterintelligence, as that was the purpose for their establishment. States did not properly recognise the cultural evolution of terrorism, which transitioned to the "hybridization of criminality, religious fanaticism, and terrorism". The need to understand this difference is therefore essential for providing possible organisational solutions to issues concerning counterintelligence and counterterrorism.

Counterintelligence and counterterrorism have both common and distinguishing features which can be recognised through the lenses of either the

[5] *For example, the German left extremist group 'Baader-Meinhof' announced its disbandment in 1998, which was five years after its last terrorist attack (Lockwood, 2011).*

[6] *For example, legislators in the United States drastically cut the intelligence budget in the aftermath of the fall of communism. The number of personnel employed in the intelligence community dropped by about a sixth in the mid-1990s. Similarly, in the United Kingdom, intelligence and security services faced lower budgets and the first personnel layoffs since World War II (Warner, 2014).*

'law enforcement model' or the 'intelligence model'. Through further analysis, we attempt to prove that although several aspects of counterintelligence and counterterrorism are similar, there are significant differences which can have a serious impact on the overall efficiency of national security (for the purpose of this analysis, see the simplified version of the counterintelligence and counterterrorism comparison in Table 2). As mentioned, the main aim of counterintelligence is to counter the intelligence threat, while the main aim of counterterrorism is to counter the terrorist threat. The intelligence threat usually comes from foreign states and their intelligence services, while the terrorist threat often comes from international terrorist organisations and domestic political extremist groups or individuals.

Table 2: Comparing counterintelligence and counterterrorism

	Counterintelligence	**Counterterrorism**
Aim and focus	To counter the intelligence threat To protect institutions (state and non-state)	To counter the terrorist threat To protect institutions and the civilian population
Threat	Foreign states	Domestic and/or foreign political extremists
Defensive role	Protecting secrets Deterrence and detection	Protecting potential targets and victims Target hardening Critical infrastructure protection Monitoring people, money, goods and services
Proactive role	Detection, deception and neutralisation	Detection, disruption, prevention and neutralisation
Imminent risks	Loss of information	Loss of life
Time	Ally (long-term investigations tolerated)	Enemy (urgent short-term action)
Information	Need to know	Need to share
Overlap	Risk assessments and surveillance Evidentiary standard and prosecution State-sponsored terrorism Non-state group intelligence efforts	

3.1 The Defensive Role of Counterintelligence and Counterterrorism

Counterintelligence and counterterrorism can be divided into defensive and proactive[7] roles. Pedahzur (2009) added a defensive model to the other counterterrorism models mentioned earlier. The defensive model does not deal directly with potential terrorists but focuses on the protection of potential targets and victims of terrorism. The same can be applied to counterintelligence, with

[7] *Counterintelligence and counterterrorism are usually divided along defensive/offensive or passive/active modes or lines (Duvenage & Von Solms, 2015). But because these roles are not easily distinguishable from each other, and often overlap, we use a somewhat hybrid distinction, using defensive and proactive modes as a benchmark.*

the exception that its chief mission is to protect state secrets (Britovšek, 2017). Defensive counterintelligence includes deterrence and detection (Prunckun, 2012, 2014), while defensive counterterrorism encompasses target hardening, protection of critical infrastructure and the monitoring and regulation of the flow of people, money, goods and services (Crelinsten, 2014). All of these defensive activities strive to deny or discourage opponents' activities. However, some measures will differ since deterring mere access to information, usually held in a government facility or computer network, is not the same as hardening a target from a kinetic attack whose aim is to kill or cause as much physical damage as possible to facilities, infrastructure and civilian population.

Defensive counterterrorism's role is not strictly or exclusively reserved for law enforcement and security services. Because the terrorist threat endangers a much wider population, counterterrorism is usually implemented throughout national security structures (e.g. military, police, border controls and immigration officers) including the private sector (e.g. private security and banking system) (Crelinsten, 2014). On the other hand, defensive counterintelligence is more limited and concentrated on protecting certain organisations or institutions. It is manifested in physical security, personnel security (vetting), information security and communications security of the organisation it seeks to protect (Prunckun, 2012).

3.2 Proactive Roles of Counterintelligence and Counterterrorism

Both counterintelligence and counterterrorism have proactive roles. The starting point of proactive counterintelligence is detection, which may also be considered part of its defensive role. It is an act of noticing an event that is or can be associated with a breach or potential breach of secret or protected information. This leads to an investigation and surveillance of the targets (Prunckun, 2012). The agency then has a choice regarding how to neutralise the threat. This depends significantly on the abovementioned environment. It can decide to follow the 'law enforcement model' and gather evidence and prosecute the culprits, or use the 'intelligence model' and gather more intelligence and find out more about the *modus operandi* of those responsible, also utilising deception techniques to neutralise the threat. The gathered information is used in threat and risk assessments according to which the agency and the state can implement new defensive measures to further deter the threat.

Although counterintelligence also deals with certain crimes such as espionage, subversion and sabotage, it is rare for counterintelligence cases to be brought before the court in criminal proceedings. The focus is more on observing, exploiting and managing the threat than prosecuting the culprits. In most cases, the responsible agents are members of a foreign state intelligence service, often with diplomatic immunity, and prosecuting them would rarely bring the desired results. What is more certain is that any action against state agents, like naming certain individuals *persona non grata*, will be followed by similar steps from the opposing state. So-called 'tit for tat' retaliation or reciprocity is one of the main mechanisms that regulates and manages the behaviour of most countries and their diplomatic personnel in the international environment (Fakhoury, 2017). States' leadership must therefore often act wisely when foreign agents are discovered or need to assess their countries' global position, their international relations or economic and political interests.

In some respects, counterintelligence can be viewed similarly to investigations dealing with organised crime. Professionals will traditionally work backwards, from a crime or event up the operational chain, covertly mapping the organised networks and slowly building a case against them. To further illustrate, investigations of an organised criminal group or foreign intelligence service depend on surveillance of several transfers of illicit goods or 'stolen' sensitive information. The research is built slowly, gathering all the intelligence and, in the case of organised crime, also collecting relevant evidence that must meet the judicial system's evidentiary threshold. It would make no sense to use the same techniques in counterterrorism where the equivalent to a one-off drug shipment or stolen secret would be a single terrorist attack. But the whole aim of counterterrorism is to prevent that one attack, which should make it obvious that counterterrorism differs from counterintelligence and organised crime investigations. The key point here is that time can be an ally in counterintelligence. Yet this is not the case with counterterrorism, where the exact opposite is true. Time is an enemy and delaying action can prove fatal (Bauer, 2016).

Issues and rivalries also arise from different cultures within the police on one hand and intelligence and security services on the other. The role of intelligence is to collect and analyse intelligence, while the role of the police is to investigate and prevent crimes through prosecution. The former makes sense when dealing with foreign intelligence but not when a terrorist act is being planned or conducted, as the case of a German neo-Nazi group demonstrates[8]. The latter needs urgent interference and disruption, not time-consuming intelligence gathering and mapping of a whole network while lives are at stake. Bringing suspects in, questioning them and conducting thorough investigations may be more effective and could save lives.

According to Lutwak (2015), it all comes down to the question of methods, derived from one fundamental insight: "Terrorist actions cannot be anticipated and prevented – all such efforts are simply futile because there are just too many possible targets and infinity of possible dates. Nor can one hope to detect even imminent attacks because terrorists need not reveal themselves until it is too late". Surveillance of all suspects, who in some countries can be quite numerous[9], is practically impossible as that would take up a significant number of personnel and resources. Further, the most intrusive surveillance methods in western liberal

[8] *For example, from 2000 to 2007 Germany witnessed a series of murders of migrants committed by a neo-Nazi group. Germany's security service had the group under surveillance. However, members of the group were able to conduct ten murders in the period when the service had paid informants who were also close to the perpetrators. The agency had known the leading culprits and their organisation had been known to them since the early 1990s, but they failed to share information with the police, who were investigating these crimes. Besides institutional failure in sharing information, there is also the issue of rivalry between the intelligence and security services and the police (McGowan, 2014).*

[9] *For example, according to French authorities in 2016 around 20,000 people represented a security risk in France (Peter, 2016).*

democracies are usually legally restrained in scope and duration. In the case of counterterrorism, the solution is to bring down the number of relevant suspects to a manageable size, and taking action the moment the first indications of potential involvement in terrorism come to light, as is the case with Italy[10]. The issue is that most European countries' intelligence and security services have included counterterrorism in their intelligence and counterintelligence framework (Bauer, 2016) where they tend to prolong the surveillance of suspects and write multiple reports and assessments for policymakers. This is appropriate for pure intelligence work, somewhat less so for counterintelligence, and not at all for counterterrorism.

3.3 Risks, Time Sensitivity and Sharing of Information

There is a large qualitative gap between the risks pertaining to unsuccessful counterintelligence and counterterrorism efforts. In the case of counterintelligence, the primary imminent risk is the loss of information, meaning sensitive information or secrets that enable a state to function or stay ahead of other states, especially hostile ones. This risk varies regarding the level of competition and hostility in the environment (Britovšek, 2017). On the other hand, failure in counterterrorism holds imminent risks for lives and property. Loss of information can in some cases lead to the loss of life but usually in the context of a war or as an indirect consequence. There are, however, considerably fewer traumas compared to terrorism where there may be a direct loss of lives, especially civilians'. The latter can trigger drastic changes in policy as seen in the examples of increased surveillance and wars in Afghanistan and Iraq (Adams, Nordhaus, & Shellenberger, 2011), while failure to protect secrets, although damaging, typically does not have the same drastic impact on policy.

The need to act upon threats is therefore more urgent in counterterrorism than in counterintelligence because there is exposure to a greater imminent risk, namely the loss of lives. Consequently, to ensure proactive counterterrorism it is essential to fuse the 'law enforcement model' and 'intelligence model' by for example identifying dangerous people, profiling, surveillance, intelligence-led policing, sting operations and preventative detention (Crelinsten, 2014). Urgency also brings forward the 'need to share' principle in counterterrorism, which lies in contrast to counterintelligence dealing with foreign governments where secrecy is of the outmost importance and where the 'need to know' principle prevails.

There is a constant conflict between the need to balance the 'need to know' and 'need to share' principles in information-oriented organisations. The former notion is associated with who gains access to sensitive information and who does not. This essentially means ensuring that the right person has access to and insight

[10] *In most cases, a friend or an acquaintance would report a person that is bragging or speaking of carrying out or supporting violent attacks. What follows such a report is a thorough interrogation and investigation that reveal if there is any more to the initial indication. If a suspect's militancy is confirmed, they are held while investigators check additional records to build a criminal case as part of which they could arrest, try and imprison the suspect (Lutwak, 2015). Italy has also relied heavily on administrative measures. Thus far, one of the most successful counterterrorism measures, at least in the short to medium term, has been the deportation of foreign suspects in association with restrictive naturalisation laws (Marone, 2017).*

into certain information, which they need to perform their duties, and limited or no access to information they do not require (Best, 2011). This 'need to know' principle applies especially to counterintelligence since the protection of sensitive information is one of its crucial goals. The value of that principle rises along with the environment's level of competitiveness. The 'need to share' principle became prominent after the 9/11 terrorist attacks in the United States. The investigation of the handling of the attack found that 'stovepiping' and bureaucratic hoarding of information had contributed to a major counterterrorism failure (Miller, 2011).

However, the sharing of information also creates possibilities for leaks, which is a main concern of counterintelligence, particularly in the context of relations with other states. Counterterrorism, in dealing with protecting people's lives, unlike counterintelligence (which deals with protecting information), needs prompt, actionable and useable information. If both activities are conducted by the same organisation, tensions between these principles will arise which, if unresolved, can have a paralysing effect on a state's overall national security (Bauer, 2016; Miller, 2011). In addition, besides the mentioned lower evidentiary standards of intelligence, the 'need to know' principle leads to secrecy and the use of secret intelligence in courts can threaten the fairness of legal proceedings and make it more difficult to conduct prosecutions or hold governments accountable for misconduct (Roach, 2015).

4 OVERCOMING THE ISSUES AND PROPOSED SOLUTIONS

Considering the abovementioned differences and conflicts between counterintelligence and counterterrorism, issues emerge by virtue of most western countries assigning the tasks of counterterrorism to their agencies that have traditionally been involved in counterintelligence. To deal with these issues, we devised four principles to be considered while locating counterintelligence and counterterrorism within the organisational or institutional structure of a national security system. First, the 'intelligence model' is needed for identifying threats and assessing risks. Second, the 'law enforcement model' is needed for lawfully disrupting and prosecuting suspects. Third, the 'need to share' principle is essential in counterterrorism, while the 'need to know' principle is vital for counterintelligence. Finally, time is immensely important for counterterrorism, but less important in counterintelligence.

In accordance with these principles, some organisational solutions are presented. When dealing with organisational and institutional issues, we propose the separation of counterintelligence and counterterrorism at the state level; leaving counterintelligence as part of the traditional security and intelligence structures and establishing a new agency to take the lead in and work exclusively on counterterrorism issues. The burden and constraints of counterintelligence at the state level would be lifted from this agency, meaning it could share information rapidly and freely, while counterintelligence would continue to focus on protecting sensitive information in relation to foreign intelligence threats. In the context of counterterrorism, the application of counterintelligence can then be applied as needed, usually with a limited scope, such as the operational security of ongoing investigations.

There is also an option to reform the current institutional structures. As most states have separate defence and interior ministries, it would be economical and sensible to separate responsibilities between these ministries, especially in smaller states. The ministry responsible for defence is responsible for defending the state from foreign threats, mainly foreign governments, their institutions and activities. It therefore makes sense to place state counterintelligence tasks with the defence ministry, or its security intelligence department. The tasks of counterterrorism would be left to the interior ministry or the state's civilian security and intelligence agencies[11]. The basic idea is that defence ministries provide defence against other states and the threats emanating from them, such as by intelligence gathering, while interior ministries or civilian intelligence and security agencies deal with the issue of terrorism as part of protecting public safety and fighting crime. Nonetheless, an umbrella organisation for information sharing, coordinating and de-conflicting activities would still likely be needed.

While the primary target of counterintelligence is not terrorism (and vice versa, the primary counterterrorism target is not a foreign intelligence service), their activities do sometimes overlap and the information collected can be of interest to agencies engaged in either role. As time-urgent information is needed more in counterterrorism, many countries have created 'counterterrorism centres' where information can be stored and accessed by different agencies (Riedel, 2016). For more comprehensive information exchange, de-confliction and coordination of various national security-related issues and activities, the creation of 'fusion centres' or 'information and coordination bodies' is also likely to be effective (Britovšek & Čretnik, 2016).

An important issue is the balance between the 'law enforcement model' and 'intelligence model', namely between intelligence and police powers. Here countries' strategies vary, with some trying to expand the 'intelligence model' and others trying to expand the 'law enforcement model'. But issues arise mainly from gathering intelligence and transforming it into evidence that can then be used in courts and the criminal justice system. One solution may be to combine intelligence and police powers within a single organisation. The need to merge the role of intelligence and law enforcement seems more apparent in counterterrorism than counterintelligence, where it has spurred the evolution of policing concepts and practices, such as into intelligence-led policing (Ratcliffe, 2016) or anticipative criminal investigations (Hirsch Ballin, 2012).

Although the Parliamentary Assembly of the Council of Europe (1999) recommended separating security intelligence tasks from those assigned to the police, a considerable number of liberal democracies still do not make this distinction (European Union Agency for Fundamental Rights, 2015; Vitkauskas 1999). Of course, the more power these agencies have, the more oversight, control and safety features the system must also incorporate. One such feature is different legislation covering constraints on surveillance versus criminal investigation. The oversight would need to be focused on the point where an intelligence-gathering activity transforms into a criminal investigation, so as to separate information

[11] *Although civilian security-intelligence agencies are often subordinated to the ministries of interior, there are instances where they are subordinated directly to the prime minister.*

derived from intelligence gathering versus from criminal investigations. The other solution, especially in the counterterrorism context, is a security service focused on gathering intelligence but with close cooperation with a special police unit responsible for sting operations, arrests and criminal investigation of suspects.

5 CONCLUSION

To sum up, counterintelligence and counterterrorism are both important parts of national security and, while they seem very similar at first glance, they do differ from each other in certain significant respects. They both lie on a spectrum between the 'law enforcement model' and the 'intelligence model', depending on the cultural, institutional and legal structures of a state, and depending on the environment and states' perception of threats. They can overlap in certain circumstances. In the context of the 'intelligence model', they both utilise surveillance and intelligence analysis, although in the 'law enforcement model', in the case of criminal investigations, threats are considered as criminal acts and information must be presented as evidence in courts. Another overlap exists when foreign states are involved in terrorism, or when non-state terrorist groups are involved in intelligence gathering.

Both counterintelligence and counterterrorism can be divided into defensive and proactive roles. The defensive role focuses on protecting sensitive information in the case of counterintelligence, and vulnerable targets in the case of counterterrorism. Measures can overlap but they more often differ due to the risks that arise from failure in each respective activity.

The focus on different threats also means dealing with different risks in the case of failure. The imminent risk in counterintelligence is the loss of information, while the imminent risk in counterterrorism is the loss of life. Other differences arise from these differences, such as the urgency of action, or time considerations. In the case of counterintelligence, time can be an ally, while in counterterrorism time is the enemy, meaning counterintelligence can take a longer time, study an opponent and enhance security measures, while counterterrorism must act swiftly in order to save lives.

This is where the principles of the 'need to know' (which is essential in counterintelligence) and the 'need to share' information (which is essential in counterterrorism) collide. The tension between these principles causes frictions and inefficiency when states' counterintelligence and counterterrorism are organised within the same institution. Dealing with foreign states is not the same as dealing with non-state groups or individuals, especially when the main aim of the latter is to cause as much physical harm as possible.

We therefore derived four principles that should be considered when implementing counterintelligence and counterterrorism in the states' national security systems: (1) the 'intelligence model' is needed for identifying threats and assessing risks; (2) the 'law enforcement model' is needed to lawfully disrupt and prosecute suspects; (3) the 'need to share' principle is essential in counterterrorism, while the 'need to know' principle is vital for counterintelligence; and (4) time is critical for counterterrorism, but less important in counterintelligence.

The main idea of these principles is to separate counterintelligence and counterterrorism at the state level. The first solution is to leave counterintelligence as part of the traditional intelligence and security services while establishing a new organisation to work exclusively on counterterrorism. The other solution and perhaps a more practical proposal, especially for smaller states, is for the defence ministry or its intelligence and security apparatus to take over the role and responsibilities of counterintelligence, while the interior ministry or civilian security service takes over the role and responsibilities of counterterrorism. Due to the hybridisation of threats and their frequent overlaps, coordination and information sharing among different services would remain vital. A coordinating umbrella body or 'fusion centre' would likely be needed to fulfil these tasks effectively.

To conclude, the most important aspect of developing and implementing the solutions presented in this paper is understanding the threats and organisational issues related to them. The need to share information, the urgency of action and the risks of failure differ between counterintelligence and counterterrorism and, while both activities have an important role to play in the overall national security system, their varying functions and characteristics must be recognised to create and develop an organisational and legal environment in which these roles can be fulfilled effectively and appropriately.

REFERENCES

Adams, N., Nordhaus, T., & Shellenberger, M. (2011). *Counterterrorism since 9/11: Evaluating the efficacy of controversial tactics*. Oakland: The Breakthrough Institute. Retrieved from https://thebreakthrough.org/images/pdfs/CCT_Report_revised-3-31-11a.pdf

Azani, E. (2013). The hybrid terrorist organization: Hezbollah as a case study. *Studies in Conflict & Terrorism, 36*(1), 899–916.

Bauer, A. (September 13, 2016). *Who is the enemy? Terrorism as an unidentified fighting object.* International Institute for Counter-Terrorism. Retrieved from https://www.ict.org.il/Article/1774/who-is-the-enemy-terrorism-as-an-unidentified-fighting-object#gsc.tab=0

Berkowitz, B. (February 2, 2003). The big difference between intelligence and evidence. *The Washington Post*. Retrieved from https://www.washingtonpost.com/archive/opinions/2003/02/02/the-big-difference-between-intelligence-and-evidence/b589df3b-b735-4c40-8177-b5358331a690/?utm_term=.cef76f231090

Best, A. R. (2011). *Intelligence information: Need-to-know vs. need-to-share*. Washington: U.S. Congressional Research Service. Retrieved from https://fas.org/sgp/crs/intel/R41848.pdf

Bigo, D., Carrera, S., Hernanz, N., & Scherrer, A. (2015). *National security and secret evidence in legislation and before the courts: Exploring the challenges* (CEPS Liberty and Security in Europe Papers, no. 78). Brussels: Centre for European Policy Studies. Retrieved from https://www.ceps.eu/system/files/No%2078%20National%20Security%20and%20Secret%20Evidence.pdf

Britovšek, J. (2017). *Zasebna obveščevalna dejavnost v Republiki Sloveniji – teoretični, pravni in praktični vidiki* [Private intelligence in the Republic of Slovenia – a theoretical, legal and practical perspectives] (Doctoral dissertation). Ljubljana: Fakulteta za varnostne vede.

Britovšek, J., & Čretnik, A. (2016). Obveščevalno-varnostni sistem Republike Slovenije: Reorganizacija in sistemske rešitve [Intelligence and security system of the Republic of Slovenia: Reorganisation and systemic solutions]. *Varstvoslovje, 18*(3), 325–348.

Britovšek, J., Sotlar, A., & Tičar, B. (2017). Private intelligence in the Republic of Slovenia: Theoretical, legal, and practical aspects. S*ecurity Journal, 31*(2), 410–427.

Crelinsten, R. (2014). Perspectives on counterterrorism: From stovepipes to a comprehensive approach. *Perspectives on Terrorism 8*(1), 1–14

Duvenage, P. C., & Von Solms, S. H. (2015). Cyber counterintelligence: Back to the future. *Journal of Information Warfare, 13*(4), 42–56.

Eijkman, Q., & van Ginkel, B. (2011). Compatible or incompatible: Intelligence and human rights in terrorist trials. *Amsterdam Law Review, 3*(4), 3–16.

European Union Agency for Fundamental Rights. (2015). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU*. Luxembourg: Publications Office of the European Union.

Fakhoury, A. (2017). Persona Non Grata: The obligation of diplomats to respect the laws and regulations of the hosting state. *Journal of Law, Policy and Globalization, 57*. Retrieved from http://www.iiste.org/Journals/index.php/JLPG/article/viewFile/35178/36182

Gleghorn, E. T. (2003). *Exposing the seams: The impetus for reforming U.S. counterintelligence* (Master's thesis). Monterey: Naval Postgraduate School.

Goitein, E., & Shapiro, M. D. (2011). *Reducing overclassification through accountability*. New York: Brennan Center for Justice. Retrieved from http://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/Brennan_Overclassification_Final.pdf

Harber, R. J. (2009). Unconventional spies: The counterintelligence threat from non-state actors. *International Journal of Intelligence and CounterIntelligence, 22*(2), 221–236.

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge: Cambridge University Press.

Hirsch Ballin, F. H. M. (2012). *Anticipative criminal investigation: Theory and counterterrorism practice in the Netherlands and the United States*. The Hague: T.M.C. Asser Press.

Hoffman, B. (2006). *Inside terrorism* (2nd ed.). New York: Columbia University Press.

Hulnick, S. A. (1997). Intelligence and law enforcement: The 'Spies Are Not Cops' problem. *International Journal of Intelligence and Counterintelligence, 10*(3), 269–286.

Liulevicius, G. V. (2011). *Espionage and covert operations: A global history*. Chantilly: The Teaching Company.

Lockwood, N. (December 23, 2011). How the Soviet Union transformed terrorism. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2011/12/how-the-soviet-union-transformed-terrorism/250433/

Lubin, A. (January 9, 2017). A new era of mass surveillance is emerging across Europe. *Just Security*. Retrieved from https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/

Lutwak, N. E. (December 17, 2015). Italy has lessons to teach in counterterrorism. *Nikkei Asian Review*. Retrieved from https://asia.nikkei.com/Politics/Edward-N.-Luttwak-Italy-has-lessons-to-teach-in-counterterrorism

Marone, F. (March 13, 2017). *The use of deportation in counter-terrorism: Insights from the Italian case.* The Hague: The International Centre for Counter-Terrorism. Retrieved from https://icct.nl/publication/the-use-of-deportation-in-counter-terrorism-insights-from-the-italian-case/

McGowan, L. (2014). Right-wing violence in Germany: Assessing the objectives, personalities and terror trail of the national socialist underground and the state's response to it. *German Politics, 23*(3), 196–212.

Miller, H. B. (2011). Commentary, The death of secrecy: Need to know . . . with whom to share. *Studies in Intelligence, 55*(3). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-3/the-death-of-secrecy-need-to-know...with-whom-to-share.html

Mobley, W. B. (2012). *Terrorism and counterintelligence: How terrorist groups elude detection*. New York: Columbia University Press.

Parliamentary Assembly of the Council of Europe. (1999). *Control of internal security services in council of Europe member states*. Strasbourg: Council of Europe. Retrieved from http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en

Pedahzur, A. (2009). *The Israeli Secret Services and the struggle against terrorism*. New York: Columbia University Press.

Peter, L. (July 26, 2016). How France is wrestling with jihadist terror. *The BBC*. Retrieved from http://www.bbc.co.uk/news/world-europe-36902332

Podbregar, I., & Ivanuša, T. (Eds.). (2016). *The anatomy of counterintelligence: European perspective.* Sharjah: Bentham Science.

Priest, D. (November 13, 2017). Russia's election meddling is another American intelligence failure. *The New Yorker*. Retrieved from https://www.newyorker.com/news/news-desk/russias-election-meddling-is-another-american-intelligence-failure

Prunckun, H. (2012). *Counterintelligence theory and practice*. Lanham: Rowman and Littlefield.

Prunckun, H. (2014). Extending the theoretical structure of intelligence to counterintelligence. *Salus Journal, 2*(2), 31–49.

Ramsay, G. (2015). Why terrorism can, but should not be defined. *Critical Studies on Terrorism, 8*(2), 211–228.

Ratcliffe, H. R. (2016). *Intelligence-led policing* (2nd ed.). London; New York: Routledge.

Richards, A. (2014). Conceptualizing terrorism. *Studies in Conflict and Terrorism, 37*(3), 213–236.

Riedel, B. (July 18, 2016). France needs its own National Counterterrorism Center. *Brookings.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2016/07/18/france-needs-its-own-national-counterterrorism-center/

Roach, K. (2015). Introduction: Comparative counter-terrorism law comes of age. In K. Roach (Ed.), *Comparative counter-terrorism law* (pp. 1–45). Cambridge: Cambridge University.

Schmid, A. (2004). Terrorism: The definitional problem. *Case Western Journal of International Law, 36*(2), 375–419.

Treverton, F. G. (2009). *Intelligence for an age of terror*. Cambridge; New York: University Press.

Van Cleave, K. M., (2013). What is counterintelligence? A guide to thinking and teaching about CI. *The Intelligencer, 20*(2), 57–65.

Vandepeer, C. (2011). *Intelligence analysis and threat assessment: Towards a more comprehensive model of threat*. Perth: Edith Cowan University. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1020&context=asi

Vitkauskas, D. (1999). *The role of a security intelligence service in a democracy*. North Atlantic Treaty Organisation. Retrieved from https://www.nato.int/acad/fellow/97-99/vitkauskas.pdf

Warner, M. (2002). Wanted: A definition of 'intelligence'. Understanding our craft. *Studies in Intelligence, 46*(3). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html

Warner, M. (2014). *The rise and fall of intelligence: A international security history*. Washington: Georgetown University Press.

Weinberg, L., Pedahzur, A., & Hirsch-Hoefler, S. (2004). The challenges of conceptualizing terrorism. *Terrorism and Political Violence, 16*(4), 777–794.

About the Author:

Jaroš Britovšek, PhD, is employed by the Ministry of Defence of the Republic of Slovenia. E-mail: jaros.britovsek@mors.si

VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 20
no. 2
pp. 182–201

Male Sex Work in Slovenia[1]

Monika Klun, Matevž Bren

Purpose:

The aim of this paper is to determine whether male sex work in Slovenia exists, if there are statistically significant differences in sexual orientation between male sex workers in Slovenia and men who do not engage in this type of work, and whether any factors (i.e. sexual orientation, dysfunctional family etc.) exist that can be used as predictive criteria for such behaviour.

Design/Methods/Approach:

In the first part, we used a descriptive method and in the second an empirical method. We conducted an online survey which included male sex workers and men who do not engage in this type of work. We used descriptive statistics, a chi-square test, and factor and discriminant analyses. The data collected were analysed using the SPSS program. We discussed the research results with some respondents and Dr Iztok Šori, a researcher at the Slovenian Peace Institute – Institute for Contemporary Social and Political Studies.

Findings:

Male sex work exists in Slovenia. Such workers generally define themselves as homosexual or bisexual. Among male sex workers and men who do not engage in this type of work, there are no significant differences in the socialisation process (in terms of a dysfunctional family background). In most cases, they come from functional families.

Research Limitations/Implications:

The limitation of our research is the small sample size. It is therefore questionable whether the findings can be generalised from the sample to the entire population.

Practical Implications:

Male sex work is clearly a part of Slovenian society. This should be taken into consideration while establishing policies and practices in the field of sex workers' protection and, in particular, with regard to destigmatising sex work in Slovenia.

Originality/Value:

Dealing with the comparison of male sex workers and men who are not engaged in this type of work, our study is one of the first of its kind in Slovenia. It may be seen as a starting point for future empirical studies that deal only with male sex workers.

UDC: 343.544-055.1(497.4)

Keywords: male sex work, sexual orientation, dysfunctional family, stigmatisation

[1] *This research work started in the framework of a research project within the subject »Methodology of social science research and multivariate statistical methods« in the second year of postgraduate study at the Faculty of Criminal Justice and Security.*

Moško spolno delo v Sloveniji

Namen prispevka:

Cilj prispevka je ugotoviti: ali moško spolno delo v Sloveniji obstaja, ali obstajajo statistično pomembne razlike v spolni usmerjenosti med moškimi spolnimi delavci v Sloveniji in moškimi, ki se s tovrstnim delom ne ukvarjajo, ter ali obstajajo dejavniki tveganja, ki ločujejo med preučevanima skupinama.

Metode:

V prvem delu smo uporabili deskriptivno, v drugem delu pa empirično metodo. Izvedena je bila spletna anketa, sodelovali so tako moški spolni delavci kot moški, ki se s tem delom ne ukvarjajo. Uporabili smo opisno statistiko, hi-kvadrat test ter faktorsko in diskriminantno analizo. Vse analize smo izvedli s programom SPSS 22.0. O rezultatih raziskave smo prek elektronske pošte razpravljali z nekaterimi respondenti in raziskovalcem na Mirovnem inštitutu – Inštitutu za sodobne družbene in politične študije dr. Iztokom Šorijem.

Ugotovitve:

Moško spolno delo je prisotno tudi v Sloveniji. Tovrstni delavci se po večini opredeljujejo kot geji ali biseksualci. Med moškimi spolnimi delavci in moškimi, ki se s tem delom ne ukvarjajo, ni bistvenih razlik v socializacijskem procesu (disfunkcionalnosti družin). V večini namreč oboji prihajajo iz urejenih družin.

Omejitve/uporabnost raziskave:

Omejitev svojega dela vidimo predvsem v majhnosti vzorca. Sklep iz vzorca na populacijo je zato lahko vprašljiv.

Praktična uporabnost:

Moško spolno delo je nesporno del tudi slovenske družbe, česar se je treba zavedati pri ustvarjanju politik in prakse na področju zaščite spolnih delavcev in predvsem v smeri destigmatizacije spolnega dela.

Izvirnost/Pomembnost prispevka:

V Sloveniji še ni bilo raziskave, ki bi obravnavala primerjavo moških spolnih delavcev in moških, ki tovrstnega dela ne izvajajo. Prispevek je mogoče razumeti kot izhodišče za empirično študijo v prihodnosti, ki bi obravnavala zgolj moške spolne delavce.

UDK: 343.544-055.1(497.4)

Ključne besede: moško spolno delo, spolna usmerjenost, disfunkcionalna družina, stigmatizacija

1 INTRODUCTION

Adherents of radical feminism argue that prostitution is mainly a form of male dominance over women. It is often believed that women (prostitutes) are the sole providers of sexual services, yet this activity is also performed by men (Weitzer, 2005).

Weitzer (2005) therefore claims that sex work can be differentiated by gender (male and female sex work). For the men who perform this type of work, it is namely typical that they perform it only occasionally and that they stop the period of their work activity earlier than female sex workers. Male sex workers tend to be more mobile across types of such work. It is typical for male sex workers to start, for instance, as masseurs, then they become escorts and later on they advertise themselves and become call boys (Weitzer, 2005). Boyer (1989) adds that male sex workers are more frequently forced to define their sexual orientation than female sex workers. This refers to questions that demand they define themselves as homo-, hetero-, trans- or bi-sexual.

Yet, Van der Poel (1992) does not agree with the arguments concerning gender-based differences in this line of work, stating that they are not sufficiently supported by evidence. Weitzer (2005), on the other hand, stands in contrast to Van der Poel (1992) by claiming that nearly all sex-work-related literature is divided into studies of men and women, with almost no systematic comparative view on men and women at the level of their work. Besides that, research studies that do not consider such comparisons reveal objective differences according to the type of work, with these differences representing the characteristics that can be found in studies of female sex work (West & de Villiers, 1993).

Up until the 1990s, the attention paid to sex work in literature was mainly given to female sex workers (Vanwesenbeeck, 2012), even though it is documented that the 'world's oldest profession' or line of work has also been carried out by men from Roman and Greek history and Victorian England until today (Bimbi, 2007). Several factors have contributed to the lack of legal and political discussions, knowledge and studies in connection with male sex workers. At the global level, the share of male sex workers is smaller than the share of female sex workers (Vanwesenbeeck, 2012). Leichtentritt and Davidson Arad (2005) claim that the information on the share of male sex workers is not valid because it is unknown whether this type of information reflects the reality or denial of this type of work. In addition, the men involved in this line of work are an elusive and vulnerable group of people. They purposefully eliminate themselves from discussions as they do not correspond to the 'ideal' image of sex work. Such an image is namely linked to the exploitation of women and violence against them, therefore men in this group do not 'fit' the stereotypical image of the female victim who needs to be rescued from sex work (Global Network of Sex Work Project [NSWP], 2014).

Another reason for the ignoring and stigmatising of male sex workers lies in the nature of their work. Generally speaking, they are seen as bisexually or homosexually oriented men (Koken, Bimbi, Parsons, & Halkitis, 2004), whereby we should take into consideration that in the middle of the 20th century homosexuality was still looked upon as a mental disease (Bimbi, 2007),and even today is still regarded as such in some parts of the world. Such men are pushed away from gay society as well as from the sex workers' community (Popov, 2008) and they are also discriminated against and persecuted by law enforcement authorities (NSWP, 2014). In this context, we can thus talk about double or multi-layered stigmatisation (sex workers and homosexuals) and about a deliberately overlooked phenomenon (Popov, 2008).

In society, male sex work is a taboo subject also because this type of worker faces additional social stigma. Consequently, and connected to this phenomenon, the adoption of legal acts often hinders male sex workers' access to healthcare and social services (Grimes, 2001). Also not to be overlooked are the theories of deviation which explain that male sex workers engage in this type of work due to inner or environmental pathologies (Koken et al., 2004). The claim that homosexual male sex workers are (were) the reason for the spread of the HIV infection (Vanwesenbeeck, 2012) is an additional factor showing that male sex work finds itself in a disadvantaged position compared to female sex work and has been pushed away into the remotest parts of the social bottom (Popov, 2008).

In Slovenia, women (Šori, 2005) as well as men are engaged in sex work (Pajnik & Kavčič, 2008). The indicators of active male sex work in Slovenia can be spotted in advertisements, magazines and newspapers, which also increase their revenue by advertising sexual offers. The advertising of such offers can also be found on various websites that advertise private contacts. In spite of these facts, male sex work has not been scientifically/professionally researched in Slovenia (Popov, 2008). The reasons for this may be found in the issues of anonymity and the lack of researchers' interest in male sex workers in contrast to female sex workers (Pajnik, 2008). Another reason for the lack of research in this field is that stigmatisation is contagious, meaning that part of the stigma can be transferred to the researchers too (Popov, 2008). Maybe the exact reasons no longer apply and we are able to overcome them. These are the reasons underpinning our research in which we compared the socio-psychological characteristics of male sex workers in comparison with men who do not perform this type of work. More specifically, we focused on the dysfunctionality of their (nuclear) families and on their sexual orientation.

The following three hypotheses arise from the above stated objectives:

Hypothesis 1: In Slovenia, male sex work exists.

Hypothesis 2: There are statistically significant differences in sexual orientation between male sex workers and men who do not perform this type of work.

Hypothesis 3: Standpoints on their (dysfunctional) families differ among sex workers and men who do not perform this type of work.

In respect of the contents, the hypotheses are based on the facts set out in the introductory section, whereas the wording of the hypotheses was dictated by the results of research performed by Earls and David (1989), Bar-Johnson and Weiss (2015), Abdullah Avais, Wassan, Chandio and Balouch (2014) and Minichiello et al. (2002). Within the framework of the discussion and interpretation, our research results will be compared with the results of this research and professional opinions. The results of our research were discussed by e-mail with Dr Iztok Šori, a researcher at Peace Institute – Institute for Contemporary Social and Political Studies, and some participants of our research. Dr Iztok Šori is interested in the connection between gender, migration and work, which he explores in the frame of various social fields (sex work, politics, private life). He has participated in several research projects focusing on gender equality, political representation and emancipation, prostitution, human trafficking, racism, populism, migration and lifestyles.

In the following chapters, we provide a comprehensive review of the literature on the factors that influence the decision to commence sex work. We also explore the history of scientific research of male sex work around the world and in Slovenia. In the Methods section, we describe the target population, the sample and the data collection. We also present how the questionnaire was designed as well as the content of its parts. As part of the Results, we try to determine once again whether male sex work in Slovenia exists. We explore whether statistically significant differences exist in sexual orientation among male sex workers and men not performing this type of work in Slovenia. We try to establish whether there are risk factors which distinguish male sex workers from men who do not perform this type of work. At the end in the Discussion section, we verify the posed hypotheses and place our results in the current context of research on male sex work. We conclude by discussing options to reduce the stigmatisation of male sex work in Slovenia.

2 SCIENTIFIC RESEARCH ON MALE SEX WORK

2.1 Scientific Research on Male Sex Work Across the World

Scientific research on male sex work started between 1940 and 1970. The first studies of this kind were carried out in the United States and in the United Kingdom during the 1940s and 1950s. The early studies chiefly addressed the factors of the provision of male sex work, their typology, sexual identity and courses of treatment (Kaye, 2003). In both countries, homosexuals were treated as a problematic segment of the population. The discussion about homosexuality started, influencing the manner in which the studies on sex work were conducted (Bimbi, 2007). From the 1960s until the early 1970s, male sex work was presented in studies from the bio-psychological perspective. These studies were conducted by psychologists who focused on the search for the psychopathological traits of sex workers and researching their social environment. In this way, they uncovered the predisposing factors which were supposed to lead a person into sex work. These factors were connected to their personality traits, genetic make-up, learnt behaviour or socialisation processes at home or at school (Caukins & Coombs, 1976; Reiss, 1961). The majority of studies addressed male sex work in the context of bio-sociological positivist explanations (Browne & Minichiello, 1996). The male sex worker was presented as a »helpless victim, the result of personality deficits and a traumatic childhood, or of the bad economic conditions that lead into anxiety, sex work and hatred« (Davies & Feldman, 1997, p. 33).

Minichiello, Scott and Callander (2013, p. 266) state that male sex workers were labelled in the epidemiological literature as »reservoirs of disease and the vector of disease for the 'innocent' population of the 'heterosexual world'«. The rationale for this association was grounded in the notion that both prostitutes and homosexuals constituted 'risk groups'. In the early years of the HIV epidemic it was thought that the sexual networks of sex workers made them a risk for transmitting HIV to other populations. During this period, the role of alcohol and drugs was portrayed as occupying an inordinate level of importance in male sex workers' lives (Browne & Minichiello, 1996). It should be emphasised that many studies from this period focused on outdoor sex workers. Today, much research questions the notion of male sex workers as vectors of disease transmission (Minichiello et al., 2013).

2.2 Scientific Research on Male Sex Work in Slovenia

While the question of offering efficient help and counselling to female sex workers has already been addressed abroad, in Slovenia such changes and thinking in this direction seem to appear with a time lag. This is connected to the traditional social structure and the former political ideological system. In the previous socialist society, prostitution was namely defined as an unacceptable form of sexuality (Zaviršek, 1993).

The first publications on this topic date back to the 1960s, to the study by Kobal and Bavcon (1969), the case of the socio-pathological treatment of prostitution. Their study dealt with female prostitution and in the introduction they mentioned the reason for that is the fact that male prostitution is only occasional or seasonal.

Over the next few decades, publications on prostitution were relatively rare and they only re-emerged in the 1990s, whereas the first research on human trafficking and prostitution emerged after the year 2000 (Pajnik, 2008). We can claim that in Slovenia criminology and criminal law studies on prostitution and on human trafficking have prevailed in scientific publications (Kanduč, 1998; Petrovec, 2000). Tratnik Volasko (1996) discussed some of the basic characteristics of prostitution in Slovenia and talked about prostitution from the legislative and monitoring points of view. She established that street prostitution in Slovenia does not exist. In this context, she established that male prostitution also exists in Slovenia and that homosexual prostitution encounters took place in the environment of the traditional meeting places of these groups, particularly around the bus and train stations, in gay clubs and via advertising. Similarly, in his discussion Petrovec (2000) also focused on the social aspects of prostitution.

In her work, Pajnik (2008) also writes about male sex work from the viewpoint of a unique or dualistic concept of prostitution. She argues that whereas unique concepts of prostitution draw attention to certain dimensions of prostitution, they do not address its diversity and inconsistency. She claims that such a concept is inappropriate because it excludes secondary phenomena in prostitution such as, for instance, prostitution of men who accept women as their clients, same-sex prostitution or transsexual prostitution.

Further on, when reviewing court documentation for the period between 2001-2005, Pajnik and Kavčič (2008) established that male sex workers did not appear in judicial processes, but in the evidence for two court cases they found the records of a massage agency and a real-estate agency that also offered male prostitution.

Pajnik and Šori (2014) analysed 44 websites of individual and organised providers (male and female) of sex work in Slovenia. They established that the visual materials found on the websites confirmed the characteristic differences between the sexes. The share of male sexual workers presented on these sites was much smaller than the share of female sex workers. This especially holds true for websites which advertise nightclubs/bars, escort services or erotic massage.

We can conclude that it would be unjustified to assume that at the start of scientific research on prostitution in Slovenia male prostitution was not known. But we can assert that, in scientific research, male sex work was mentioned later than female sex work. Based on these findings, we may conclude that even at the beginning of scientific research prostitution was particularised (female and male) but, due to its rarity, the latter did not receive considerable attention in Slovenian literature. We have not come across any research that narrowly focused on empirical research of male sex work, as can be seen from the mentioned social or psychological dimensions of female sex work.

2.3 Typology of Male Sex Workers

Caukins and Coombs (1976) claim that a hierarchy exists in the field of male sex work. The lowest level is represented by street sex workers who receive the lowest payment for their sexual services. These are followed by sex workers in bars and call boys. Male sex workers are, generally speaking, classified according to their place of work and, consequently, the type of services they provide as: street sex workers; prostitutes (gigolos); bar dancers, erotic dancers; escorts; theatre actors; models and erotic masseurs (Browne & Minichiello, 1996). Lucas (2004), in addition, also puts peer sex workers in this typology. With the development of technology, we have also witnessed male escorts who advertise their sexual services online (Parsons, Bimbi, & Halkitis, 2001). Generally speaking, research studies focus predominantly on street sex workers, the ones working in bars, and call boys, even though the majority of male sex workers work through agencies or by means of their own advertising. Little attention has been paid to other groups of sex workers such as masseurs, gigolos and models (Browne & Minichiello, 1996).

2.4 Some Factors of Male Sex Work

In this section, we discuss, with the help of a literature overview, some dilemmas concerning non-typical segments of male sex work. We address the questions of sexual orientation and sociological factors; more specifically, the dysfunctionality of families of birth. We also discuss some other (hedonic) factors associated with this type of work.

2.4.1 Sexual Orientation as a Factor of Commencing Male Sex Work

Boyer (1989) claims that homosexual orientation is one of the factors of engaging in sex work. Such work namely provides an identity and a way of conduct that meets the cultural image of homosexuality. Kong (2014) notes that male sexual workers report they can reveal their gay identity through their work. In their contact with their clients they can be utterly relaxed and freely show that they like to engage in sexual acts with same-sex partners.

An Australian study (Minichiello et al., 2002) showed that half the sample (n=185) of male sex workers identified themselves as gay, and 31% as bisexual. Similar results were shown by a study in Prague which included men who advertised their sexual services online (n=20), and male sex workers in gay bars and clubs (n=20). With regard to men who advertised their sexual services online, it was established that most defined themselves as homosexual or bisexual, whereas male sex workers in bars primarily defined themselves as heterosexual (Bar-Johnson & Weiss, 2015). In some countries, for instance in Mexico, homosexual identity is still stigmatised in society. Because male sex workers there deny or hide their homosexual orientation, they are, generally speaking, not stigmatised (Mednoza, 2014).

We may therefore conclude that social bias against homosexuality influences how male sex workers define their sexual orientation. We believe that this still reflects the influence of the social oppression of homosexuality throughout history. We can, however, assume that homosexuality is becoming less and less of a social taboo, whose strength of influence also depends on geographical area (urban/rural areas) and social class. Yet this assumption needs to be empirically proven.

2.4.2 Sociological Factors of Male Sex Workers

Timpson, Ross, Williams and Atkinson (2007) support the opinion that male sex workers often have a number of problems. These include escaping from home, and early school leaving, which leads to a lack of educational, social and employment skills. They also note it is typical that such men live(d) in dysfunctional families or are homeless.

Based on a study of 50 male sex workers, Earls and David (1989) established that 60% of them reported they were sexually abused in childhood. The findings of Earls and David (1989) suggest that such children are up to eight times more likely to become involved in male sex street work than those who are not victims of childhood sexual abuse (Wilson & Widom, 2010).

A study of male sex workers in Larkana (n=37) by Abdullah Avais et al., (2014) shows that 84% of the respondents reported sexual abuse in their childhood; 86% of them reported physical abuse, and 78% of them emotional abuse. Lankenau, Clatts, Welle, Goldsamt and Gwadz (2005) claim that young boys probably would not have become male sex workers had they only been given family support in their childhood and if they had not lived in dysfunctional families.

A study conducted in Prague revealed differences among male sex workers in bars and clubs (n=20) and male online sex workers (n=20). The results show that male online sex workers more frequently grew up with both of their parents than sex workers in bar and clubs. The latter were less likely to have had a happy childhood and less likely to have good relationships with their parents than male online sex workers (Bar-Johnson & Weiss, 2015).

On the other hand (Earls & David, 1989), male sex workers were presented as mentally stable individuals who performed sex work as a professional choice out of rational/economic reasons. Male sex workers are namely no less educated and there is no higher probability of them having grown up in a dysfunctional family than men who do not engage in this type of work. Their findings also suggest that childhood abuse has a smaller impact on their becoming involved in sex work than, for instance, factors like financial benefits, sexual orientation (homosexuality) and early sexual experience.

Such contradictory descriptions can emerge from different groups of male sex workers being included in studies and on which particular (theoretical) premises the studies were based. Namely, the studies which show male sex work as »deviant« and »punishable« in comparison with the studies that treat this kind of work as a personal choice make contradictory findings. For example, among street sex workers it can come to a cyclic relationship between motivation for starting this type of work, poverty, drug addiction and homelessness. On the other hand, male escorts who enjoy the lifestyle of the middle social and economic class can engage in sex work to support their desire for a more luxurious lifestyle (Browne & Minichiello, 1996). Moreover, certain studies (Abdullah Avais et al., 2014; Bar-Johnson & Weiss, 2015; Earls & David, 1989) are based on small and non-representative samples (the snowball sampling method), rendering their conclusions about this segment of the population questionable. Browne and Minichiello (1996) explain that even though certain male sex workers can fit the negative stereotypes, these cannot be generalised to all men who engage in male sex work. Such representations tend to overlook a broader structural understanding of prostitution and worsen the cultural and political standing of male sex workers (Browne & Minichiello, 1996).

2.4.3 Hedonic Factors for Commencing Male Sex Work

One theory about the factors that lead to male sex work is the socio-cognitive theory by Bandura (1978). This theory offers a broader view of how to explain male sex work without pathological assumptions (Smith, Grov, Seal, & McCall, 2013). Whereas in the USA (Smith et al., 2013) only 10% of the participants (n=38) perform sex work for material benefits (e.g. clothing, electronic devices, cars), in both Dublin and San Francisco a large majority i.e. 93% of the participants (n=23) stated financial profit as the primary reason for engaging in this type of work with which they are otherwise supposed to finance the purchase of drugs (Mc Cabe et al., 2014). This is similar to the findings of the mentioned research in Prague (Bar-Johnson & Weiss, 2015) in which 90% of the participants (n=20) reported their main reason for engaging in this type of work was a financial crisis. In Prague, men start this type of work also due to compassion for their families (to provide money for their families, to save their families from material and financial deprivation), out of a search for loving partnership relationships, the need for security or socialising, the desire to make their partner jealous or by way of seeking revenge on him (McCajor Hall, 2007). The reasons for entering into male sex work also include gaining higher self-esteem (Kong, 2014), the lack of (well-paying) jobs and the pressure of family members (United Nations Office for Drugs and Crime, 2007).

Financial gains are therefore the only feature that describes the male sex worker as a worker who is subject to the same rights as workers in other professions. In this way, sex work is equal to any other type of work and not a consequence of (traumatic) childhood experience (Browne & Minichiello, 1996). Therefore, we can talk about a crime-preventing effect of sex work. Criminal acts such as thefts can thereby be prevented (Kaye, 2003). This finding is related to a comment by one participant in the research conducted by Kuhar and Pajnik (in press): "OK, I would not kill for money, but I would steal".

3 METHODS

In our research, we conducted an online survey and used snowball sampling. In order to analyse the data required to verify the hypotheses, univariate, bivariate and two multivariate statistical methods were used. In checking the first hypothesis, only frequencies were calculated, while in the second hypothesis a chi-square test was employed. In order to verify the third hypothesis, factor and discriminant analyses were carried out.

3.1 Description of the Population, Sampling and Data Collection

The target population included all male sex workers and men who do not engage in this type of work. Spatially, our studied population refers to Slovenia while the time period for the data collection was December 2017. The sample consisted of 53 individuals who answered the entire questionnaire, and of 20 individuals who interrupted their participation and answered only part of the questionnaire. Data were collected via an e-survey. The questionnaire was published using the online tool 1KA. Contacts with prospective respondents were made from 10 August 2017; future respondents were informed of the survey and invited to participate. In the 'pre-phase' of the research, it remained an open question whether anyone would be willing to cooperate, and if the response would be sufficient to successfully carry out the research. On the 'public chatroom' on the website "avanture.net", we gave an incentive to complete an online anonymous survey to respondents who are men who considered themselves as male sex workers. Due to the lack of response, male portal users who were promoting sexual services online were invited to a 'private chat'. They were informed of our goals and we exchanged email addresses with the interested prospective research participants. They were subsequently asked to forward our enquiries to their acquaintances. The data were collected between 1 and 18 December 2017. A web link to the survey was sent to the previously informed participants from the "avanture.net" website. Many of the men who were initially interested in co-operating had changed their mind. Due to the insufficient sample, the link to the survey was repeatedly forwarded to the 'public chatroom' on the portal and to 'private chats' with men who advertised sexual services on the "erodate.com" website. Since the selection of units for the sample was not probabilistic, and therefore each population unit did not have the same probability of selection, the sample is not random. Therefore, the results obtained cannot be generalised to the population without reservation. The sample was collected through the non-probability method of snowball sampling. On the websites we visited, we also found men who had not engaged in sex work so these respondents were also obtained from the aforementioned websites.

3.2 Description of the Sample

Our sample consisted of 73 respondents, 33 (45.2%) of whom reported that they performed male sex work, and of 40 respondents (54.8%) who did not perform this type of work (see Table 1). Table 2 shows that the majority, that is 39 respondents, who perform male sex work (57.5%), reported having completed secondary school, and a minority reported holding a master's degree (12.5%). The majority (49%) of men who were not engaged in such work reported having completed secondary school, and a minority (12%) reported having a master's degree. The age of the participants was not important for our study so the participants were not asked about it. The respondents (homosexual male sex workers) also were not asked whether they offer their services to homo- or bi-sexual men or women as well. In addition, their clientele were not included in our sample. Namely, this was not the subject of our research.

Table 1: Descriptive statistics*

Which statement applies to you?	Frequency	Percentage
I perform male sex work	33	45.2
I do not perform male sex work	40	54.8
Total	**73**	**100.0**

Descriptive statistics of the sample: Which statement applies to you?

Table 2: Descriptive statistics of the sample: Education

Which statement applies to you? Education			Frequency	Percentage
I perform male sex work	Valid	Secondary school	16	48.5
		Undergraduate	6	18.2
		Master's degree	4	12.1
		Total	**26**	**78.8**
I do not perform male sex work	Valid	Secondary school	23	57.5
		Undergraduate	4	10.0
		Master's degree	5	12.5
		Total	**32**	**80.0**

3.3 Description of the Questionnaire

The questionnaire consists of 15 questions that measure 43 variables. The aspects included in the questionnaire were determined based on the theoretical premises of the problem. The first set of questions, comprising 16 variables, related to the dysfunctionality of the family of birth. The variables were measured on a five-level Likert scale (1 – I strongly disagree, 2 – I disagree, 3 – I partly agree, partly disagree, 4 – I agree, 5 – I strongly agree). The questions were compiled with the help of the research by Earls and David (1989) in combination with the surveys conducted in Larkana (Abdullah Avais et al., 2014) and Prague (Bar-Johnson & Weiss, 2015).

The second set of questions relates to drug and alcohol addiction and includes four variables. These were also measured on a five-level scale (1 – I am not addicted at all, 2 – I am not addicted, 3 – I am partially addicted, partially not addicted, 4 – I am addicted, 5 – I am severely addicted). The third set contained questions on the frequency of consuming drugs and alcohol. All four variables of this set were also measured on a five-level scale (1 – never, 2 – less than once a week, 3 – once a week, 4 – more than once a week, 5 – daily). The questions in the second and third sets were compiled by combining the studies by Minichiello et al. (2002) and Bar-Johnson and Weiss (2015).

The last three sets of questions contain eight variables, all of which were measured on a five-level Likert scale of agreement (1 – I strongly disagree, 2 – I disagree, 3 – I partly agree, partly disagree, 4 – I agree, 5 – I strongly agree). With regard to the contents, the questions referred to financial stability, early sexual experience and the educational process. This part of the questions was summarised according to the study by Earls and David (1989). In order to gain a better insight into the content, we finally asked five open questions about the perception of stigmatisation and the rights of male sex workers in Slovenia. We translated certain parts of questionnaires from foreign studies. The variables were determined by not including the entire dimension from particular studies. Certain statements reflected the characteristics of male sex workers in Australia, Larkana and the Netherlands, where, in our opinion, the characteristics of sex work differ from those in Slovenia.

For the reliability test, we used Cronbach's coefficient α, which measures the reliability of the questionnaire based on the correlations between the variables (Šifrer & Bren, 2011). The questionnaire's reliability was tested for the set "Dysfunctionality of the Family", which included "General Dysfunctionality" and "Abuse in the Family". Coefficient α for the set "General Dysfunctionality", which contains six variables, is 0.871. The "Abuse in the Family" set contains two variables, and Cronbach's alpha is 0.821.

All analyses of the collected data were carried out using the IBM SPSS Statistics version 22 SW package.

4 RESULTS

4.1 Descriptive Statistics

Table 1 shows that most respondents who reported performing sex work were bisexual (52%). The majority of respondents who did not perform sex work, however, defined themselves as heterosexual (85%).

Table 3: Descriptive statistics – sexual orientation

Which statement applies to you? / Sexual orientation		Frequency	Percentage
I perform male sex work	Homosexual	4	12.1
	Heterosexual	12	36.4
	Bisexual	17	51.5
	Total	**33**	**100**
I do not perform male sex work	Homosexual	1	2.5
	Heterosexual	34	85
	Bisexual	5	12.5
	Total	**40**	**100**

From the set of questions relating to dysfunctionality of the family, we found that all of the variables (measured on a five-level scale from 1 – I strongly disagree to 5 – I strongly agree) had an average value of less than three. Men who reported performing male sex work had the highest average (2.62), which is still quite low, and in response to the statement "There were often quarrels in the family" they most often answered with "I disagree". The variable "There was heroin in the family" had the lowest average (1.37). The most frequent answer to the majority of the variables was "I strongly disagree". In the sample of men who were not engaged in sex work, the variable with the highest average (2.06) was the variable "Tobacco was often present in the family", whereas the lowest average (1.06) was seen for the variables: "Heroin was often present in the family", "Cocaine was often present in the family", and "I was a victim of drug problems in my family". In response to all of the variables, the respondents most frequently indicated "I strongly disagree".

Table 4 shows that the data on drug and alcohol addiction show that all variables have an average value of less than two or equalling two. Men who perform sex work state more often that they are addicted to the listed substances than men who do not engage in such work. Both men who perform sex work, and men who do not perform this type of work, reported they were most addicted to tobacco, and least addicted to heroin. The difference between the studied samples is that the men who do not perform this type of work have a more unified opinion on addiction to heroin than the men who perform such work.

Table 4: Descriptive statistics*

Assess your addiction to these substances		Alcohol	Tobacco	Marijuana	Cocaine	Heroin
I perform male sex work	N	27	27	27	27	27
	Average	1.70	2.00	1.56	1.44	1.37
	Standard deviation	.775	1.330	.974	.801	.884
I do not perform male sex work	N	33	33	34	33	33
	Average	1.48	1.64	1.56	1.06	1.00
	Standard deviation	.566	1.168	1.260	.348	.000

Descriptive statistics – addiction to substances (variables were measured on a five-level scale (1 – I am not addicted at all, 2 – I am not addicted, 3 – I am partially addicted, partially not addicted, 4 – I am addicted, 5 – I am severely addicted)

Men who perform sex work more often stated they are addicted to the listed substances than men not engaging in this type of work. Both men who perform sex work and men who do not perform such work reported they were most addicted to tobacco, and least addicted to heroin. The difference between the studied samples is that the men who do not perform this type of work have a more unified opinion on addiction to heroin than the men who perform such work.

4.2 Performing Male Sex Work and Sexual Orientation

We were interested in whether in Slovenia there are statistically significant differences in sexual orientation between male sex workers and men who do not perform this type of work. We set the following null and alternative hypotheses:

H_0: Sexual orientation is not related to male sex work.
H_1: Sexual orientation is related to male sex work.

Since both variables were measured at a nominal level, a chi-square test was performed. We had to combine the variables "bisexual" and "homosexual" as the expected frequencies were less than 5 (Brvar, 2007). The value of Pearson coefficient was 18.353 at one degree of freedom. The p-value was 0.000; therefore, the null hypothesis stating that sexual orientation is not related to male sex work was rejected, and we accepted the alternative one, namely that there is a relationship between those variables.

4.3 Different Types of Family Dysfunctionality

We were interested in whether male sex workers live(d) in more dysfunctional families than men who did not engage in this type of work. We checked the assumption with a discriminant analysis. Prior to that, we were interested in whether the variables can be reduced to factors that will reflect all the characteristics of these variables. We must point out a breach of the assumption about the sample size (Bren, 2017).

The calculation of asymmetry and kurtosis showed that values exceeded the limits of -3 and 3 for the variables: "Cocaine was often present in the family", "Heroin was often present in the family", "Tobacco was often present in the family", "Marijuana was often present in the family", "I was a victim of drug problems in my family", "I was a victim of alcohol problems in my family", and "I was a victim of sexual abuse". Therefore, these variables were excluded from further analysis. There was no multicollinearity among the variables (the value of the determinant was 0.005). The Kaiser-Meyer-Olkin measure of the sample's suitability was 0.807 and the p-value of Bartlett's test was 0.000. The sample suitability was therefore optimal and the correlation matrix was not the identity, meaning we were justified in performing a factor analysis (Šifrer & Bren, 2011).

With the principal axis factoring method, two factors were extracted (initial eigenvalues above 1) and with the Oblimin with the Kaiser normalisation rotation method we tried to optimise the factor analysis results. The first factor explained about 50% of the total variance, and the second almost 10%. The total explained variance of both factors was approximately 60%.

The first factor ("*General Dysfunctionality*") included the variables: "There were often quarrels in the family", "I had an unhappy childhood", "Alcohol was often present in the family", "When growing up, I at times quarrelled with my family members so seriously that I left home", "I was a victim of violence among my parents" and "I grew up in a one-parent family". The variables "When growing up, I was a victim of physical abuse", and "When growing up, I was a victim of emotional abuse" composed the second factor ("Abuse in the family"). We excluded the variable "Generally speaking, the atmosphere at home was unpleasant" from further analysis because it did not correspond to any of the factors.

As a follow-up, we conducted discriminant analysis. In comparison with the men who did not engage in this type of work, male sex workers had higher mean values for both composite variables, but also higher standard deviations.

We applied the discriminant analysis to verify whether the differences between the two groups are statistically significant. We set the null hypothesis on the equality of the averages of the factors' means for both groups : , and the alternative hypothesis that the averages are different (Šifrer & Bren, 2011). For the factor "General Dysfunctionality", the p-value was 0.001, and for the factor "Abuse in the Family" it was 0.048. The null hypothesis on the equality of the averages for the factors was therefore rejected.

The value of Wilks' lambda was 0.829 with the statistically significant feature of the discriminant function of 0.006. We obtained one discriminant function, which was a linear combination of factors and statistically significantly differentiated between the groups. The factor "Abuse in the family" had a smaller weight than the factor "General dysfunctionality", so the latter differentiated the two groups more distinctly from each other. In total, 67.2% of the participants were properly classified, namely 48% of those who perform male sex work, and 81.8% of those who did not perform this type of work.

5 DISCUSSION

In the present research we tried to compare some socio-psychological characteristics of men performing as male sex workers and men who do not engage in this type of work.

In the empirical part, we analysed the collected data using descriptive and multivariate statistics. We tried to determine once again whether male sex work in Slovenia exists. We explored whether there are any statistically significant differences in sexual orientation among male sex workers and men who do not perform such work in Slovenia. We attempted to establish whether there risk factors exist which differentiate male sex workers from men who do not perform this type of work. According to the results of these analyses and the issues we addressed in our research, we can namely adopt a targeted approach to reduce the stigmatisation of male sex workers and to address the question of potential support and counselling. In this part, we explain the results and locate them in the current context of the research on male sex work.

Based on frequencies from the descriptive statistics of the sample, the first hypothesis about the existence of male sex work in Slovenia cannot be rejected. Namely, 33 respondents who reported they performed male sex work completed the questionnaire. On the other hand, we have to note that we obtained our data from various online forums where people frequently register themselves using a false identity. Online we can find a lot of pretending and misleading, including by men who claim to be escorts for female clients, as many of them would wish to be escorts for women and thus pretend to be so but, in reality, they do not have any clients. In this context, instead of the term "male sex workers" the term "men offering sexual services online" is more appropriate since we cannot be certain that in this case we are actually dealing with male sex workers (I. Šori, personal communication, November 24, 2017). The question of whom our research actually investigates therefore remains open.

We can not reject the second hypothesis: Among male sex workers and men who do not engage in this type of work there are statistically significant differences in sexual orientation. The chi-square test was statistically significant. At a 0.05 level of risk, we can say there are statistically significant differences in sexual orientation between male sex workers in Slovenia and men who do not engage in such work. (Non)-performance of male sex work is therefore linked to sexual orientation. These results are consistent with research results showing that the majority of male sex workers are homosexual or bisexual (Ballester Arnal, Salmerón Sánchez, Gil Llario, & Giménez García, 2014; Grimes, 2001; Koken et al., 2004). However, in the questionnaire we did not ask questions about what type of sex work they performed. We believe that sexual orientation affects the type of sex work a person performs. For example, an erotic dancer or an erotic masseur are, in our opinion, more likely to define themselves as heterosexual than a street sex worker. The assumption has yet to be empirically proven and Dr Iztok Šori (personal communication, November 24, 2017) claims that discussing different forms of sex work together is methodologically appropriate and in line with most of the literature in this field.

The third hypothesis, which refers to the differences in birth families' dysfunctionalities among men who perform sex work and those who do not cannot be rejected. The discriminant analysis showed that the differences between the two groups are large enough to conclude that the views on their (dysfunctional) families do differ. Therefore, we may conclude that those respondents who performed male sex work live(d) in more dysfunctional families than men who did not perform this type of work. However, their families are not dysfunctional as already follows from the descriptive statistics, which show that all respondents come from relatively functional families. These results coincide with similar research results by Bar-Johnson and Weiss (2015), and Earls and David (1989). Kuhar and Pajnik (in press) claim that circumstances in explaining male sex work refer to male sex workers' families that faced social, economic and legal insecurity. One of our participants commented on the results as follows: "Well yeah... I know a lot of individuals who prostitute themselves…their dad a drunk and a junkie ... but I also know a lady doctor who is a prostitute and has no problems at home".

Due to the limitations of our research, great care should be taken when interpreting and making conclusions. It therefore makes more sense to discuss the issues raised by our research. One of the possibilities of interpreting the question of the lack of a connection between the dysfunctionality of the family and engagement in male sex work may relate to a comment made by one participant: "This is essentially not work, it is a passion that also represents a source of income". Obviously, psychological factors are not as important as, for instance, economic factors. In society, the general belief prevails that only a person with whom 'something is wrong' might become engaged in sex work (I. Šori, personal communication, February 17, 2018). It is underpinned by the findings that the starting of sex work occurs at the crossroads of poor socio-economic circumstances as a trigger and career decision-making (Kuhar & Pajnik, in press). Our research shows that, in contrast with the general social opinion, sex workers are far more 'normal'. This is also illustrated by the descriptive statistics: the respondents on average did not report addiction to alcohol, tobacco, marijuana, cocaine or heroin. These findings, however, contradict the opinion of Ballester Arnal et al. (2014) who claim that the majority of male sex workers are addicted to prohibited substances (especially cocaine) and alcohol. Bar-Johnson and Weiss (2015) consider there is a greater likelihood of alcohol and drug abuse among sex workers working in bars and clubs compared to workers who advertise their services online. Yet Earls and David (1989) argue that alcohol and drug consumption among male sex workers is higher than among men who do not engage in this type of work.

Dr Iztok Šori (personal communication, November 24, 2017) claims that comparing male sex workers and males who do not engage such work is not necessary; moreover, it is not methodologically appropriate. Thus, our research can also be understood as additional stigmatisation of sex workers and sex work, although this was not our purpose. However, we still believe that our results can help with the destigmatising of sex workers and their work. One respondent commented: "There is a lot of this going on and it's still a taboo topic". All of the respondents in Kuhar and Pajnik (in press) also see their work as highly stigmatised. We think the solution to this is to raise people's awareness so they begin to realise that male sex work also exists and not just the female version. The feelings of acceptance of male sex workers could lead to the point where registration of their profession and adequate activities would become a reality, allowing conditions to be created that protect male sex workers. Similarly, the results of Kuhar and Pajnik (in press) show that this stigmatisation largely informs, defines and frames sex work in Slovenia. The tripartite decriminalisation (of male and female sex workers) in New Zealand has had a positive effect on improving the human rights of people performing this type of work and has also improved their relations with the police (Armstrong, 2016). It may be seen as an example of good practice so we believe that Slovenia could be inspired by their model. In this way, we would recommend training for police officers in order to eliminate stereotypes, stigmatisation and ensure consistent treatment in the event of violence. Inspiration for this may be drawn from the same example of the New Zealand model as the results of their survey show the positive effects a professional attitude of the police can have when police officers are properly informed and educated about male sex work (Armstrong, 2016). We found there is a shortage of organisations in Slovenia that work actively to reduce the stigmatisation of sex workers. Therefore, it is a good idea to consider setting up organisations, initiatives and programmes that provide information, help and support to sex workers without (secondary) stigmatisation.

REFERENCES

Abdullah Avais, M., Wassan, A. A., Chandio, R. A., & Balouch, A. S. (2014). Male prostitution in Larkana city: An unrevealed truth. *Academic Research International, 5*(5), 319–326.

Armstrong, L. (2016). From law enforcement to protection? Interactions between sex workers and police in decriminalized street-based sex industry. *British Journal of Criminology, 57*(3), 570–588.

Ballester Arnal, R., Salmerón Sánchez, P., Gil Llario, M. D., & Giménez García, C. (2014). Sexual behaviors in male sex workers in Spain: Modulating factors. *Journal of Health Psychology, 19*(2), 207–217.

Bandura, A. (1978). The self-system in reciprocal determinism. *American Psychologist, 33*(4), 344–358.

Bar-Johnson, M. D., & Weiss, P. (2015). A comparison of male sex workers in Prague: Internet escorts versus men who work in specialized bars and clubs. *The Journal of Sex Research, 52*(3), 338–346.

Bimbi, D. S. (2007). Male prostitution: Pathology, paradigms and progress in research. *Journal of Homosexuality, 53*(1–2), 7–35.

Boyer, D. (1989). Male prostitution and homosexual identity. *Journal of Homosexuality, 17*(1–2), 151–184.

Bren, M. (2017). *Metodologija družboslovnega raziskovanja in multivariatne statistične metode – II. del*, Študijsko gradivo [Methodology of social science research and multivariate statistical methods – II. Part, Study material]. Ljubljana: Fakulteta za varnostne vede.

Browne, J., & Minichiello, V. (1996). Research directions in male sex work. *Journal of Homosexuality, 31*(4), 29–56.

Brvar, B. (2007). *Statistika* [Statistics]. Ljubljana: Fakulteta za varnostne vede.

Caukins, S. E., & Coombs, N. R. (1976). The psychodynamics of male prostitution. *American Journal of Psychotherapy, 30*(3), 441–451.

Davies, P., & Feldman, R. (1997). Prostitute men now. In G. Scambler & G. Scambler (Eds.), *Rethinking prostitution: Purchasing sex in the 1990s* (pp. 29–53). London: Routledge.

Earls, C. M., & David, H. (1989). A psychosocial study of male prostitution. *Archives of Sexual Behavior, 18*(5), 401–419.

Global Network of Sex Work Project [NSWP]. (2014). *The needs and rights of male sex workers*. Edinburgh: NSWP. Retrieved from http://www.nswp.org/resource/briefing-paper-the-needs-and-rights-male-sex-workers

Grimes, T. (2001). *Such a taboo: An analysis of service need and service provision for males in prostitution in the Eastern Region*. Dublin: Irish Network Male Prostitution and East Coast Health Board.

Kanduč, Z. (1998). Prostitucija: Kriminološke, viktimološke in kazenskopravne perspektive [Prostitution: Criminological, victimological, and criminal law aspects]. *Anthropos, 30*(1–3), 88–106.

Kaye, K. (2003). Male prostitution in the twentieth century: Pseudohomosexuals, hoodlum homosexuals and exploited teens. *Journal of Homosexuality, 46*(1–2), 1–77.

Kobal, M., & Bavcon, L. (1969). Prostitucija [Prostitution]. In M. Kobal, L. Milčinski, K. Vodopivec, & B. Uderman (Eds.), *Socialna patologija* (pp. 158–179). Ljubljana: Mladinska knjiga

Koken, J., Bimbi, D. S., Parsons, J. T., & Halkitis, P. N. (2004). The experience of stigma in the lives of male internet escorts. *Journal of Psychology and Human Sexuality, 16*(1), 13–32.

Kong, T. S. K. (2014). Male sex work in China. In V. Minichielli, & J. Scott (Eds.), *Male sex work and society* (pp. 314–342). New York: Harrington Park Press.

Kuhar, R., & Pajnik, M. (in press). Negotiating professional identities: Male sex workers in Slovenia and the impact of online technologies. *Sexuality Research and Social Policy*.

Lankenau, S. E., Clatts, M. C., Welle, D., Goldsamt, L. A., & Gwadz, M. (2005). Street careers: Homelessness, drug use, and sex work among young men who have sex with men. *The International Journal on Drug Policy, 16*(1), 10–18.

Leichtentritt, R. D., & Davidson Arad, B. (2005). Young male street workers: Life histories and current experiences. *British Journal of Social Work, 35*(4), 483–509.

Lucas, A. (2004). Hustling for money: Male prostitute's experiences of social control. In R. Miller, & S. Browning (Eds.), *For the common good: A critical examination of law and social control* (pp. 188–210). Durham: Carolina Academic Press.

Mc Cabe, I., Mills, R., Murphy, D., Winders, S. J., Hayden J., Reynolds, D. … McQuaid, A. (2014). A psychocultural comparison of male street prostitutes in Dublin and San Francisco. *Irish Journal of Psychology, 35*(2–3), 91–105.

McCajor Hall, T. (2007). Rent-boys, barflies, and kept men: Men involved in sex with men for compensation in Prague. *Sexualities, 10*(4), 457–472.

Mendoza, C. (2014). Places, spaces and bodies: Male-to male sex tourism in Puerto Vallarta (Mexico). *Athens Journal of Tourism, 1*(3), 175–189.

Minichiello, V., Scott, J., & Callander, D. (2013). New pleasures and old dangers: Reinventing male sex work. *The Journal of Sex Research, 50*(3–4), 263–275.

Minichiello, V., Mariño, R., Browne, J., Jamieson, M., Peterson, K., Reuter, B., & Robinson, K. (2002). Male sex workers in three Australian cities: Sociodemographic and sex work characteristics. *Journal of Homosexuality, 42*(1), 29–51.

Pajnik, M. (2008). *Prostitucija in trgovanje z ljudmi: Perspektive spola, dela in migracij* [Prostitution and human trafficking: Gender, labour, and migration aspects]. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične vede.

Pajnik, M., & Kavčič, U. (2008). Sodne prakse, povezane s trgovanjem z ljudmi in prostitucijo v Sloveniji [Case law related to trafficking in human beings and prostitution in Slovenia]. *Revija za kriminalistiko in kriminologijo, 59*(2), 141–154.

Pajnik, M., & Šori, I. (2014). Seksualna industrija v Sloveniji na spletu: Med oligopoli organizatorjev in nemočjo seksualnih delavk [Sex industry in Slovenia on the web: Between oligopoles of organizers and powerlesness of sex workers]. *Annales, 24*(1), 143–156.

Parsons, J. T., Bimbi, D., & Halkitis, P. N. (2001). Sexual compulsivity among gay/bisexual male escorts who advertise on the internet. *Sexual Addiction and Compulsivity, 8*(2), 101–112.

Petrovec, D. (2000). Nekaj teoretičnih in praktičnih vidikov prostitucije [Some theoretical and practical aspects of prostitution]. *Revija za kriminalistiko in kriminologijo, 51*(4), 314–319.

Popov, J. (2008). *Prostitucija: Priročnik za prostitute-ke, stranke in moraliste-ke* [Prostitution: A handbook for prostitutes, clients and moralists]. Maribor: Pivec.

Reiss, A. J. (1961). The social integration of queers and peers. *Social Problems, 9*(2), 102–120.

Smith, M. D., Grov, C., Seal, D. W., & McCall, P. (2013). A social-cognitive analysis of how young men become involved in male escorting. *The Journal of Sex Research, 50*(1), 1–10. doi: 10.1080/00224499.2012.681402

Šifrer, J., & Bren, M. (2011). *SPSS – multivariatne metode v varstvoslovju* [SPSS – multivariate statistical methods in criminal justice and security]. Ljubljana: Fakulteta za varnostne vede.

Šori, I. (2005). Prostitucija v Sloveniji: Akterji, podoba, problemi in odnosi [Prostitution in Slovenia: Actors, image, problems and relations]. *Etnolog, 15*(1), 61–80.

Timpson, S. C., Ross, M. W., Williams, M. L., & Atkinson, J. (2007). Characteristics, drug use, and sex partners of a sample of male sex workers. *American Journal of Drug Alcohol Abuse, 33*(1), 63–69.

Tratnik Volasko, M. (1996). *Prostitucija: Zakonodajni, sociološki in nadzorstveni vidiki pojava* [Prostitution: Legal, social and supervision aspects]. Ljubljana: Ministrstvo za notranje zadeve.

United Nations Office for Drugs and Crime. (2007). *A study report on Luanda dancers: Dancing boys: Traditional prostitution of young males in India*. Retrieved from https://www.unodc.org/unodc/search.html?q=dancing+boys&site=unodc&btnG=Search&site=unodc&proxyreload=1&sort=date%3AD%3AL%3Ad1&entqr=0&entqrm=0&ud=1

Van der Poel, S. (1992). Professional male prostitution: A neglected phenomenon. *Crime, Law and Social Change, 18*(3), 259–275.

Vanwesenbeeck, I. (2012). Prostitution push and pull: Male and female perspectives. *The Journal of Sex Research, 50*(1), 11–16.

Weitzer, R. (2005). New directions in research on prostitution. *Crime Law and Social Change, 43*(4), 211–235.

West, D. J., & de Villiers B. (1993). *Male prostitution*. Binghamton: Haworth Press.

Wilson, H. W., & Widom, C. S. (2010). The role of youth problem behaviors in the path from child abuse and neglect to prostitution: A prospective examination. *Journal of Research on Adolescence, 20*(1), 210–236.

Zaviršek, D. (1993). Prostitucija – izziv za drugačno socialno delo [Prostitution – A challenge for a different way of doing social work]. *Revija za kriminalistiko in kriminologijo, 44*(1), 3–10.

About the Authors:

Monika Klun, a master's student at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: monika.klun@student.um.si

Matevž Bren, PhD, a full professor of Statistics and Methodology at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia is also a researcher at the Institute of Mathematics, Physics and Mechanics and a member of a research programme. E-mail: matevz.bren@fvv.uni-mb.si

VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 20
no. 2
pp. 202–217

Art Crime and Preventive Measures for Museums, Churches and Sacred Objects

Saša Kuhar

Purpose:

The purpose of the paper is to present art crime and preventive measures that reduce crime involving art in museums, churches and sacred objects.

Methods:

Art crime and preventive measures are analysed by applying a descriptive method and literature review. Statistical data are considered to present the scale of art crime in Europe.

Findings:

Art crime has been present in society for millennia. Statistics show art thefts from private buildings, galleries, churches and sacred objects prevail. Thefts from museums attract the greatest media attention. The perpetrators are usually unaware of the value of the stolen art. The biggest difficulty is the hidden nature of crime involving art because many cases go unreported, especially when occurring in museums. The reason is that it affects the reputation of museums. In particular, they do not the public to know they have weak preventive measures. Safeguarding art works in museums and churches as well as sacred objects is a very demanding and responsible task. Artworks need to be kept simultaneously safe and accessible to visitors. A combination of security measures is essential; physical and technical protection as well as forensic marking. In the future, greater attention should be paid to raising public awareness of the value of artworks for society.

Originality/Value:

The paper describes the preventive measures that should be applied to reduce and prevent art crime in museums and churches and concerning sacred objects. The owners of museums, security services and archival institutions can use the proposed measures to minimise such art crime.

UDC: 343.3/.7:7

Keywords: art crime, prevention, museums, churches, sacred objects

Preventivni ukrepi na področju kriminalitete zoper umetnine v muzejih, cerkvah in sakralnih objektih

Namen prispevka:

Namen prispevka je predstaviti kriminaliteto zoper umetnine in preventivne ukrepe, ki pripomorejo k zmanjševanju kaznivih dejanj zoper umetnine v muzejih, cerkvah in sakralnih objektih.

Metode:

Za pripravo prispevka smo uporabili deskriptivno metodo in metodo analize dokumentov. Z analizo statističnih podatkov smo predstavili kako številčna je kriminaliteta zoper umetnine v Evropi.

Ugotovitve:

Kriminaliteta zoper umetnine je v družbi prisotna že tisočletja. Statistični podatki kažejo, da prevladujejo tatvine umetnin iz zasebnih objektov, galerij, cerkva in sakralnih objektov. Medijsko najbolj izpostavljeni so primeri tatvin iz muzejev. Storilci se običajno ne zavedajo vrednosti umetnine, ki so si jo protipravno prilastili. Po mnenju strokovnjakov je veliko kaznivih dejanj zoper umetnine, predvsem tistih, ki so storjena v muzejih, neprijavljenih. Razlog je v tem, da si muzeji ne želijo slabe reklame, hkrati pa ne želijo javnosti pokazati, da imajo slabe zaščitne ukrepe. Varovanje umetnin v muzejih, cerkvah in sakralnih objektih je zelo zahtevna in odgovorna naloga, saj je potrebno umetnine hraniti varno, hkrati pa morajo biti dostopne obiskovalcem. Nujno je potrebna kombinacija varnostnih ukrepov; fizičnega in tehničnega varovanja ter forenzičnega označevanja. V prihodnje je treba veliko pozornosti nameniti tudi ozaveščanju prebivalstva o pomenu umetnin za družbo.

Izvirnost/pomembnost prispevka:

Prispevek predstavi preventivne ukrepe katere je potrebno uporabiti, da bi zmanjšali in preprečili izvedbo kaznivih dejanj zoper umetnine v muzejih, cerkvah in sakralnih objektih. Podatki bodo v pomoč lastnikom muzejev, varnostnim službam in nadškofijam, da bi s predlaganimi ukrepi zmanjšali kriminaliteto zoper umetnine.

UDK: 343.3/.7:7

Ključne besede: kriminaliteta zoper umetnine, preprečevanje, muzeji, cerkve, sakralni objekti

1 INTRODUCTION

Art crime has a very long tradition, but has become even more attractive in the past decades due to the high financial gains and low rate of successful investigations. According to Hollington (2014), art crime generates proceeds ranging from USD 2 to 6 billion per year, most of which is used to support international organised crime groups. Wylly (2014) states that Bonnie Magness-Gardiner, retired director of the FBI Art Theft Programme, estimated the annual loss incurred due to art crime at USD 8 billion a year.

Art crimes include various types of criminal offences; theft, forgery, vandalism, negligence, fraud, unauthorised imports and exports of works of art, destruction of artworks as a result of war, and others. Data from the Slovenian police (Ministrstvo za notranje zadeve, Policija, 2016) show that, on average, 100 art crimes occur every year in Slovenia. But art crime is an even bigger problem in other countries. Mustajbegović (2015) states that 30,000 crimes involving art happen in Italy annually. The sheer scale of art crimes forces the police in some countries to establish special departments that specialise solely in this type of crime. Independent organisations are also involved in investigating art crime. They have their own Internet webpages where they publish pictures and details of artworks that are the subject of criminal activity. Europol (2017, 2018) reported two successful police operations (Athena, Pandora and Pandora II) in 2017 that saw more than 41,000 artworks being seized across the world. This was a result of coordinated law enforcement actions. The artworks were the subject of illicit trafficking, theft, looting and Internet sales.

Statistical data show (Dobovšek, 2010; Kuhar, 2017; Wittman, 2010; Wylly, 2014) that art theft from private premises, galleries, churches and sacred objects dominates. The perpetrators are usually unaware of the value of the art they have stolen or damaged. Thefts from museums attract the greatest media attention because of the high value of the works involved. According to Dobovšek (2007), many art crimes, especially those committed in museums, go unreported. The reason is that museums do not want to acquire a poor reputation or to show the public they have weak security.

Safeguarding art works in museums and churches and sacred objects themselves is a very demanding and responsible task as they simultaneously need to be kept safe and accessible to visitors. The key elements are to reduce opportunities to commit a crime, to make the risk of such crime greater, and to reduce the proceeds of crime. A combination of different security measures is essential; both physical and technical protection, internal and external video surveillance, as well as forensic marking. It is also important to raise public awareness of the value of artworks for society.

For the purpose of this paper, art crime and preventive measures were analysed by applying a descriptive method and literature review. Statistical data were considered to present the scale of art crime in Europe.

In the future, considerable attention should be paid to security, preventive measures, raising awareness of the population and conducting research in the field of art. This is the only way to reduce the scale of the problem. The paper aims to present art crime, especially where it involves museums, churches and sacred objects. The emphasis is given to preventive measures that help to reduce art crime in museums and churches and concerning sacred objects. The findings can be useful for police and art owners, especially museum management, security services and leaders of archdioceses who should pay more attention to the security of the artworks in their care. Artworks are a mirror of the past. They must be protected, not only because of their monetary value but also due to their significance for humanity.

2 ART CRIME

Art crime has existed for millennia. Various types of art crime have emerged over the years. O'Keefe (2014), Conklin (1994), Durney (2011) and Hufnagel (2015) include theft, forgery, smuggling and illegal exports of artworks within the concept of art crime. According to O'Keefe (2014), it is impossible to determine the true extent of art crime since statistics are insufficient indicators given that many of such crimes are unreported.

Thefts, robberies and trade in stolen artworks have become an international problem. Interpol has been trying to combat it since 1947 by connecting police units from around the world. But variations in the concept of art and countries' different laws are the primary problems investigators face in their work. Another problem is that art theft is often recorded as property crime and art forgeries as fraud. This leads to doubt about the actual number of art crimes annually reported.

The proceeds of art crime can be extremely large, but the consequences for human history cannot be measured in cash alone. According to Interpol (Koldehoff & Koldehoff, 2004), trading in stolen artwork does not lag much behind the trade in illicit drugs and human smuggling. Europol (2005) noted that trade in artworks and cultural objects is an area where organised crime has been present for years and its influence continues to grow.

According to some reports, the loss caused by art crime reaches billions of US dollars per year. Hollington (2014) estimated that USD 2 to 6 billion is earned through art crime yearly. The retired director of the FBI Art Theft Programme Bonnie Magness-Gardiner (Wylly, 2014) stated the estimated annual loss incurred by art crime is USD 8 billion. In addition, Wylly (2014) believed this is a very low estimate as we must be aware that the statistics include only one-third of the 192 United Nations member states.

The most common form of art crime is theft. Theft of art works from churches and profane sacred objects dominate. This could be reduced by taking preventive measures and raising public awareness of the value of artworks for a nation's history. Art theft occurs in museums, galleries and private collections where, according to Tijhuis (2006) and Wylly (2014), they are even more frequent due to poor protection. Typically, the offenders just break a door open or smash the glass of a window. According to the literature review, occasional art thefts are very common. Kursar Trček (2002) calls these situational thefts. For example, a tourist who did not initially plan to commit any theft takes a piece of an artwork or even the whole item as a souvenir simply because the art was poorly protected.

It is hard to sell stolen art immediately after it is taken. Perpetrators usually wait some time before the artwork appears on the market. According to Durney (2009), the price of stolen art on the black market is just 7% to 10% of the actual market value. This makes the basic price of the artwork even more important. Offenders usually do not sell a stolen artwork by a famous artist. They use it as payment within a criminal organisation. Artworks may be exchanged for drugs or weapons or given to compensate for other services.

It is very difficult to obtain reliable data about the number of stolen artworks and it is unlikely the true scale will ever be known. Country statistics about art crime are often based on property crime and do not provide accurate information about stolen artworks (Interpol etc.).

According to Belaj (2010), in 2001 Interpol published a list of five countries where the highest numbers of artworks are stolen. Topping the list was Italy where approximately 22,000 artworks were stolen every year. Second place was taken by the Czech Republic with 5,300 stolen art items a year, followed by Russia with 4,400 art thefts, Switzerland with 3,100 art thefts and Turkey with 1,700 art thefts a year. More recent data given by Mustajbegović (2015) show that in Italy approximately 30,000 art thefts occur annually. Russia is in second place where some 2,000 art thefts happen per year. The scale of art crimes in 20 EU countries is presented in Table 1.

Table 1: Number of art crimes in 20 EU countries between 2007 and 2010

		Year			
Country	2007	2008	2009	2010	Total
Austria	131	125	113	n.d.*	369
Bulgaria	206	164	204	191	765
Belgium	229	223	252	175	879
Cyprus	8	7	10	14	39
Czech Republic	370	639	1527	954	3490
Denmark	57	62	50	82	251
Estonia	8	9	8	7	32
France	2,714	2,223	1,751	1,442	8,130
Germany	2,003	2,265	2,055	n. d.	6,323
Greece	75	87	72	91	325
Italy	1,085	1,031	882	817	3,815
Latvia	46	94	79	100	319
Lithuania	15	13	14	12	54
Malta	9	8	9	6	32
Netherlands	n. d.	n. d.	n. d.	831	831
Poland	1,132	776	814	804	3526
Portugal	164	233	200	159	756
Slovakia	24	25	26	29	104
Slovenia	28	55	42	66	191
Spain	443	432	489	543	1907
Total	8,747	8,471	8,597	6,323	32,138

**n. d. = no data*

Source: Block (2012)

According to Slovenian Police data (Ministrstvo za notranje zadeve, Policija, 2016), 94 art crimes were committed in Slovenia in 2007, 145 in 2008, 92 in 2009 and 81 in 2010. Considering that the data for the Republic of Slovenia shown in Table 1 are not the same as the police's statistical data, one can be suspicious of the credibility of the data presented for all countries. Nevertheless, they can give us an approximate picture of the scale of art crimes in other EU countries. The percentage share of recovered stolen artworks is extremely low. A potentially easier way to find a stolen painting, which has fallen into the hands of a criminal organisation, is to hire a private investigator.

Art theft from churches and private collections prevails. The true scale will never be known to the public as only thefts of art works by famous artists are typically reported. Art crimes committed in museums and churches and involving sacred objects are presented below.

2.1 Art Crime in Museums

Thefts from museums attract the widest media attention. The reason is that the value of the items stolen from museums is higher than for items stolen from other places. Protection plays an important role in thwarting art theft. According to Dobovšek (2009), thefts from museums are mostly prepared in advance, offenders are only interested in a specific item that already has a buyer waiting. They have information about the location of the art work and how it is protected.

Art is often stolen in broad daylight when a museum is full of visitors, but nobody notices anything. The reason for this state of affairs is poor protection, both technical and physical. Offenders disappear together with the stolen art item in a very quick time.

Interpol (Wylly, 2014) states that 11% of all art theft occurs in museums. According to Wittman (2010), between 1990 and 2005, thieves stole art works from museums with a total value of over USD 1 billion.

Samardžić (in press) states that in many cases the offenders of an art crime in museums are employees. They have access to the item concerned and inside information that helps them commit the crime. According to Wittman (2010), a good example of the theft of artworks by an employee is what happened in the Walters Art Museum in Baltimore, USA. A security guard on the night shift stole 145 artworks over eight months. Another case occurred in the Hermitage Museum (Saint Petersburg) where the curator took artworks valued at USD 5 million over 15 years.

One of the best known art thefts in history (Charney, 2007) is the theft of the *Mona Lisa* from the Paris Louvre Museum in 1911. The theft was committed by Vincenzo Peruggia. Hidden in the museum's warehouse, he changed his clothes. During the night when no one was in the museum, he took the picture off the wall and wrapped it in his smock, and simply walked out of the museum with it in the morning. The security guard let him out, thinking he was a worker who had accidentally stayed at the museum overnight. It was 24 hours before anyone even noticed the Mona Lisa was missing. The Louvre had over 400 rooms but only 200 guards and even fewer on duty through the night. The museum basically had no alarms. The painting was recovered 28 months later.

A prospective offender may not be deterred by the presence of an alarm in a museum. Burglars have often triggered an alarm, but security guards do not necessarily pay much attention to it because they believe it is a false alarm. An example of this is a theft in the Art History Museum in Vienna in 2003. This crime entailed precisely that combination of circumstances. Security guards there had regularly encountered false alarms. On 11 May, the museum's most famous sculpture Saltcellar of Francis I, an extraordinary gold-plated saltcellar and one of the world's greatest Renaissance artefacts was stolen, yet they did not respond. When the alarm was triggered, the guards thought it was a false alarm and switched it off. The thief had 54 seconds available to carry out the theft. The saltcellar, whose value was estimated at EUR 60 million, was found in January 2006 when the offender was identified (Traynor, 2003).

According to Lawler (n. d.), the biggest case of theft, looting and destruction of art works in history was committed in the National Museum of Iraq in 2003. It was looted during and after the 2003 invasion of Iraq. The Iraq Museum contained precious relics from the Mesopotamian, Babylonian and Persian civilisations. International efforts led to many of the stolen artefacts being returned. After remaining closed for many years while being refurbished and being rarely open for public viewing, the museum was officially reopened in February 2015.

Museums have seen better protection against theft in recent years. This has led to a rise in the number of armed robberies which museums find difficult to protect. One of the biggest robberies and a good example of organised crime being involved in art crime in Europe took place in Switzerland in 2008 when four paintings by world-known artists – a Cézanne, a Degas, a van Gogh and a Monet – were stolen. One of these was the painting *Boy in a red vest* by Paul Cezanne whose price on the art market was EUR 100 million. According to witnesses, the robbery was carried out in just three minutes (Marković–Subota, 2012). The rapidly occurring robbery and explosion that neutralised both staff and visitors show the robbery was well planned. Some possible preventive measures against robbery are presented in the next chapter.

The third form of art crime occurring in museums is vandalism, including damage to and the destruction of artworks. Vandals use different tools to damage an art item such as a pen, paint, fire, knife, explosives, firearms and other. Rude and brutish behaviour such as sticking on chewing gum, spitting and marking certain parts of an artwork is considered a lighter form of vandalism. In 1911, someone tried to cut the Rembrandt painting *The Night Watch* with a knife but could not cut through the thick varnish applied to the painting. After this event, the painting was restored. However, in 1975 the painting was again cut with a knife in dozens of zigzag lines. The offender was wrestled to the ground by the guards. It took six months to restore the painting and traces of the cut marks still remain. The third attack involving the same painting was in 1990 when a man threw acid on the painting. Museum guards seized the attacker and handed him over to the police. The guards managed to quickly dilute it with water so that it only penetrated the varnish layer, and the painting was restored again (Puchko, 2015).

One of the possibilities of preventive action is to educate children and youth. We need to imbue in them a cultural attitude to art because young people are often the proponents of vandalism. It is also necessary to raise awareness among older people of the importance of art and cultural heritage.

2.2 Art Crime in Churches and Involving Sacred Objects

Churches and sacred objects are often considered a special and safe place, but they have become the main targets for criminals in the last few years. Without appropriate security measures, a church or sacred object makes an easy target for theft or vandalism.

According to Dobovšek and Samardžić (2012), with most museums having improved their security systems, art theft from smaller, unsecured churches has increased. Hundreds of churches and sacred objects across Europe are vulnerable to thieves. Thefts of works of art from religious and secular-sacred building are the predominant type of crime and could be prevented by adopting preventive measures and raising public awareness of the value of such works of art for a nation's history.

Artworks and objects from churches and sacred objects themselves are made of expensive materials and richly decorated. Paintings and frescoes have a historical value and are thus attractive targets for offenders.

Statues, decorative objects, liturgical items, gold and silver icons and relics stolen from churches and monasteries in Cyprus, Greece, Russia, Armenia, Serbia and elsewhere are sold for several hundred to hundreds of thousands of euros, especially in the USA and Western Europe.

Besides art theft, vandalism and damage to art from churches and sacred buildings is widespread. The motives for this type of crime vary and may be religious, social or political. The perpetrators are often minors who destroy artworks simply because they have easy access to them and because the items are not protected.

With the cooperation of the Ministry of Culture, the Slovenian Police has already made some recommendations to the bishop's conference. They wanted to increase awareness that greater attention has to be paid to chapels and churches, including locking them up regularly. It is understandable that a church is a temple of God and must be constantly open. But it is only with regular locking and security measures that art crime can be reduced. Some churches already have video surveillance, are more often locked, grates have been installed over ground-floor windows, and more secure doors are being used.

According to Kuhar (2017), the Slovenian Ministry of Culture has already been in contact with church dignitaries in the past and informed them of the problem of art theft from churches and sacred objects. It is essential to talk with church dignitaries and explain to them why it is essential to increase control over artworks in churches and sacred objects.

It is recommended that churches conduct an inventory of all art items located in churches, sacred objects and other church premises. They started taking an inventory in the past, but it was not finished. The biggest fear of church dignitaries is that the inventory would reveal information about church assets. Yet churches must be aware that such an inventory along with the forensic marking of art items are just preventive measures and the data will not be publicised. It is also important to increase the level of control and video surveillance over churches and sacred objects and regularly check their status. This is the only way of reducing art crimes.

3 ART CRIME AND PREVENTION MEASURES

The art of museum security is no less profound than some of the masterpieces hanging in the spaces that require protection. Analyses of art theft show that the places where the art item was located were relatively easily accessible and uncontrolled during the crime.

The most typical form of preventive action is situational prevention. Meško (2002) presented Clarke's definition that situational prevention is where these measures are directed at highly specific forms of crime, involving the management, design, or manipulation of the immediate environment in a systematic and permanent way.

Situational crime prevention uses techniques that focus on reducing the opportunity to commit a crime. Some techniques here include making the crime more difficult, increasing the risk entailed in crime, and reducing the proceeds of crime (Clarke, 1997). Situational prevention is important when talking about preventing art crime, especially the prevention of theft, burglary and vandalism.

Meško (1996) proposed the following main measures of situational prevention: measures that force the perpetrator to invest more effort to commit a crime; measures that increase the risk entailed in a crime and measures that reduce the potential rewards for committing an offence.

It is necessary to combine several preventive measures; otherwise, the effect of preventive activity cannot be increased. In addition, situational prevention implies greater self-protection by citizens regarding their property, while the responsibility of business entities is linked to the various possibilities of committing a crime.

Protecting artworks in museums and churches and sacred objects themselves is a very demanding and responsible task. It is essential to keep art items protected, while at the same time allowing visitors to encounter masterpieces. This requires a lot of work, planning and some new technology, as presented below.

3.1 Physical Security

In the past, only physical protection was provided to protect people, items and objects. It still plays an important role in protecting artworks. Privately employed security guards are responsible for ensuring the safety and security of employees, visitors and artworks. It is necessary to develop a physical protection plan for each item individually. The personnel who provide physical security must be familiar with the procedures (Golob, 1997).

Security personnel has to be qualified, trained, interested in the work and proactive. In addition, it is necessary to have sufficiently motivated security guards. If a crime occurs, they have to react as soon as possible. As we saw in the case of Vienna, thieves do not need much time to steal a piece of art. They only need 54 seconds to steal art worth EUR 60 million.

Security guards must pay as much attention to fire exits as they do to the art itself. They also communicate with the security control centre, which dispatches staff to suspicious situations. In addition, several other preventive measures are possible: post the appropriate number of guards to detect and deter potential attacks; limit the number of people who may visit at any one time and urge visitors to keep moving, enabling the guards to maintain an overview of the situation.

Many examples from practice (Marković-Subota, 2009; Marn, 2007) show that man is the weakest link in any security system. Lack of interest, bribery and reduced attention at work are only some of the problems encountered with security personnel. It is necessary to combine technical and physical protection because having in place a combination of different security measures proves to be the most effective.

3.2 Technical Protection

Technical security systems are:

> individual or functionally connected equipment and mechanical devices for protection, anti-theft and anti-burglary devices, devices for supervision of entry, exit or movement, screening of persons, transport means, cargo or baggage, prevention of forcible entry, automatic detection of unauthorised presence and alarming, transmission of alarm messages and equipment for processing and archiving such messages (video and audio surveillance, security alarms, sensors and motion detectors, alarm surveillance systems, cameras and sensors), electric, electromagnetic, magnetic or biometric devices for supervision of entry and other systems and devices intended for providing security pursuant to this Act. Technical security systems pursuant to this Act shall include other systems inseparably connected with technical security systems pursuant to this Act, while interference with these systems shall mean interference with technical security systems pursuant to this Act (fire protection, alarming in case of explosive and other gases, social alarms, systems for the detection of explosive and poisonous substances, gases and fumes, security strong-boxes, security doors, locks, vaults, and safes). Devices for supervising stock and inventory and other devices and systems not intended for providing security in accordance with this Act shall not be considered technical security systems (Zakon o zasebnem varovanju [Private Security Act], 2011).

It is necessary to employ some technical protection such as movement sensors and picture-hanging systems sensitive to a particular sequence of movements. The art item concerned should be attached to a base (technical security that disables the unauthorised physical removal of the item and with a silent alarm, which is connected to the control room). It is recommended to increase the distance between visitors and the art, prevent any touching and to use magnetic contacts for doors and stair gates that, when a door is opened or a silent alarm is triggered transmits relevant images to the control room.

An organisation responsible for safeguarding art items does not need a lot of money for such actions. A statue can be connected with a steel mesh to a base. A sensor should be located underneath to detect vibrations. This kind of system cannot be detected by thieves as the base is generally hollow. If the statue is lifted, the steel mesh, which cannot be cut, holds the statue in place and triggers an alarm. The cost of such a measure is around EUR 50 (Mazi, 2009).

Potokar and Bernik (2014) state that technical protection is today an indispensable tool in protecting an item's value. To help to secure premises, mechanical protection can be used, such as fencing, security gates, multipoint locks, bulletproof window panes, bars on windows and barriers that restrict access to the art. One recommended measure for securing art works is to place a glass wall in front of a painting. This measure is unsuitable if a painting is too big. Another critical issue is the distance between the art and the visitors. The distance should be increased and barriers erected to avoid touching and attacks using sharp objects.

CCTV equipped with video content analysis technology should be used to monitor the public. In this way, if a person crosses a defined line an alarm is automatically triggered (usually an audible signal to alert both visitors and the guard). Use of CCTV alone has little effect on the response time. The control room is an important part of the security regime because it enables control of the action outside and within the building with the help of external and internal video surveillance.

Wireless protection of artwork

Over time and with the development of techniques, various ways of protecting buildings and arts have emerged. As mentioned, one of the most basic and simple ways for technically protecting art items is to tie them down with steel mesh. Companies have been improving such protection in recent years. Art Guard (n. d.) has been one of the leading companies in the field of art protection in the last decade. It provides innovative and high-quality ways to protect artwork against theft. Thieves who steal art items from museums and galleries have changed their modus operandi. Art theft is often committed during opening hours when the museum or gallery is filled with visitors. Due to the heavy physical protection of art items during opening hours, a device called a "safe hook" was invented, which triggers an alarm if an artwork is removed from the hook. The device is small, suitable for installation on art hanging from the ceiling and is independent of the power supply.

The second invention is the wireless magnetic protection of artwork. It is suitable for artworks that stand or hang on walls. A magnet is attached to the artwork and a frequency transmitter is mounted on the wall or floor to detect any displacement of the magnet on the artwork. In this case, when the alarm is triggered it can be heard by everyone in the building (Art Guard, n. d.). Due to its reliability, ease of use, low costs, and adaptability to the size of the artwork and the ways of exhibiting, such systems provide one of the most appropriate preventive measures against art theft. Such systems are suitable for museums, galleries, private collections, churches and sacred objects, namely the places that are most often targeted by thieves in recent times.

3.3 Forensic Marking

The most recent method of preventing art theft is forensic marking. Forensic marking is a method of marking valuable items with artificial 'DNA'. It is almost impossible to remove the forensic marking from the art without damaging it. Any damage to the art could reduce its value in further resale on the black market. This makes such art items less attractive to thieves. In addition, it not only reduces crime and art theft but also allows easy identification of ownership and enables police to link criminals to the crime scene (Kuhar, 2015).

One of the most advanced forensic marking systems for reducing the scale of offences is *SelectaDNA*. It combines its unique 'DNA' coding with microdot technology. It serves as indisputable evidence of ownership in court proceedings, links the perpetrators with the crime scene, and enables the police to establish a link between the perpetrator and the crime scene.

An increasing number of European countries use *SelectaDNA* in various preventive activities. Moreover, ever more insurance companies around the world recommend forensic marking to their policyholders as the best preventive measure to reduce the number of thefts, burglaries and robberies. Some insurance companies even require assets to be forensically marked as a condition for obtaining insurance. This measure is especially recommended for art owners. According to the British police (SelectaDNA, n. d.), forensic marking reduced thefts, burglaries and robberies in some cases by up to 83%.

Offenders are aware that 'DNA' is the most powerful weapon available to the police for convicting criminals. Therefore, the 'DNA fear factor' is highly understood and acts as a considerable deterrent. Offenders view items marked with *SelectaDNA* as constituting too high a risk and are further put off from stealing them as they have little or no resale value. Using *SelectaDNA* to mark property is the ultimate theft and burglary deterrent.

When we want to protect art items that are located outside, we can use *SelectaDNA* grease. It is specially designed to protect outdoor materials and its structure makes it more appropriate for art items, which are exposed to weather changes. Once a thief is exposed to the grease, it transfers onto his/her hands and clothes. The offender is then forensically linked to the crime scene.

A burglary can be prevented by using a *SelectaDNA* intruder spray. It contains a solution with a UV tracer and a unique 'DNA' code, which irrefutably links the offender to the scene of the crime. Police can take traces of the 'DNA' marker from the skin, hair and clothing of the offender, and send them away for forensic analysis. The solution can remain on the criminal for weeks, clinging to fibres and settling in creases of the skin. The DNA Spray can be armed with a panic button and linked to an existing intruder alarm system (SelectaDNA, n. d.).

3.4 Security Smoke Systems

Security Smoke Systems are technical devices whose operation obscures the vision of intruders and makes it practically impossible for them to commit a crime. By activating the system in the room, the device produces smoke that due to the high temperature instantly evaporates, creating a hot, extremely dense vapour. It cools in an instant and condenses to form a thick fog that looks like dense smoke (Security Smoke Manual, 2013). In the event of a break-in, the system fills the room with safe, harmless smoke that debilitates and disorients the intruders. Security Smoke Systems are guaranteed to leave no residue behind after deployment. People can go straight back to work without any hold-ups, mess or fuss.

This type of security system has three essential functions: it represents a physical barrier against thieves, burglars and robbers that cannot be forcibly removed (smoke cannot be broken with a tool or weapon); in a way, it works to deter thieves from entering the building; the sudden release of thick smoke debilitates and disorients the intruder. Even if thieves, burglars or robbers enter a room, they do not commit a crime because they cannot see the items and leave the room as quickly as possible (Security Smoke Manual, 2013).

The use of security smoke systems is recommended in conjunction with existing security systems since that effectively reduces the loss caused by rapidly performed burglaries and robberies. They represent an effective, innovative, health- and object-friendly way of protecting property and people, which is even more important in protecting artworks as it does not damage or ruin them.

The best preventive measure is a combination of the various security measures were mentioned above. Which will be used depends on the individual institution's financial capacity and past experience. Further, we have to raise people's awareness of the importance of art for a nation's culture and how important it is to retain artworks for future generations.

Unfortunately, artworks cannot be given complete protection. But effective protection and a combination of preventive measures can limit a significant proportion of art crime and reduce the loss incurred by the theft, robbery, burglary or destruction of artwork. In the future, we should consider securing items of art with the help of air or mobile control systems like drones, multi-sensors and multi-directional cameras for controlling external spaces where art and cultural heritage is located and where the common prevention measures are unlikely to be successful.

4 CONCLUSION

According to the literature and statistics on art crime, the theft of art prevails. Burglaries in premises that are poorly protected and uncontrolled, such as churches and sacred objects, are also very common. Offenders exploit defective self-protection regimes, shortcomings in security and obsolescent security systems. That is an important sign that security strategies need to be improved. The mentioned security and preventive measures have already demonstrated it is possible to reduce the number of offences involving artworks in practice at a small cost.

Due to the growing problem of art crime, the international community has launched many activities to limit illicit trafficking in and criminal offences involving arts. A number of international legal acts have been adopted which should encourage the signatory states to establish appropriate mechanisms to combat this type of crime. The excellent cooperation between police and international organisations in both the repressive and preventive fields is the key to success. Collaboration is particularly important in today's society where, due to the rapid exchange of information and knowledge, people and goods, cultures and values and, finally, also due to the growing social differences, new types of crime are emerging.

Moreover, another problem of art crime is that the public and government representatives are un aware of the seriousness of such offences and their consequences. As a result, they do not pay much attention to art crime. In the future, considerable effort will be needed to raise people's awareness of the problems brought by art crime. It is anticipated that in the future art crime will continue to be part of society due to the enormous profits, inadequate security, low level of successful investigation and the mild penalties. The true value of all artworks that are stolen will never be known. Experts estimate that around USD 2 to 6 billion is earned through art crime every year, but the loss caused to society and for future generations is intangible.

Arts are a mirror of our past and must be protected, not simply because of their monetary value but also because of their importance for humanity. We should be aware that artworks represent culture, values and traditions. Cultural heritage means a common bond, our community affiliation. It represents both our history and our identity. It is our bridge to the past, which is essential for our present and future.

REFERENCES

Art Guard. (n. d.). *The leading solutions for art and asset security*. Retrieved from http://www.artguard.net/

Belaj, U. (2010). Analiza največjih tatvin umetnin [The analysis of the greatest art theft]. In B. Dobovšek & G. Meško (Eds.), *Preiskovanje kriminalitete v zvezi z umetninami* (pp. 51–67). Ljubljana: Ministrstvo za notranje zadeve.

Block, L. (April 8, 2012). *Statistics on European art crime*. Association for Research into Crimes against Art. Retrieved from http://art-crime.blogspot.si/2012/04/statistics-on-european-art-crime.html

Clarke, V. R. (Ed.). (1997). *Situational crime prevention: Successful case studies*. Guilderland; New York: Harrow and Heston. Retrieved from http://www.popcenter.org/library/reading/pdfs/scp2_intro.pdf

Conklin, E. J. (1994). *Art crime.* Main: West Port.

Charney, N. (2007). *The art thief*. New York: Atria Books.

Dobovšek, B. (2007). Problematika trgovine z umetninami [The problem of trafficking works of art]. In M. Jager (Ed.), *Kraje umetnin/Art theft*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Dobovšek, B. (2009). *Transnacionalna kriminaliteta* [Transnational crime]. Ljubljana: Fakulteta za varnostne vede.

Dobovšek, B. (2010). Umetnine in kriminaliteta [Art and crime]. In B. Dobovšek & G. Meško (Eds.), *Preiskovanje kriminalitete v zvezi z umetninami* (pp. 2–17). Ljubljana: Ministrstvo za notranje zadeve.

Dobovšek, B., & Samardžić, R. (2012). Krijumčarenje i ilegalna trgovina kulturnim dobrima [Smuggling and illegal trade in cultural goods]. In Ž. Bjelajac & M. Zirojević (Eds.), *Organizovani kriminalitet: Izazov XXI veka* (pp. 367–397). Novi Sad: Pravni fakultet za privredu i pravosuđe.

Durney, M. (2009). Understanding the motivations behind art crime and the effects of an institution's response. *The Journal of Art Crime*, *2*(1), 79–83.

Durney, M. (July 16, 2011). *Ludo block on "European police cooperation on art crime"*. Association for Research into Crimes against Art. Retrieved from http://art-crime.blogspot.si/2011/07/ludo-block-on-european-police.html

Europol. (2005). *2005 EU organised crime report: Public version*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/eu-organised-crimereport2005.pdf

Europol. (January 23, 2017). *3561 artefacts seized in operation Pandora*. Retrieved from https://www.europol.europa.eu/newsroom/news/3561-artefacts-seized-in-operation-pandora

Europol. (February 21, 2018). *Over 41 000 artefacts seized in global operation targeting the illicit trafficking of cultural goods*. Retrieved from https://www.europol.europa.eu/newsroom/news/over-41-000-artefacts-seized-in-global-operation-targeting-illicit-trafficking-of-cultural-goods

Golob, R. (1997). *Sistemi zaščite in varovanja oseb in premoženja* [Systems of protection and security of persons and property]. Ljubljana: Samozaložba.

Hollington, K. (July 22, 2014). After drugs and guns, art theft is the biggest criminal enterprise in the world. *Newsweek.* Retrieved from http://europe.newsweek.com/after-drugs-and-guns-art-theft-biggest-criminal-enterprise-world-260386?rm=eu

Hufnagel, S. (2015). *Police cooperation in the area of art crime: EU and international perspectives.* Retrieved from http://www.law.kobe-u.ac.jp/STP/GMAPs/ppt/0_2_1_Saskia_Maria_Hufnagel_web.pdf

Koldehoff, N., & Koldehoff S. (2004). *Aktenzeichen Kunst*. Köln: DuMont Verlag.

Kuhar, S. (2015). Umetnine in varnost – kako preprečiti kazniva dejanja zoper umetnine [Art and securit – how to prevent art crime]. In B. Flander, I. Areh, & M. Modic (Eds.), *Dnevi varstvoslovja* (pp. 109–117). Ljubljana: Fakulteta za varnostne vede.

Kuhar, S. (2017). *Preiskovanje kaznivih dejanj zoper umetnine v Republiki Sloveniji* [Criminal investigation of art crime in the Republic of Slovenia] (Doctoral dissertation). Ljubljana: Fakulteta za varnostne vede.

Kursar Trček, A. (2002). Vrste kaznivih dejanj zoper umetnine [Types of art crimes]. In M. Pagon (Ed.), *Dnevi varstvoslovja* (pp. 48–60). Ljubljana: Visoka policijsko-varnostna šola.

Lawler, A. (n. d.). National Museum, Baghdad: 10 years later. *Archaeology*. Retrieved from http://www.archaeology.org/exclusives/articles/779-national-museum-baghdad-looting-iraq

Marković-Subota, T. (August 29, 2009). Ukrali slike vredne 112 miliona evra [They stole pictures worth 112 million euros]. *Blic*. Retrieved from http://www.blic.rs/vesti/hronika/ukrali-slike-vredne-112-miliona-evra/zsle82x

Marković-Subota, T. (April 15, 2012). Tajni agent vozio »Pink pantere« [The secret agent drove the "Pink panthers"]. *Blic*. Retrieved from http://www.blic.rs/vesti/hronika/tajni-agent-vozio-pink-pantere/ptgxd99

Marn, U. (February 17, 2007). Profil tatu [The profile of thief]. *Mladina*, (7), 54–56.

Mazi, B. (October 3, 2009). Ukradene umetnine so valuta v mafijskih poslih [The stolen arts are the currency in mafia deals]. *Dnevnik.* Retrieved from http://www.dnevnik.si/objektiv/vec-vsebin/1042304016

Meško, G. (1996). Nekatere strategije kriminalne prevencije [Some of the strategies for criminal prevention]. *Revija za kriminalistiko in kriminologijo*, *47*(3), 241–254.

Meško, G. (2002). *Osnove preprečevanja kriminalitete* [Basics of crime prevention]. Ljubljana: Visoka policijsko-varnostna šola.

Ministrstvo za notranje zadeve, Policija. (2016). *Statistični podatki o kriminaliteti zoper umetnine 2005–2015* [Statistical data about art crimes in Slovenia from 2005 till 2015]. Ljubljana: Generalna policijska uprava.

Mustajbegović, S. (August 27, 2015). Nakon oružja i droge na ilegalnom tržištu najprofitabilnije je trgovati umjetninama [After weapons and drugs in the illegal market, it is most profitable to trade with art]. *STAV, 1*(25), 69–72.

O'Keefe, P. J. (2014). Difficulties in investigating crime and recovering its proceeds: An international perspective. In D. Chappell & S. Hufnagel (Eds.), *Contemporary perspectives on the detection, investigation and prosecution of art crime: Australasian, European and North American perspectives* (pp. 151–167). London: Queen Mary University of London.

Potokar, M., & Bernik, I. (2014). Vzpostavitev sistema upravljanja varovanja informacij za projekt e-arhiviranja v skladu z ZVDAGA in ZVOP-1 [Establishment of an information security management system for the e-archiving project in accordance with ZVDAGA and ZVOP-1]. In N. Gostenčnik (Ed.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: Arhivi v globalni informacijski družbi* (pp. 17–29). Maribor: Pokrajinski arhiv.

Puchko, K. (June 2, 2015). Rembrandt's The Night Watch. *Mentalfloss.com.* Retrieved from http://mentalfloss.com/article/64381/15-things-you-might-not-know-about-rembrandts-night-watch

Samardžić, R. (in press). *Umetnost i kriminal* [Art and crime]. Beograd.

Security Smoke Manual [Internal instructions]. (2013). London: Concept Smoke Sistem.

SelectaDNA. (n. d.). *The Concept*. Retrieved from https://www.selectadna.co.uk/concept

Tijhuis, A. J. G. (2006). *Transnational crime and the interface between legal and illegal actors: The case of the illicit art and antiquities trade* (Doctoral dissertation). Leiden: Leiden University. Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/4551/tijhuis%23master%23word.pdf?sequence=1

Traynor, I. (May 16, 2003). The world's dearest pinch of salt taken in 54 seconds. *The Guardian*. Retrieved from https://www.theguardian.com/world/2003/may/16/arttheft.arts

Wittman, R. K. (2010). *Priceless: How I went undercover to rescue the world's stolen treasures*. New York: Crown publishers.

Wylly, M. J. (2014). *Motives of art theft: A social contextual perspective of value.* Retrieved from http://diginole.lib.fsu.edu/islandora/object/fsu:185344/datastream/PDF/view

Zakon o zasebnem varovanju (ZZasV-1) [Private Security Act]. (2011). *Uradni list RS*, (17/11).

About the Author:

Saša Kuhar, PhD, an advisor at the Slovenian Nuclear Safety Administration is also a part-time member of the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: sasa.kuhar@fvv.uni-mb.si, sasa.kuhar1@gmail.com

*VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 20
no. 2
pp. 218–236*

Smart Cars and Information Security

Gašper Školc, Blaž Markelj

Purpose:

'Smart cars' use a great variety of data in order to operate. They obtain this from the surrounding area using sensor technology and other available resources. The drivers and passengers of such vehicles transfer different data by connecting their mobile devices with smart-vehicle systems (and by using various apps). The purpose of this paper is to investigate the problem of user data security in smart cars and to provide an insight into the general knowledge regarding such issues held by those who drive smart cars (both private and commercial users).

Methods:

The results are based on descriptive findings arising from a literature review and a research study conducted among the Slovenian population via the "1ka.si" online portal.

Findings:

The research conducted and presented in this paper shows that the use of mobile devices and their applications, which are connected to a smart car, constitute one of the biggest risks to information security in smart cars. Drivers are aware of such risks, but consider them to be a secondary concern. In addition, the lack of a uniform definition of smart cars points to a new under researched area concerning the information security of smart devices (such as cars, mobile devices etc.). Such issues pose a problem for smart car manufacturers and application developers as well as the users of mobile devices.

Research Limitations:

The main limitation of the research study is that the target population does not possess much knowledge about the discussed topic and related issues.

Practical Implications:

The research study's findings provide an insight into data security issues (which also serve as practical implications) concerning the use of smart cars.

Originality/Value:

The findings of the paper may prove useful for both the users and owners of smart vehicles in general as well as the manufacturers of mobile devices since the relevant data flows take place at the level of smart devices. The key challenge involves the owner of a single device and the level of information security knowledge they possess.

UDC: 004.056:629.331

Keywords: smart cars, information security, data security, personal data, mobile devices, connectivity

Pametni avtomobili in informacijska varnost

Namen prispevka:

Pametni avtomobili danes za svoje delovanje uporabljajo raznovrstne podatke, ki jih pridobivajo iz okolice s pomočjo senzorske tehnologije in ostalih dostopnih virov. Uporabniki pametnih avtomobilov tako prenašajo raznovrstne podatke, ko svoje mobilne naprave povezujejo s sistemi pametnih avtomobilov (tudi z uporabo različnih aplikacij). Namen prispevka je prikazati varnost uporabnikovih podatkov pri rabi pametnih avtomobilov in izpostaviti poznavanje tovrstne problematike med uporabniki pametnih avtomobilov (tako zasebnih kot poslovnih).

Metode:

Ugotovitve, predstavljene v članku, izhajajo iz deskriptivnih dognanj in raziskave, ki je bila izvedena s pomočjo spletnega vprašalnika, objavljenega na spletnem portalu »1ka.si«.

Ugotovitve:

Raziskava, izvedena v tem članku, nam je pokazala, da eno največjih tveganj informacijski varnosti pri rabi pametnih avtomobilov predstavlja uporaba mobilnih naprav in aplikacij, ki se povezujejo s pametnimi avtomobili. Vozniki tovrstna tveganja sicer poznajo, vendar so za njih sekundarnega pomena, kar tudi nakazuje, poleg neenotne definicije pametnih avtomobilov, na novo neraziskano področje informacijske varnosti pametnih naprav (avtomobili, mobilne naprave itn.). S tovrstno problematiko se srečujejo tako proizvajalci pametnih avtomobilov in mobilnih aplikacij kot tudi uporabniki pametnih naprav.

Omejitve/uporabnost raziskave:

Omejitev raziskave predstavlja predvsem pomanjkljivo znanje prebivalstva o obravnavani tematiki in njeni problematiki.

Praktična uporabnost:

Ugotovitve raziskave omogočajo vpogled v problematiko varovanja podatkov (ki prav tako služi kot praktična uporabnost) pri uporabi pametnih avtomobilov.

Izvirnost/pomembnost prispevka:

Ugotovitve prispevka so uporabne tako za vse uporabnike in lastnike pametnih avtomobilov kot tudi za proizvajalce pametnih naprav. Pretakanje podatkov namreč poteka na nivoju pametnih naprav, razlika je le, kdo je lastnik posamezne naprave in s kakšno stopnjo informacijskovarnostnega znanja posamezno napravo upravlja.

UDK: 004.056:629.331

Ključne besede: pametni avtomobili, informacijska varnost, varovanje podatkov, osebni podatki, mobilne naprave, povezljivost

1 INTRODUCTION

The impact of technological development on individuals and societies can be seen in the ways in which they transform the methods they use in their work-related activities and, thus, their lives. Nowadays, people are constantly exposed to the unstoppable development of technology in numerous fields. In the past few years, tremendous progress has been recorded as the Internet of Things (IoT) has also started to encompass vehicles. Pacheco, Satam, Hariri, Grijalva and Berkenbrock (2016) state that, apart from mobile devices and computers, the IoT has also facilitated 'smart' cities, smart homes and other smart cars. It is precisely the way these technologies are incorporated that has led to various discussions about the relatively new phenomenon of 'smart cars'. Many scientific papers attempt to definite a smart car, but none of these definitions has been universally accepted (European Union Agency for Network and Information Security [ENISA], 2016). Further, such cars also incorporate the IoT which enables their users (drivers and passengers alike) to make advanced use of the car in order to improve the user experience and increase the car's safety (ENISA, 2016). The definition used in this paper combines several different definitions (Barret, 2012; Bernik & Markelj, 2014; Chui, Löffler, & Roberts, 2010; Eskandarian, 2012; ENISA, 2016), namely: *Smart cars are vehicles which form part of the Internet of Things, function on the basis of an adapted operating system, similarly to mobile devices, and provide access to the Internet and other mobile devices without a physical connection (wirelessly). They also encompass systems that use computers, controls, communication channels and automated technologies to provide traffic safety in general and ensure transport efficiency by reducing energy consumption and the environmental impact.*

Eskandarian (2012) distinguishes between three categories of smart cars according to their degree of autonomy, i.e. smart cars with high autonomy able to drive without any driver assistance; smart cars with moderate autonomy which assist the driver as necessary; and smart cars with low autonomy (pure driving), which completely transfer all control over the vehicle to the driver and merely warn the driver of potential errors. Activities such as the ABS and stabilisation systems along with other systems and components, which constantly measure the vehicle's condition and help provide a safe and comfortable ride, run automatically in the vehicle. Further, data regarding the vehicle as controlled by the driver, or the driver's 'personalised driving style', are also collected. Schwartz (2004) states that personal data constitute an important currency in the 21st century since personal data already have a high value that is constantly growing. The Slovenian Personal Data Protection Act (Zakon o varstvu osebnih podatkov [ZVOP-1-UPB], 2004) stipulates that every individual regardless of their nationality, race, colour, religious beliefs, ethnicity etc. shall enjoy the protection of their personal data. It also defines personal data as *any data relating to an individual, irrespective of the form in which it is expressed.*

2 THE ARCHITECTURE OF SMART CARS

The European Union Agency for Network and Information Security (ENISA, 2016) has devised the typical or general architecture of smart cars, as well as the main elements of such architecture. Nakrani (2015) states that, along with the development of technology, the car has become a space for the use of media, i.e. both a communications centre and a working area. Consequently, the number of useful functions in these cars has been increasing. According to ENISA (2016), the majority of smart cars are made up of the following domains: *the power train sub-network; the chassis control sub-network; the body control sub-network; and the infotainment sub-network* (the infotainment domain), that are all connected through a common gateway. All of these domains bring a certain level of risk to smart cars, which can be distinguished in terms of their impacts on security and privacy. The infotainment domain, which is separate from the other domains, includes navigation (GPS), communications (phone etc.) and other entertainment services (audio/video unit – multimedia unit). The electronic control unit and the system of sensors enable passengers to manage a wide array of functions, such as the main multimedia unit, audio/video contents, navigation and telephone services. Apart from entertainment services (audio/video), this domain provides access to the Internet, access to traffic information, maps, digital recording instruments (tachographs) etc. The electronic control units in this domain run on the operating systems of mobile devices, such as Windows CE, Android, Tizen or WebOS. The infotainment domain also includes Bluetooth or Wi-Fi networks. The communications unit is primarily responsible for providing connectivity, but also contains the majority of security features for protecting communications such as firewalls, authentication services etc. This unit is used for diagnostics (error notifications, messages regarding software updates etc.), accident reporting and emergency calls, car theft or geo-positioning notifications (geo-fencing) etc. Apart from Wi-Fi and 3G connectivity, it provides other interfaces intended for long-distance communications, as well as wired and wireless interfaces for local use (ENISA, 2016).

Meola (2016) states that by 2021 82% of all cars sold will be smart cars, which he considers to be the most important element of the Internet of Things in the automotive industry. Moreover, Meola (2016) believes we will witness increasing development aimed at integrating various applications into cars, such as navigation applications (which are replacing the initial vehicle GPS systems), music applications (thus making car radios redundant) etc.

3 SECURITY IN SMART CARS

Although smart vehicles have only become well known in the past few years, there are already numerous publications regarding attacks against smart cars and their systems. This issue would be less pertinent if it did not threaten both the safety and data security of their users. Završnik (2010) emphasises that people are constantly subjected to different types of control, i.e. through their mobile phones, RFID objects and documents, as well as vehicle positioning systems. He also states that our locations, communications and, thus, our needs, desires and interests are meticulously analysed, meaning we are (potentially) subjected to profiling and exposed to several threats with respect to personal data. However, such threats not only jeopardise users but also affect manufacturers who are then forced to deal with numerous vehicle recalls due to the emergence of threats and presence of vulnerabilities. Bernik and Meško (2011) add that knowledge of the situation and awareness of the threats existing in cyberspace (which also includes smart cars) are crucial if we wish to reduce the impact of such threats on individuals and enterprises. A range of institutions, including ENISA, are striving to persuade car manufactures to introduce so-called best practices to help ensure the highest level of smart car security and thereby protect them from the many cyber threats they are constantly exposed to. Yet, the security or protection of smart cars depends on every single component and system, which also includes cloud services, applications, vehicle components, as well as a host of maintenance and diagnostic tools. It is also worth mentioning that the cyber security of smart cars does not merely affect the security and privacy of those using such vehicles, but also has a strong impact on security generally. For the manufacturers of smart cars, cyber security continues to entail the greatest challenge and highest cost (ENISA, 2016).

According to ENISA (2016), numerous experts in the automotive industry and particularly in smart cars have developed three categories of best practices. These include policies, standards and organisational measures and security functions. Payne III (2017) states that a car may contain enormous quantities of data, something its user may not even be aware of. When we wish to connect our phone to a smart car, the system always displays a notification asking us whether we wish to transfer data from our phone to the system of the vehicle. Transferred data may include text messages, calls and various other data. Even if the user rejects the vehicle's offer to exchange data, the vehicle may still record data regarding the device it has connected to. Thus, a smart car data may be unaware that the vehicle may even record data on the number of times they opened or closed car doors and switched on the lights, information about the route they entered into the navigation system, their favourite locations and locations that have been saved by the vehicle. The fact such data may help in the investigation of criminal offences (for instance, terrorism) is a positive aspect of their recording and storage. Payne III (2017) also states that users are unaware of the quantity of data a smart car can store, which is why the mere sending of an image of a driver's licence, credit card or even the credit card number alone can give an unauthorised person accessing such data an opportunity to cause an unfortunate event, which could also entail identity theft or financial damage. Peppet (2014) adds that the habits, routines and everyday activities of smart car users are also recorded. He notes that insurance companies may be able to use such data to determine the quality and method of a person's driving which could, at least theoretically, reduce the costs of insurance. Silberg, Plesco, Rotman and Le (2016) emphasise that smart cars record masses of information and data concerning drivers' routines and tendencies, as well as current data about the car and its diagnostics. This enables car manufacturers to obtain new insights since they become familiar with individual drivers' specific needs, their behaviour and the ways in which they control the car. On one hand, this allows manufacturers to increase the safety and security of their vehicles, yet it also provides them with an opportunity to monetise such data. They also state that manufacturers who collect such data may be able to support their existing smart car users in not merely purchasing a vehicle, but also for other services like 'premium' parking services, car transport and rental services, battery charging and refuelling services etc.

4 THREATS

Browne (2016) contends that most people do not have any concerns regarding cyber security when using smart cars and other devices connected to the Internet of Things. The problem arises from the fact that consumers wish for ever-greater connectivity of their devices with the outside world from any location, leading to potential vulnerability of the system and, thus, of their privacy. This not only concerns smart cars, which are able to connect to home-security systems, smart TV sets, smart refrigerators and other smart devices, but also smart houses and apartments, as well as the personal data stored on such devices. All of them are connected via numerous networks, while their users are not necessarily aware of the vulnerability of these systems. Users tend to be more aware of security issues and the vulnerability of personal computers than those pertaining to mobile devices, which also include smart cars and other IoT devices.

Unauthorised persons may carry out the following activities (ENISA, 2016):

- - *damage/loss* (loss of information stored in a cloud, loss/leak of sensitive information – about payment, driving routines and similar when selling the car etc.);
- - *wiretapping/bugging/interception/hijacking* (repeating messages, when adequate protection measures are not in place, attackers can easily manage the braking, steering and other functions of a car);
- - *MITM* (man-in-the-middle) or session hijacking (potential financial loss, uploading of malware, obtaining a legitimate key in order to steal the vehicle, network data collection etc.);
- - *criminal offences/abuse* (denial of service (DoS, DDoS), which leads not only to network failure but also to unexpected behaviour of the vehicle; unauthorised access to the information system/network (attackers take over control of the vehicle));
- - *disclosure of confidential information*;
- - *identity fraud* (most often resulting from cloning the key aimed at misrepresenting the vehicle within the road infrastructure systems (toll payments etc.)); and
- - *malware/malicious activity* (exploiting well-known pathways for attacks against the Linux, Android and Windows environments. Such attacks are subsequently also carried out against smart cars).

Today's cars use hundreds of sensors linked to numerous inter-connected computers. These technologies not only provide comfort for their users while travelling but are also used to guarantee their safety and security. Hartfield (2017) claims that the integration of smart phones into cars is not due to constant pressure by IT services providers, but also arises from car manufacturers themselves. This which is evident from the development of their own technologies, such as BMW's Connected Drive, Volkswagen's Car-Net, Mercedes' mbrace etc. Other vulnerable systems include USB technologies, which increase the risk of potential attacks on smart vehicles (USB enables devices such as music players, navigation systems or charging components to be connected, while this particular interface is often targeted by attackers who are able to modify the USB hardware, which cannot be detected by the end-user) and may also change vehicle settings, and Bluetooth technologies that are most often used to transfer directories or contacts into the car system, but can also be used to transfer passwords and applications for later use by attackers for the purposes of wiretapping or intercepting communications, stealing personal data and other malicious acts. The integration of smart phones into cars thus contributes to additional vulnerabilities hidden in communications channels, such as 3G/4G, Wi-Fi, Bluetooth etc. Further, third-party applications downloaded by users onto their smart phones could also be extremely problematic. These applications are usually allowed certain privileges which may put users at risk. Mobile platforms, which face this issue most often, include the Apple iOS and Android system (Harfield, 2017).

McAfee (2017) states that every electronic device consists of several components produced by numerous manufacturers/suppliers. Hardware, software, developer tools, testing tools and many other systems are not the product of any single manufacturer. The issues arising from the production of such devices relate to the fact that products manufactured or assembled in this way are normally cheaper and more accessible to consumers. These production processes may lead to security risks since the manufacturers of these components do not necessarily use the same level of security applied by the manufacturers of original parts. McAfee (2017) also claims that such components must be detected and security measures taken during the following steps in the supply chain: the use of authorised distribution channels for the purchase of hardware and software used for maintaining and assembling cars; the use of a tracking system which detects critical components containing security systems; continuity of supply, which is based on a long-term policy with respect to the availability of spare parts; recording of risks stemming from production processes; control over finished products and potential risks (wrong description, falsification or forgery etc.).

Apart from physically stopping the vehicle, messing around with the air-conditioning system, ventilators and windscreen wipers, attackers can also direct their attacks elsewhere. Such attacks include car theft or causing electronic damage/disabling car functions; falsification of car data (mileage); access to personal data (mobile phone numbers, addresses, bank details, location data etc.) to be used immediately or subsequently for the purposes of extortion; wiretapping or intercepting voice and data communication between users and their cars; and access to the manufacturer of peripherals, service provider or to data regarding application providers or applications as such (Schorer, 2015).

Based on concrete examples, one could observe that the development of information security within smart cars is still an ongoing process. The first example occurred in 2017 when Smith (2017) reported an incident that had allegedly happened in London. Unknown persons used a device which can be purchased on eBay to increase the range of a key (which was located in the victim's house) of a new BMW in order to unlock the car, start its engine and steal the vehicle. This example points to the significant vulnerability of contactless keys, even among vehicles of a higher price range.

The second example was reported by Greenberg (2016) who demonstrated how two researchers in England, namely Charlie Miller and Chris Valasek, took over certain controls of a Jeep Cherokee manufactured by Chrysler. They conducted their first 'attack' in 2015 by using a unit, which is able to physically connect with a computer, in order to hack into the electronic control system, thereby accessing certain parts of the car and allowing them to remotely control particular elements (for instance, operate the windscreen wipers, turn off the braking system when the car drove slower than 8 km/h, turn the steering wheel when the gearshift lever was in reverse etc.). Following this 'attack', Chrysler recalled 1.4 million of its vehicles in order to install upgrades to prevent or disable such attacks. A year later, Miller and Valasek (in Greenberg, 2016) used a new method to hack the controller network of the same vehicle, which helped them circumvent certain safeguards and security elements that had prevented them from fully carrying out their 'attack' during their first attempt. By accessing the controller network, they were able to send a command to the vehicle from a remote location, which enabled them to take control of the entire vehicle (including braking at high speeds, reducing speed, turning the steering wheel while driving etc.). This case demonstrates that smart cars are just as vulnerable as personal computers or other mobile devices, yet attacks against smart cars may prove more threatening because they not only affect the data of drivers connected to such cars, but also their health and safety.

The third example shows that, despite a sound level of protection, the user data that are stored in the vehicle are not encrypted. Constantin (2017) states that a USB port can be used to enter malicious script which is then run by the system automatically and with full administrator rights. This was established by Gabriel Cîrlig (in Constantin, 2017) who also found unencrypted data belonging to the users of connected mobile devices (e.g. call history, text messages and email addresses, contact lists etc.) stored in the infotainment module. In addition to such data, he found other sensitive data like the list of favourite locations from or to which the car was travelling, the sound profiles of different commands, as well as GPS coordinates entered by users into the GPS unit of the infotainment module. This means that every security feature used by mobile devices therefore becomes superfluous as they are connected to the infotainment domain of the smart car examined by Cîrlig via a Bluetooth connection. He also claims the infotainment module of this particular vehicle was manufactured in Japan and represents a paradise for hackers since it uses both Wi-Fi and GPS and is based on Linux operating systems that provide full access to the terminal, while the module itself also contains numerous error-detection tools (including for the GPS system) which the developers had failed to protect (Constantin, 2017). This case depicts another example of potential threats against smart vehicle users since it is precisely the drivers (apart from unprotected data) who represent the most substantial risk as attackers are able to use a malicious USB key to access their data, hack through open Wi-Fi networks and gain real-time (live) access to location data.

5 SOLUTIONS

Given that numerous smart cars use the infotainment domain, car manufacturers are forced to incorporate different security features. These include unique personal identification numbers and specific sets of radio-frequency signals, encryption, masking, scanning, detection of anomalies, use of certificates, filtering, firewalls, intrusion detection systems, whitelists, fraud detection, encryption of data regarding network connections, protection of keys and the use of closed systems which prevent the writing of code without authorised tools (Browne, 2016). The National Highway Traffic Administration (NHTSA) adopted the Security and Privacy in Your Car Act (2015) in an attempt to ensure cyber security in vehicles. They wanted to achieve adequate protection against unauthorised access to electronic controls or to any data related to driving, such as data on location and speed, as well as data regarding the owner or passengers. Moreover, they wished to prevent any unauthorised access to the data collected and stored by electronic systems built into the vehicle (Pearson, 2017). Smart cars need an occasional software upgrade just like any other smart device, from smart phones to smart robot vacuum cleaners. Anderson et al. (2014) emphasise that such vehicles may be connected with each other, with the infrastructure or the Internet, meaning they can be exposed to cyber attacks. The increasingly improved connectivity of smart cars (Internet, USB connection, mobile phones etc.) gives rise to new security challenges and therefore to an ever-greater number of entry points that can be abused for the purpose of carrying out malicious attacks against the vehicle and (the privacy of) its users. It should also be pointed out that software updates always require access to the Internet, which gives an opportunity for computer viruses to infect the system during a completely legal software update, thus misappropriating considerable quantities of personal data belonging to the user. That is why several authors stress that connections to servers must be extremely secure. Among the myriad of threats affecting smart cars, the most important threat, i.e. the human being, must not be overlooked. Technology enthusiasts always wish to have access to different systems to obtain control over elements for which car manufacturers have prevented or disabled access. In the context of mobile phones, experts point to the phenomena of 'jail breaking' and 'rooting' that enable technology enthusiasts to gain greater access to and increased flexibility of their device. Smart cars can also fall victim to these phenomena because users will want greater efficiency or wish to use their own software, even if that means they will be putting their own physical safety and security, as well as the security of their personal data, at risk (Anderson et al., 2014).

Schober (2016) compares the prevention of cyber attacks on smart cars with the prevention of cyber attacks on personal computers: users must ensure their software and hardware are up to date; they should avoid installing devices or applications not authorised by the manufacturer; they should take note of any unauthorised interference with or intrusion into the vehicle since many intrusions into smart cars actually require physical access to cars (inserting a USB key etc.). Ward (2017) states that security ought to be provided throughout the life-cycle of cars and systems they use. Beltov (2016) claims the incorporation of the IoT in vehicles and use of smart cars' platforms provide an opportunity to view, control and adapt vehicle settings via smart phones, tablets and computers. Similar issues also arise when using third-party software and applications for such manipulations as they may pose a threat to users' personal data. Zurkus (2015) states that smart cars are technologically-advanced and computer-supported devices which are connected to navigation and entertainment systems that enable them to store personal data, which can be targeted by numerous attackers. Naturally, the question arises as to who the owner of such data is, where and how the data is shared/sent and how smart car manufacturers are protecting it (Zurkus, 2015). These issues were regulated when the European General Data Protection Regulation entered into force. While discussing privacy in smart cars, it is worth asking what kind of information and data our car actually holds. Payne III (2017) states that smart car manufacturers will undoubtedly start applying methods to conceal such information, but the method they will choose to achieve this has yet to be revealed.

6 METHODS

The research study was based on the following hypotheses:

Hypothesis 1: Male car users believe that the abuse of smart cars is more likely to lead to the misappropriation of data than female users.

Hypothesis 2: Car users believe the abuse of smart cars is most likely to lead to the misappropriation of their contact details (phone numbers, e-mail addresses etc.).

The research study was conducted through an online questionnaire made publicly available on the "1KA" online portal (www.1ka.si). The questionnaire was active for 10 days in 2017. Drivers were informed about the research study via Facebook profiles and the *Avtomobilizem.net* online forum. In terms of the geographical element of the population is in line with the period, during which the data were collected; in terms of the geographical element, the population was located in Slovenia, while in terms of the content, the population included all drivers aged between 18 and 90. The questionnaire contained questions posed in such a way to enable the researchers to obtain an insight into the knowledge, awareness and use of security solutions, as well as the awareness of threats that could materialise during the use of smart cars and affect their connectivity to other devices. Data were analysed using the SPSS software, version 22. At this point, we note that our sample is not random and therefore the results of our analysis cannot be generalised to the whole population.

The sample was selected using snowball sampling, i.e. a non-probability method, and includes 113 individuals (as shown in Table 1), 87 of whom responded to the questionnaire in its entirety while in 26 cases respondents interrupted their completion of the questionnaire, thus providing a partial response. The majority of respondents were between 19 and 30 years of age (as shown in Figure 1); 64% were male and 36% female (Table 1), with the majority of respondents stating they frequently drive a car (see Figure 2).

Table 1: Descriptive statistics of the sample – respondents' gender

		Frequency – n	Valid share (%)
Valid	Male	56	64.4
	Female	31	35.6
	Total	87	100
Missing	Interrupted	25	
	Total	26	
Total		113	

Figure 1: Descriptive statistics of the sample – respondents' age

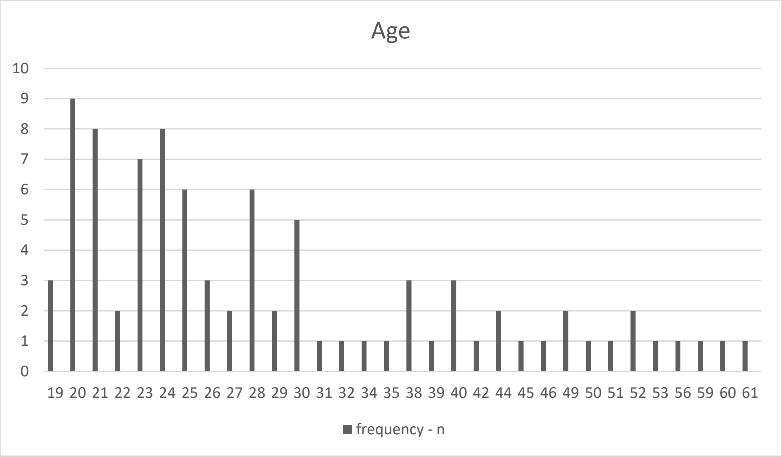
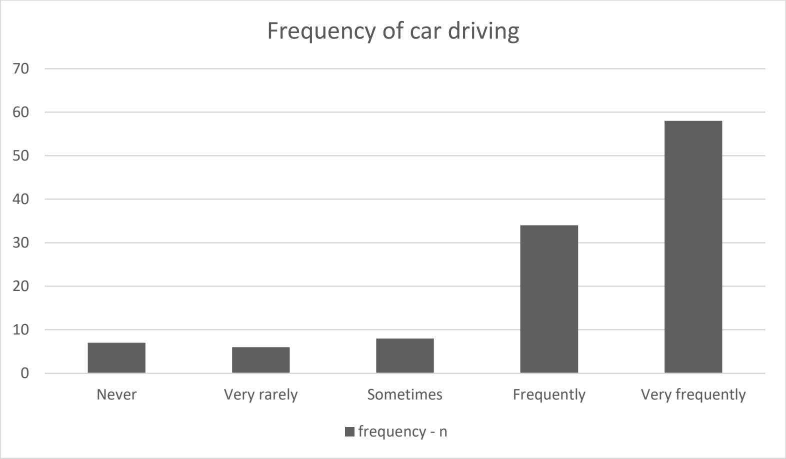


Figure 1 shows the sample mainly consisted of drivers, most of whom stated they drove cars very frequently.

Figure 2: Descriptive statistics of the sample – frequency of car driving



7 RESULTS

The research study was based on the following hypotheses:

Hypothesis 1: Male car users believe that the abuse of smart cars is more likely to lead to the misappropriation of data than female users.

Hypothesis 2: Car users believe the abuse of smart cars is most likely to lead to the misappropriation of their contact details (phone numbers, e-mail addresses etc.).

Discriminant analysis based on two groups (males and females) was undertaken in order to test the first hypothesis. This method was used to analyse a question the responses to which were provided on a 5-point Likert scale, where 1 meant "I completely disagree" and 5 "I agree completely".

Table 2: Group statistics – Discriminant analysis based on two groups

Do you agree with the following statements? It is highly likely that the abuse of a smart car will lead to the misappropriation of my:		Average	Standard deviation Unweighted	Valid N	
				Weighted	
Male	photo and/or video contents	3.15	1.008	53	53.000
	documents (work-related, private, confidential etc.)	3.06	1.117	53	53.000
	calendar entries (work-related, private)	2.91	1.024	53	53.000
	certificates (for online banking, access to business systems etc.)	3.06	1.247	53	53.000
	passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)	3.11	1.235	53	53.000
	contact details (phone numbers, email addresses etc.)	3.21	1.116	53	53.000
Female	photo and/or video contents	3.45	.827	29	29.000
	documents (work-related, private, confidential etc.)	3.41	.946	29	29.000
	calendar entries (work-related, private)	3.14	.953	29	29.000
	certificates (for online banking, access to business systems etc.)	3.52	1.122	29	29.000
	passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)	3.59	1.240	29	29.000
	contact details (phone numbers, email addresses etc.)	3.55	.910	29	29.000
Total	photo and/or video contents	3.26	.953	82	82.000
	documents (work-related, private, confidential etc.)	3.18	1.067	82	82.000
	calendar entries (work-related, private)	2.99	1.000	82	82.000
	certificates (for online banking, access to business systems etc.)	3.22	1.217	82	82.000
	passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)	3.28	1.250	82	82.000
	contact details (phone numbers, email addresses, etc.)	3.33	1.055	82	82.000

Table 2 shows the average values and standard deviations of the variables pertaining to the two groups. Compared to the first group (males), the second group (females) exhibits higher average values and lower standard deviations with respect to all variables (with the exception of *"passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.)"*, where the standard deviation is higher). These results suggest that, in comparison with their male counterparts, female respondents believe there is a greater likelihood of the abuse of smart cars leading to the misappropriation of users' data. The group of male respondents believe the abuse of a smart car is most likely to lead to the misappropriation of contact details (phone numbers, email addresses etc.), while the female respondents believe that such abuse would most likely lead to the misappropriation of passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/debit cards etc.). The comparison of the average values of both groups shows they believe that the abuse of smart cars would most likely lead to the misappropriation of contact details (phone numbers, email addresses, etc.), which was expected since smart cars are most often connected to mobile devices which synchronise users' contact details with the systems in the car.

The second hypothesis was tested by applying descriptive statistics and the confidence interval related to the type of misappropriated data. As demonstrated in Table 3, two variables had an average value above 3, meaning that on average the car drivers included in the sample agree that the connection between smart cars on one hand and mobile devices and GPS systems on the other is secure. With respect to the variable *"The connection among smart cars is secure"*, one can observe that respondents were undecided given the average value of exactly 3. They believe that connections to wireless networks, smart homes and cities are less secure since the average value of these variables is below 3. The highest average value (3.47) was attributed to the connection between smart cars and GPS systems, while the lowest average value (2.88) was observed for the connection between smart cars and smart cities. This means the respondents believe that the use of GPS systems in smart cars is the most secure form of connectivity, while the connectivity between smart cars and smart cities is perceived as the least secure.

Table 3: Descriptive statistics – connection security*

		Connections between smart cars and mobile devices are secure	Connections between smart cars and wireless networks are secure	Connections between smart cars and GPS systems are secure	Connections among smart cars are secure	Connections between smart cars and smart homes are secure	Connections between smart cars and smart cities are secure
N	Valid	85	84	83	84	84	85
Average		3.18	2.98	3.47	3.00	2.96	2.88
Standard deviation		.833	.864	.915	.905	.898	.851

**Measured on a 1 to 5 scale, where 1 means "I completely disagree" and 5 means "I agree completely"*

Table 4 shows the majority of variables have an average value above 3, which means the car users included in the sample believe there is a high likelihood of the misappropriation of the listed data, with the exception of the variable *"Calendar entries (work-related, private)"*, where the variable's average value is below 3. It is therefore possible to conclude the respondents believe that the likelihood that abuse of a smart car would to lead to the misappropriation of data from mobile devices is high.

Table 4 also shows that *"Contacts (phone numbers, e-mails, etc.)"* were attributed with the highest average value (3.32). This value falls within the boundaries of the 95% confidence interval of the mean, which has a lower endpoint of 3.11 and an upper endpoint of 3.53. However, the confidence intervals intersect for every single variable. Nevertheless, the average value of *"Contacts (phone numbers, email addresses, etc.)"* is significantly higher than the values for other variables. These results enable us to confirm that respondents believe that smart car abuse would most likely lead to the misappropriation of contact details (phone numbers, email addresses, etc.).

Table 4: The likelihood that smart car abuse would lead to the misappropriation of data*

		Photo and/or video contents	**Documents (work-related, private, confidential etc.)**	**Calendar entries (work-related, private)**	**Certificates (for online banking, access to business systems etc.)**	**Passwords and PIN codes for accessing various systems (mobile banking, business systems, credit/ debit cards etc.)**	**Contact details (phone numbers, email addresses etc.)**
N	Valid	102	101	99	99	99	100
Average		3.21	3.19	2.97	3.23	3.29	3.35
Standard deviation		.968	1.084	1.015	1.194	1.223	1.058
95% confidence interval of the mean	Lower endpoint	2.97	2.95	2.75	2.97	3.03	3.11
	Upper endpoint	3.36	3.38	3.16	3.46	3.53	3.53
5% truncated mean		3.19	3.18	2.96	3.24	3.31	3.36

**Measured on a 1 to 5 scale, where 1 stands for a very low likelihood and 5 for a very high likelihood*

8 DISCUSSION

The purpose and objectives of the presented research study were achieved by applying the selected methods and obtaining the results explained in the previous section. We were able to measure the views of smart car users. The following statements represent the key findings of our research: Respondents believe that smart cars are relatively safe since they do not seem to be aware of potential threats. They also hold relatively positive views concerning the use and usefulness of smart cars. This result can be further substantiated by the fact that many respondents expressed enthusiasm for and interest in the research study and the response rate was quite high given the large number of completed questionnaires. The second finding, which is quite surprising, relates to the fact that male respondents believe smart cars are safer than female respondents do. Nevertheless, male respondents still believe the possibilities of such threats materialising are more likely in comparison with the females. By conducting discriminant analysis, the first hypothesis was rejected because the results of the analysis show that, compared with men, women recorded higher mean values in relation to all variables, except one. This means the female respondents believe the abuse of smart cars is more likely to lead to the misappropriation of data compared with their male counterparts.

The second hypothesis was tested by applying descriptive statistics and using the sample to deduce the characteristics of the population or, to put it differently, by calculating the confidence interval for the average values of individual variables. The results show the respondents believe that their contact details (phone numbers, email addresses, etc.) would most likely be misappropriated in the event of abuse involving a smart car, which is not surprising. This means the second hypothesis may be accepted. It is, however, interesting that the respondents do not believe there would be a higher likelihood of misappropriation for passwords given that people tend to be the most protective of data that could open the gateway to other personal or business information.

At this point, we wish to reiterate that our sample is not random and therefore the results of our analysis cannot be generalised to the whole population.

The results of this research study lead to the following recommendations: The issue of information security in smart cars is widely recognised by drivers, even though the topic is relatively new and under-researched. The results show that smart cars are considered as secure, yet the respondents believe there is a high likelihood of their data being misappropriated when smart cars are abused, so it makes sense to introduce additional measures to secure the connections between smart cars and other elements of the Internet of Things (e.g. by certifying the devices connecting to the cars). Users should also be advised not to download or store important data on their mobile devices, unless it is unavoidable. However, they should ensure their devices, data and connections with a smart car are properly protected with several security features such as data and connection encryption, coupled with the use of strong passwords that allow access to individual parts of mobile devices and their data.

The number of drivers who use smart cars very frequently is quite high, indicating the great demand for such vehicles, although this might also be a consequence of the sampling method used. Trends in the automotive industry show that it will become very difficult not to drive a smart car, which is why the level of safety and security within such cars will have to grow along with the ease and simplicity of their use. The increase in safety and security should not merely include physical safety, i.e. by improving collision-warning systems and similar solutions, but also focus on information security since a number of cases show the abuse of the car's information system can allow such a vehicle to be controlled remotely, which may lead to drivers' physical injury/death.

Nevertheless, there is still a widespread belief it is highly likely that users can have their smart car misappropriated or stolen, which is why it is advised to not only improve the security of connections, but also to increase the level of security against physical intrusions permitted by a cyber attack (for instance, by copying keys via a mobile device, remotely unlocking the car using a signal amplifier etc.) and create the possibility of a security-clearance procedure before starting the engine. In doing so, the level of security will undoubtedly rise but it must be emphasised that the users of many devices do not regard such additional security elements as a good idea since they restrict use of the device, and this also applies to smart cars. Therefore, we believe that users ought to be informed and made aware of the importance of information security in smart cars.

Naturally, it is up to the car owners to decide whether to provide a greater information security in smart cars, and how. Our findings point to the fact that the likelihood of such threats materialising and the subsequent misappropriation of data remains high.

9 CONCLUSION

Smart cars are one of the latest topics of discussion regarding the IoT and smart devices, and remain an under-researched area in Slovenia. Experts have been paying ever greater attention to this issue lately as the threats and risks affecting smart cars have been growing in proportion to the introduction of these new technologies and their use. The infotainment domain or system used to display and connect to various entertainment contents that drivers do not actually need, but wish to have available in the car, remains the biggest problem in terms of protecting or securing a smart car. By attacking the infotainment domain with malicious code and/or exploiting a driver's own carelessness, attackers are able to cause greater damage than by hacking into personal computers (instead of merely stealing personal data, which may lead to significant damage, as it could jeopardise our identity, the abuse of a vehicle might also endanger the physical well-being and safety of both drivers and passengers). Since smart cars will become more accessible to everyone, the protection of drivers and passengers and the data they store on their mobile devices should not only be accompanied by introducing security features for devices and cars, but also by providing adequate training and awareness raising to all users who use smart cars in their everyday lives. Despite the abundance of security and protection mechanisms, humans remain the weakest link in providing information security in general and smart cars in particular. It is also important for the devices used by drivers and passengers and smart cars alike (that are typically manufactured by several manufacturers), to be certified to ensure a higher level of protection. At the same time, drivers should be informed of these issues when buying or selling such cars. Smart cars should be used cautiously and safely, just like any other mobile devices or computers.

REFERENCES

Anderson, M. J., Kalra, N., Stanley, D. K., Sorensen, P., Samaras, C., & Oluwatola, A. O. (2014). *Autonomous vehicle technology: A guide for policymakers*. Santa Monica: RAND Corporation.

Barret, J. (October 5, 2012). *The internet of things TEDxCIT* [Video]. Retrieved from https://www.youtube.com/watch?v=QaTIt1C5R-M

Beltov, M. (2016). *Smart cars and security - the game of risks.* Retrieved from https://bestsecuritysearch.com/smart-cars-security-game-risks/

Bernik, I., & Markelj, B. (2014). Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo [Ensuring the security of information by understanding user behaviour on a mobile device]. *Varstvoslovje, 16*(1), 5–15.

Bernik, I., & Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto [Internet study of familiarity with cyber threats and fear of cybercrime]. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Browne, W. (2016). *Internet of things devices increases cyber vulnerability of vehicles* (Master's thesis). Utica: Faculty of Utica College.

Chui, M., Löffler, M., & Roberts, R. (2010). The internet of things. *McKinsey Quarterly*, (March). Retrieved from https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things

Constantin, L. (November 16, 2017). Researchers hack car infotainment system and find sensitive user data inside. *Motherboard.* Retrieved from https://motherboard.vice.com/en_us/article/3kvw8y/researchers-hack-car-infotainment-system-and-find-sensitive-user-data-inside

Eskandarian, A. (2012). Introduction to smart vehicles. In A. Eskandarian (Ed.), *Handbook of smart vehicles* (pp. 2–13). Washington: Center for Smart Systems Research in the George Washington University.

European Union Agency for Network and Information Security [ENISA]. (2016). *Cyber security and resilience of smart cars: Good practises and recommendations.* Retrieved from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/at_download/fullReport

Greenberg, A. (January 8, 2016). The Jeep hackers are back to prove car hacking can get much worse. *Wired.* Retrieved from https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Hartfield, S. R. (2017). *21st century automobiles: Vulnerabilities, threats, cyber security and digital forensics* (Master's thesis). Utica: Faculty of Utica College.

McAfee. (2017). *Automotive security best practises.* Retrieved from https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

Meola, A. (December 20, 2016). Automotive industry trends: IoT connected smart cars & vehicles. *Business Insider*. Retrieved from http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10

Nakrani, P. K. (2015). *Smart car technologies: A comprehensive study of the state of the art with analysis and trends* (Master's thesis). Tucson: University of Arizona.

Pacheco, J., Satam, S., Hariri, S., Grijalva, C., & Berkenbrock, H. (2016). IoT security development framework for building trustworthy smart car services. In L. Zhou, L. Kaati, W. Mao, & G. A. Wang (Eds.), *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data* (pp. 237–242). Piscataway: IEEE.

Payne III., L. R. (2017). *Vehicle manipulation and forensics* (Master's thesis). Utica: Faculty of Utica College.

Pearson, T. E. (2017). *The need for encryption and secure systems within vehicles* (Master's thesis). Utica: Faculty of Utica College.

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review, 93*(85), 85–178.

Schober, S. (2016). *Cybersecurity and the future of smart cars*. Retrieved from http://www.ibmbigdatahub.com/blog/cybersecurity-and-future-smart-cars

Schorer, M. (2015). *Connected car business brief series*. Retrieved from https://www.vmware.com/ciovantage/wp-content/uploads/2015/12/ConnectedCar-2-Security.pdf

Schwartz, P. M. (2004). Property, privacy, and personal data. *Harward Law Review, 117*(7), 2056–2128.

Security and Privacy in Your Car Act (SPY Car Act). (2015). *Library of Congress (114th Congress).* Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/1806

Silberg, G., Plesco, R., Rotman, D., & Le, D. (2016). *Your connected car is talking. Who's listening?* Delaware: KPMG LLP. Retrieved from https://assets.kpmg.com/content/dam/kpmg/id/pdf/2017/04/id-your-connected-car-is-talking.pdf

Smith, L. J. (October 17, 2017). Car thieves steal £50,000 BMW in seconds – is your car at risk too? *Express.* Retrieved from https://www.express.co.uk/life-style/cars/866987/car-theft-hack-keyless-entry-video-BMW-stolen

Ward, B. D. (2017). *Automotive cybersecurity - redifining war driving* (Master's thesis). Utica: Faculty of Utica College.

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1) [Data Protection Act]. (2004, 2005, 2007). *Uradni list RS,* (86/04, 113/05, 51/07, 67/07).

Završnik, A. (2010). Tehnično nadzorovanje vsakodnevnega življenja – postdisciplinske teoretične perspektive [Technical surveillance of everyday life – "post disciplinary" theoretical perspectives]. *Revija za kriminalistiko in kriminologijo, 61*(2), 178–190.

Zurkus, K. (March 25, 2015). Are smart cars putting our safety at risk? *CSO.* Retrieved from https://www.csoonline.com/article/2900654/data-protection/are-smart-cars-putting-our-safety-at-risk.html

About the Authors:

Gašper Školc, B.A. in Information Security Studies, master's student at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: gasper.skolc@student.um.si

Blaž Markelj, PhD, assistant professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: blaz.markelj@fvv.uni-mb.si

Assaults on Police Officers in Slovenia Between 2007 and 2017

VARSTVOSLOVJE,
Journal of Criminal Justice and Security,
year 20
no. 2
pp. 237–258

Srečko Felix Krope, Vladimir Ilić

Purpose:

The paper examines the trend of assaults on police officers between 2007 and 2017 period based on annual reports produced by the Ministry of the Interior of the Republic of Slovenia, Police. We analysed these trends by considering movements in the number of assaults. The purpose of the paper is to determine the trend of assaults on police officers over a longer period of time.

Methods:

We analysed the annual reports of the General Police Directorate concerning assaults on police officers. We considered annual reports containing data on assaults from 2007 to 2017 and assessed the trends and questions of legality.

Findings:

The highest number of assaults on police officers was seen between 2009 and 2013, with a steady decline being registered after 2013. The number of injured police officers, especially in 2012 and 2011, was quite significant. When determining the reasons for this figure, we found that this was a time of major protests in various Slovenian cities and interventions in Roma settlements that involved mass assaults on police officers.

Research Limitations/Implications:

The research was conducted using data collected about all assaults on police officers reported between 2007 and 2017. We do not know how many attacks went unreported.

Practical Implications:

The results are useful for predicting the trend of assaults on police officers and identifying ways to increase the safety of police officers and persons during police procedures.

Originality/Value:

Previous analyses of assaults on police officers were conducted for individual years only and not for any longer period.

UDC: 351.741

Keywords: police, police officers, assaults, education and training, police powers, police procedure, criminal offences

Napadi na policiste v Sloveniji v obdobju 2007–2017

Namen prispevka:

V prispevku proučujemo trend napadov na policiste v obdobju 2007–2017 na podlagi letno izdelanih poročil Generalne policijske uprave. Analizirali smo trende napadov z vidika porasta ali padca števila napadov. Namen je ugotoviti gibanje števila napadov na policiste v daljšem časovnem obdobju.

Metode:

Opravili smo analizo letnih poročil Generalne policijske uprave s področja napadov na policiste. Analizirali smo letna poročila s podatki o napadih od leta 2007 do leta 2017 ter ugotavljali trende in zakonitosti.

Ugotovitve:

Največ napadov na policiste je bilo v obdobju 2009–2013 in šele po tem letu gre za dejanski stalen padec. Izstopajoč podatek je tudi število poškodovanih policistov, zlasti v letih 2011 in 2012. Pri iskanju vzrokov za takšno število najdemo obrazložitev, da je šlo za obdobje množičnih protestov v slovenskih mestih in na račun intervencij v romskih naseljih, kjer je prihajalo do množičnih napadov na policiste.

Omejitve/uporabnost raziskave:

Raziskava je bila opravljena na podlagi zbranih podatkov o vseh napadih na policiste v obdobju 2007–2017. Število neprijavljenih napadov ni znano.

Praktična uporabnost:

Rezultati so uporabni pri spremljanju napadov na policiste ter ukrepih za povečanje varnosti policistov in oseb v policijskem postopku.

Izvirnost/pomembnost prispevka:

V dosedanjem obdobju so bile opravljene analize napadov na policiste za posamezno leto ali krajša obdobja, ne pa tudi za daljše časovno obdobje.

UDK: 351.741

Ključne besede: policija, policisti, napadi, izobraževanje in usposabljanje, policijska pooblastila, policijski postopki, kazniva dejanja

1 INTRODUCTION

Foreign and Slovenian literature reveal that assaults on police officers have become ever more frequent, with some authors (Novak, 1996) defining the profession as one of the most hazardous. Research on this aspect conducted around the world (Lester, 1985) and in Slovenia (Gomboc, 1996) has so far considered the usual descriptive statistics. The aforementioned authors used simple descriptive methods to establish: which group of police officers is most endangered; when is the most critical time for assaults to happen; during which official actions do assaults occur, and the most common places where are assaults made.

Based on analyses, various authors (Bristow, 1963; Chapman, 1986) make recommendations to police officers that should be considered during police procedures to help reduce the probability of becoming victims of assault. Ignjatović (2006) interviewed suspects or people convicted of such criminal offences to establish the reasons officers are assaulted. Some authors (Dempsey & Forst, 2005; Vidmar, 1993) have sought to affect the process of educating and training police officers based on research.

The findings of a number of authors (Pinizzotto, Davis, & Miller, 2000) show that police officers were most often victims of assault while performing tasks in the areas of road transport, maintaining peace and order, and investigating criminal offences etc. Perpetrators most commonly use physical force, tools or weapons and means of transport to make such assaults. To deter assaults, police officers use coercive measures, typically physical force and their batons, handcuffing and binding, gas spray, and firearms.

While studying coercive measures and assaults, Terrill, Leinfeld and Kwak (2008) established several types of resistance by persons undergoing police procedures. They identified the mildest form as verbal resistance, including comments and insults made by the person in a procedure, passive resistance when a suspect tries to avoid a procedure by dragging or pushing, and active resistance entailing the attempted or actual assault of an officer.

In examining assaults on officers during 2005 and 2006 on the basis of 363 submitted criminal charges, Krope and Lobnikar (2015) established that a total of 531 officers aged 21 to 50 years had been injured or assaulted. Most of these officers had 5 years of active service. The longer one's active service, the lower the probability of a police officer becoming the victim of assault. Assaults on police officers were most frequent in small police directorates, i.e. Nova Gorica and Novo mesto, where every 5th or 6th police officer had been assaulted. Based on an analysis, they gave some proposals to reduce the number of assaults on officers. These proposals focus on the appropriate structure of patrols, suitable technical equipment and the use of protective equipment in the workplace, as well as psycho-social support for assaulted officers. Attackers and officers were often physically injured during criminal offences. In individual periods, more police officers than attackers were injured during such offences. Therefore, the public has developed certain opinions and trust regarding the police that primarily affects:

- the population's satisfaction with police services;
- the reputation of the police;
- the number of complaints about police work;
- the use of coercive measures; and
- injuries to civilians or police officers.

Krope and Ilić (2017) studied Slovenian police officers' use of coercive measures in the 2008–2016 period. They found there was a constant statistical decline in the number of assaults on police officers, but there were also assaults that caused the death of officers. The number of injuries related to use of coercive measures is decreasing, meaning that officers are employing social skills while exercising their powers leading to less or no resistance, or they are more professional when applying coercive measures.

Building on various studies on the quality of police procedures, Krope (1998) emphasised the importance of standardising and classifying police procedures as two factors that contribute to improving the quality of police services. Improved police procedures have the effect of reducing the number of complaints concerning police procedures and the number of assaults on officers, while improving public opinion with respect to the police and safety. The data used in this paper refer to police procedures that have proven most problematic in the research and analyses conducted by individual departments of the Ministry of the Interior. These procedures mostly involve:

- identification;
- security checks;
- handcuffing and binding;
- escorting and detaining persons; and
- the use of weapons.

Based on annual Police reports about assaults on police officers, Mravlja and Krope (2007) established the reasons for them, dividing them into internal and external causes. Internal causes include indecisiveness, an unsuitable approach and inappropriate communication (where a police officer adds to the severity of the conflict), inappropriate intervention management, notification and sending of data about a violation, incompetence and inappropriate protection of procedures. External causes include the attacker's aggressiveness due to inebriation, disagreements concerning a police officer's decision, small fines, the ineffectiveness of punitive policy, revenge, and people's ignorance of police powers.

The term "assault on a police officer" in this paper encompasses the following criminal acts:

- an individual obstructing an official act or taking revenge against an official
- assault on an official while performing security duties;
- collaboration in a group to prevent an official from carrying out an official act; and
- incitement to rebellion.

Criminal offences are given the same terms in the Criminal Code from 2004 and the one from 2008, yet while the provisions of the articles have entirely the same content, the numbers of the articles are altered. For instance, the obstruction of an official act or an act of revenge against an official under Article 302 of the Criminal Code (Kazenski zakonik, 2004) or Article 299 of the Criminal Code (Kazenski zakonik, 2008).

All the mentioned criminal offences in the Criminal Code are included under "Criminal offences against public order and peace". Assaults on police officers do not include other acts by persons during procedures with police officers who did not observe a legitimate order and actively or passively resisted; their actions are defined as offences pursuant to the Protection of Public Order Act (Zakon o varstvu javnega reda in miru, 2006) or the Act on Criminal Offences against Public Order and Peace (Zakon o prekrških zoper javni red in mir, 1974) then valid, i.e. as a minor offence, not a criminal offence.

In the aforementioned criminal offences, the victims may include police officers and other officials carrying out certain official duties based on powers granted to them by law or regulations issued based on the law (Article 126 of the Criminal Code (Kazenski zakonik, 2004)). This paper focuses on criminal offences when the injured persons are police officers. Article 16 of the Criminal Code (Kazenski zakoni, 2008) describes a criminal offence as follows: "A criminal offence shall mean unlawful conduct that the statute due to necessary protection of legal values determines as a criminal offence, while defining the elements thereof and the sentence for the guilty perpetrator".

Article 6 of the Minor Offences Act (Zakon o prekrških, 2011) establishes that a minor offence is an act violating a law, a government decree, a decision of a self-governing community, or of a local community which is as such determined as a minor offence, and the sanction for the minor offence is also identified. It further prescribes that in the minor offence procedure the provisions of the Criminal Code shall be used with regard to self-defence, extreme urgency, urgency and threat, insanity, intent, negligence, mistake of fact and mistake of law, collaboration in a criminal offence and the time and place of the commission of a criminal offence if the Minor Offences Act does not determine otherwise.

2 CRIMINAL OFFENCES – ASSAULT ON POLICE OFFICERS

2.1 Definition of Basic Terms

To understand the contents of this paper, we explain some of the terms appearing in the text and subject to our study. We explain them to ensure the subject matter is clear and unambiguous. We base our findings on police tasks and powers.

Article 4 of the Police Tasks and Powers Act (Zakon o nalogah in pooblastilih policije, 2013) defines police tasks and police powers which are also determined in other regulations, such as the Minor Offences Act (Zakon o prekrških, 2011), Criminal Procedure Act (Zakon o kazenskem postopku, 2012) and other specific regulations.

Police powers comprise concrete powers granted to police officers for them to successfully complete their tasks. These powers include an officer's right to use a specific power in certain cases to successfully perform a task, while the person or authority against whom the power is used must act in accordance with police powers (Žaberl, 2001).

Various terms used in this text are defined below:

- criminal offence – a minor offence;
- official – a police officer; and
- order, resistance – assault.

The terms are presented in the manner they are described in individual legal and executive acts regulating police work.

Article 16 of the Criminal Code (Kazenski zakonik, 2008) describes a criminal offence as follows: "A criminal offence shall mean unlawful conduct that the statute due to urgent protection of legal values determines as a criminal offence, while defining the elements thereof and the sentence for the guilty perpetrator". This provision somewhat follows Bele's (2001) claim since it slightly changes the former meaning of a criminal offence, i.e. stating that a criminal offence is a human illegal act determined by law for the necessary protection of legal values as a criminal offence, and at the same time determines its features and the penalty for a perpetrator. Article 16 introduces slightly different and more specific features of criminal offences. As for "criminal offence", Article 16 introduces the following:

- it is a human illegal act (the previous version determined that a criminal offence is an illegal act);
- to ensure the necessary protection of legal values (before, it was only due to non-security); and
- it stipulates the penalty for perpetrators (before, it stipulated only the penalty for a criminal offence).

Article 6 of the Minor Offences Act (Zakon o prekrških, 2011) provides that a minor offence is an act violating a law, a government decree, a decision of a self-governing community, or of a local community determined therein as a minor offence, and the sanction for the minor offence is also determined. It further determines that in the minor offence procedure the provisions of the Criminal Code shall be used with regard to self-defence, extreme urgency, urgency and threat, insanity, intent, negligence, mistake of fact and mistake of law, collaboration in a criminal offence and the time and place of the commission of a criminal offence if the same act does not determine otherwise.

Article 126 of the Criminal Code (Kazenski zakonik RS, 1994) determined who is an official, and the Criminal Code (2008) stipulates this in Article 99. It states that officials include a member of the National Assembly, a member of the National Council, a person carrying out official duties or exercising a public function with management powers and responsibilities within a state authority; any other person exercising official duties by authorisation of a law or by-law. According to Žaberl (2001), persons who perform certain official duties usually hold the status of an official. Such persons are gamekeepers, fishery keepers, inspectors working at inspection services and others. In the police, some officials have special duties and special rights for exercising professional (police) tasks, and also hold special powers. They also acquire the status of an authorised official.

The power to "order" is defined in Article 39 of the Police Tasks and Powers Act (Zakon o nalogah in pooblastilih policije, 2013) and stipulates that police officers may give instructions by way of an order to natural persons, legal entities and public authorities and demand they act or refrain from acting in order to be able to implement police tasks laid down in this Act or other regulations in line with the law. Police officers give direct orders verbally, by using technical means or in any other appropriate manner.

The powers are divided into five sets, with Žaberl (2001) giving the following specific examples:

- The protection of people's lives
  Such circumstances are typical and understandable because the protection of life is the primary and most important police task. An attempt to stab someone endangers life. A police officer gives an order to the person involved to immediately end the assault and drop the knife. Every order is followed by a warning concerning what will be done if the person does not obey.

- The protection of property against destruction, damage, theft and other forms of harm
  These cases are quite common in police officers' day-to-day work. A police officer who catches a person spraying graffiti on walls or in any other way destroying property gives an order to stop.
- Ensuring road traffic safety
  Police orders in road traffic are typically given using signs. A traffic police officer at a crossroads gives orders with hand signals, a whistle etc. These signals are understood by everyone because they are internationally recognised and valid signals. The "STOP" sign or illuminated "STOP" sign on the back of a police vehicle instructs road traffic participants to pull over. Police officers may give orders verbally, for example: "You are prohibited from driving further", "Step out of the vehicle" and so on.
- When riots, unrest and similar other public order violations have to be prevented
  There are many such cases in police practice. The most common is an example of police intervention in a fight. The first act of the police officer is an order such as: "Stop the fight, otherwise we will use physical force". If the people involved do not observe the order, police officers take the steps warned about.
- When the harmful results of natural and other accidents must be eliminated
  Harmful effects are caused by natural and other accidents such as floods, fires, epidemics, explosions, major car accidents etc. Authorities competent for ensuring protection against natural and other accidents are authorised to make certain decisions, and the Police is obliged to execute them. In such cases, a police officer issues an order to a group of people that no one may come close to the endangered area or similar. In such cases, the police are mostly bound by the preliminary decisions of authorities competent for protection against natural and other accidents. In most of these events, police officers give orders by using technical means (for instance with megaphones, "STOP – POLICE" plastic tape ...), and also verbally in the direct vicinity of the area.

Many tasks undertaken by police officers are repressive and coercive against people in a procedure. A police officers prohibits or orders something (e.g. prohibits any further driving or orders a person to come to the police station etc.). This involves intervening in a person's freedom because they may no longer do as they wish and must submit themselves to the police officer's order. According to Žaberl (2001), a person in a procedure does not always want to submit to the police officer's will, often making them disobedient for various reasons such as:

- the person thinks the police officer's order or prohibition is not based on law;
- the person thinks that no one may prohibit or order them;
- the person always has a hostile attitude to authority and the representatives of authorities;

- the person knows the police officer personally so they think it is offensive to be treated like that; and
- the person is surrounded by their friends so they are ashamed of having to obey a police officer.

Article 3 of the Police Tasks and Powers Act (Zakon o nalogah in pooblastilih policije, 2013) determines and defines resistance, forms of resistance and assault on a police officer. It stipulates that resistance is any unlawful conduct by a person that impedes police officers in their carrying out of a lawful police task or prevents them from doing so. Passive resistance includes when a person disregards a police officer's lawful order or who, through unlawful conduct, impedes police officers from performing a lawful police task or prevents them from doing so by sitting or lying down, turning away or by behaving in a similar manner. Active resistance is resistance involving the use of weapons, dangerous implements, other objects or substances, animals or physical force, whereby a person who offers resistance intends to stop police officers executing a lawful police task. Active resistance also includes incitement to resist, flight of a person, and endangerment. Endangerment means that a person, in their posture, gestures or conduct, indicates they will attack a police officer or another person or building protected by a police officer. Assault is any unlawful direct activity of a person using physical force, an animal, a weapon, an implement or any other object or substance with the aim of injuring or taking the life of a police officer or another person or endangering the security of a building protected by a police officer.

2.2 Obstructing an Official Act or Taking Revenge Against an Official

In this paper, criminal offences under the aforementioned article committed since 2007 are examined. The Criminal Code (Kazenski zakonik, 2004) defined this offence in the way described above and stipulated a fine. The Criminal Code (Kazenski zakonik, 2008) that entered into force on 1 November 2008 renumbered this offence (while retaining the same name) as Article 299 and introduced some changes referring to criminal offence elements and the amount of penalty. The first paragraph stipulates three months' to three years' imprisonment for the same offence, and the Criminal Code (Kazenski zakonik, 2004) up to two years'. It also omits the second paragraph stipulating that an attempted offence is punishable. This is understandable since the general provision on an attempt in the Criminal Code (Kazenski zakonik, 2008) stipulates that an attempt is criminal if up to three years' imprisonment can be imposed or if the act explicitly determines that an attempt to commit an individual criminal offence is punishable. In some elements, the Criminal Code (Kazenski zakonik, 2008) omits the wording about organised crime groups and also introduces the tasks of inspection supervision. For an offence under Article 302/3 of the Criminal Code (Kazenski zakonik, 2004), the Criminal Code (Kazenski zakonik, 2008) increases the penalty from six months to five years. Other provisions or elements of a criminal offence remain the same. The fifth paragraph of the mentioned article is important because it protects an official when no longer on duty, stipulating that a person is equally punished for taking revenge on an official who performs or has performed actions in a violations procedure or criminal prosecution, exercises the tasks of the police, performs acts of administrative inspection supervision, conducts or has conducted an investigation, or judges or has acted as a judge in criminal proceedings, for acts performed by himself or another official within his rights, so as to put in danger the life, limb, personal security, or property of the official or his/her close relatives.

According to Deisinger (2002), the prevention of an official act refers to an act an official intended to exercise within their rights. These are the rights of an official determined in appropriate regulations or within the specific tasks ordered within the scope of such regulations.

2.3 Assault on an Official While Performing Security Tasks

Due to the renumbering, the Criminal Code (Kazenski zakonik, 2008) treats a criminal offence as in Article 300 as well as in three paragraphs with individual amendments. A new element is added, i.e. when an official is protecting a person or exercises tasks in connection with the execution of criminal sanctions. In the first paragraph, it raises the penalty of imprisonment from six months to three years. In the second paragraph, it increases the term of imprisonment from six months to five years.

According to Bele (2001), this offence can be committed by anyone merely by intention. The perpetrator thinks that an official is exercising the tasks indicated in the first paragraph of this article or that another person is assisting this official in doing so. The perpetrator's motive is irrelevant. The offence is shown as an assault or a serious threat of assault. An assault means the use of physical force against an official or person assisting the official. An assault pursuant to paragraph one is only committed if no other forms as envisaged by the second paragraph are entailed (threat with a knife, misconduct, minor physical injury) because the criminal offence is then committed as per the second paragraph of this article. Threat under the first paragraph encompasses threat with the use of physical force (not weapons because in such cases a criminal offence under the second paragraph is committed). An official or any person assisting the official in the exercise of the task can be the subject of an assault.

The assistance of another person can take any form, physical or psychological (e.g. notifications, advice etc.). The offence of assault on an official while performing security tasks is differentiated from the offence of preventing an official act and taking revenge against an official in the fact that the criminal offence of assault involves an assault intended to endanger an official or their assistant. A summary procedure is used for this criminal offence.

2.4 Participation in a Group Obstructing an Official in Their Performance of an Official Act

Article 301 of the Criminal Code (Kazenski zakonik, 2008) mentions the elements needed for the commission of this offence by increasing the imprisonment as per the first paragraph, i.e. from three months to two years. As per the second paragraph, it stipulates imprisonment from six months to three years.

Bele (2001) states that a criminal offence pursuant to this article may be committed by anyone participating in a group, as determined in the first paragraph of the article, and the act can only be committed intentionally. The perpetrator believes that he is collaborating in a group for the purpose of obstructing an official in the performance of an official act. The offence is the same as in the offence of preventing an official act or taking revenge against an official. The joint actions of the group entail the use of force or the threat of using force. A completed act of obstructing an official act or taking revenge against an official and attempted revenge are deemed equivalent. Coercing an official to perform an official act has to be done quite oppositely because an attempt to do this is not punishable under the first paragraph of this article. A group contains an indefinite number of people.

According to Bele (2001), a group comprises a large number of people, at least five. A group can be founded to obstruct an official act, or a lawful association of people (e.g. at various manifestations, sport competitions, meetings) can turn into a group that acts with the purpose under the first paragraph of the mentioned article. It is characteristic of such a group that it has assembled with a special intention, i.e. to obstruct an official in performing an official act or to coerce an official to perform an official act. A person who leaves the group before such conduct starts or joins the group after the conduct is finished is not deemed a participant. The leader of a group who commits an offence pursuant to the first paragraph is deemed to have committed a serious offence under the second paragraph. The group leader is not a leader in the sense of organising a criminal group. It is not necessary for the leader to have organised the group; it is important the person was the leader of the group during the commission of the offence under the first paragraph, and that she/he acted as the actual leader of the group and similar. If it can be proven that an individual committed an offence according to the first paragraph of Article 302 (obstruction of an official act ...), this individual will also be held responsible for this offence, and all other participants of the group will be held responsible for committing an offence under Article 304 (collaboration in a group ...).

2.5 Incitement to Rebellion

Article 302 of the Criminal Code (Kazenski zakonik, 2008) covers the same offence in two paragraphs and does not define the offence very differently from the Criminal Code (Kazenski zakonik, 2004) and does not stipulate a different sanction.

According to Bele (2001), anyone may be a perpetrator of this offence, and the offence can only be committed with intent. The perpetrator is aware that they are inciting rebellion. Incitement to rebellion is similar to solicitation and encompasses all forms of solicitation, except that it is not directed against individuals but an indefinite number of people. Incitement can be directed at the activity of other people (such as violent rebellion). The offence can be committed in any way that enables realisation of the perpetrator's intent (e.g. incitement in public, incitement in the press etc.). Rebellion means conduct other than that required by a lawful decision or order or by an official. A state authority's decision or measure must be lawful; otherwise, no criminal offence is committed. The same applies to the official act of an official. The offence itself ends with the perpetrator's incitement. If such incitement has a result, the criminal offence is deemed to be committed under the second paragraph of the article. If those incited prevented an official from exercising an official act or attempted to do so, they will, as participants of a group, if such an association is assessed as such, be held liable for the criminal offence of collaborating in a group that obstructed an official in the performance of an official act as per the first paragraph of Article 304 of the Criminal Code (Kazenski zakonik, 2004). The perpetrator of an offence under the first paragraph of Article 305, who is also a participant of such an offence, will commit concurrent criminal offences under both the first paragraph of Article 305 and the first paragraph of Article 304. If this offence is committed by the perpetrator as the leader of a group, this shall be considered as concurrent criminal offences according to both the second paragraph of Article 305 and the second paragraph of Article 304. A summary procedure is used for this criminal offence.

3 METHOD

Our paper is based on data from annual reports concerning assaults on police officers prepared annually by the Ministry of the Interior of the Republic of Slovenia, and the Police. The Police structure at the local level also changed in the mentioned period with three police directorates (PDs) being abolished, i.e. the Slovenj Gradec PD, which was merged with the Celje PD, the Postojna PD, which was merged with the Ljubljana PD, and the Krško PD, which was merged with the Novo mesto PD. Data about these three PDs, i.e. from 2009 and 2010, were absorbed by those police directorates that merged with the abolished PDs. We analysed data from annual reports from 2007 to 2017. The reports were based on data from the computer records of assaults on police officers and use of means of coercion. Individual findings were compared with the papers by various authors discussing assaults on police officers in different periods. We used the Freehand curve (or Graphic) method and methods of time series to determine the trend.

4 PRESENTATION AND INTERPRETATION OF THE RESULTS

4.1 Assaults on Police Officers Occurring Between 2007 and 2017

Data were collected from police annual reports and prepared as summaries. The data collection methodology also varies every year. The data comprise findings for the previous year and instructions or guidelines on reducing the number of assaults. We cannot draw from these reports those factors that impact the assaults on police officers, as presented by Krope, Lobnikar and Pagon (2013), who drew data from every specific case.

Table 1: Number of criminal acts of assaults on police officers and number of officers assaulted between 2007 and 2017

Year	No. of assaults	No. of persons assaulted
2017	151	231
2016	163	244
2015	177	279
2014	204	316
2013	231	334
2012	284	513
2011	276	517
2010	254	361
2009	260	390
2008	204	277
2007	208	305

Source: Ministry of the Interior of the Republic of Slovenia, Police (2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016a, 2017, 2018)

All reports show that police officers were most frequently attacked on roads, in apartments, other housing premises and in their direct environment, in traffic, on hospitality premises, on sales and business premises, at public events, on official police premises etc. With regard to the areas of work, assaults most frequently occurred in relation to public peace and order, road traffic, other forms of work, criminal offences and state border surveillance (Ministry of the Interior of the Republic of Slovenia, Police, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016a, 2017, 2018).

Individual reports also provide data on the number of criminal offences of assaults on police officers by police directorate, but only concerning where the maximum and minimum assaults happened. The reports show (but not in every year's report) that most assaults in 2016 occurred in the area of the Ljubljana PD, i.e. 57 assaults, and the lowest number, i.e. 5, occurred in the area of the Koper PD. In 2014 and 2015, most assaults happened in the area of the Ljubljana PD (66, 6) and the least in the area of the Koper PD (6, 6) (Ministry of the Interior of the Republic of Slovenia, Police, 2014, 2015, 2016a).

Figure 1: Number of criminal acts of assaults and number of police officers assaulted in the same period

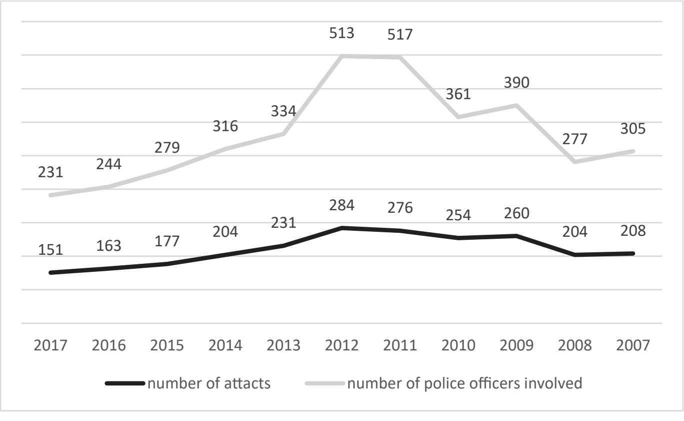


Figure 1 shows a clearer image than Table 1 because the graphic image reveals that most assaults on police officers happened between 2009 and 2013. Since 2013, a constant decline has been noted. The number of injured police officers, especially in 2012 and 2011, was quite significant. When determining the reasons this figure, we found this was a period of major protests in various Slovenian cities and interventions in Roma settlements.

The report (Ministry of the Interior of the Republic of Slovenia, Police, 2016a) shows an almost 7.9% drop in the number of criminal offences against police officers compared to 2015, and that there were 12.5% fewer injured officers; however, the report expresses concern regarding the increasingly aggressive forms of assaults on officers. The report highlights an assault on an officer who coincidentally attended the scene of a doctor's murder, where the perpetrator then shot the officer and killed him. The perpetrator also shot another officer who came to intervene, causing serious physical injury to that police officer.

A detailed review of criminal offences of assaults on police officers can be seen in the annex to the 2017 report (Ministry of the Interior of the Republic of Slovenia, Police, 2017) that displays relevant offences by units, as shown in Table 2.

Table 2: Criminal offences by units

	2016		2017		
Organisational unit	**No. of criminal offences**	**Share of investigated criminal offences**	**No. of criminal offences**	**Share of investigated criminal offences**	**Increase/ decline in criminal offences**
Celje Police Directorate	23	100.0%	29	100.0%	26.1%
Koper Police Directorate	3	100.0%	11	90.9%	266.7%
Kranj Police Directorate	12	100.0%	10	100.0%	-16.7%
Ljubljana Police Directorate	57	98.2%	42	97.6%	-26.3%
Maribor Police Administration	19	100.0%	15	100.0%	-21.1%
Murska Sobota Police Directorate	17	100.0%	9	100.0%	-47.1%
Nova Gorica Police Directorate	6	100.0%	7	100.0%	16.7%
Novo mesto Police Directorate	20	100.0%	21	100.0%	5.0%
Total	157	99.4%	144	98.6%	-8.3%

Source: Ministry of the Interior of the Republic of Slovenia, Police (2017, 2018)

In both years, most criminal offences happened in the areas of the Ljubljana, Celje, Novo mesto and Maribor PDs. Until 2010, the same data could have given different results because three police directorates were abolished in 2011, i.e. the Slovenj Gradec, Postojna and Krško PDs. The abolished units were merged with the Celje, Ljubljana and Novo mesto PDs, respectively.

Table 3: Criminal offences by months

	2016	2017	
Month of the final document	**No. of criminal offences**	**No. of criminal offences**	**Increase/decline in criminal offences**
January	7	6	-14.3%
February	9	10	11.1%
March	3	12	300.0%
April	12	10	-16.7%
May	24	14	-41.7%
June	15	13	-13.3%
July	10	8	-20.0%
August	6	15	150.0%
September	16	13	-18.8%
October	13	14	7.7%
November	21	9	-57.1%
December	21	20	-4.8%
Total	**157**	**144**	**-8.3%**

Source: Ministry of the Interior of the Republic of Slovenia, Police (2017, 2018)

Table 3 presents data by months about finalisation of the paperwork, i.e. on the lodging of a criminal complaint with the State District Attorney's Office (SDA). Therefore, we cannot define criminal offences by months. We cannot obtain precise information from this table and only refer to finalisation of the paperwork. Krope et al. (2013) found that most criminal offences are committed in October and the least in December.

In terms of days of the week, the report (Ministry of the Interior of the Republic of Slovenia, Police, 2017) shows that most criminal offences/assaults in 2016 happened on Sundays (31), Thursdays (29) and Tuesdays (24). In 2017, the distribution by days is slightly different since most criminal offences of assaults were committed on Wednesdays (29), Fridays (28) and Sundays (22). Most perpetrators were men in the age group 34 to 44 years. Krope et al. (2013) found that most assaults were committed on Saturdays, Thursdays and Tuesdays. They also found that most perpetrators were 25 years old.

4.2 Comparative Analysis of Assaults on Police Officers in the First Nine Months of 2016

In 2016, the Police undertook a comparative analysis of criminal offences/assaults in 2016 and 2015 (Ministry of the Interior of the Republic of Slovenia, Police, 2016b) by comparing several factors that impact assaults on police officers. The comparative analysis was motivated by the greater number of brutal attacks on police officers and sought to ascertain the causes of the attacks. On this basis, it prepared measures that are important for reducing attacks on police officers. The comparative analysis comprises data and uses a similar methodology as used by Krope et al. (2013). Below are some of the key findings:

- in 2015 and 2016, officers were most frequently assaulted on roads (e.g. a road or car park), 39.6% in 2015, 34.8% in 2016; the second-most common location of assaults on officers is housing along with the immediate vicinity;
- most assaults on officers in both years happened at night; one-third between 20:00 and 24:00 (33.6% in 2015 and 31.3% in 2016); and assaults on officers most frequently occurred on weekends;
- in 2016, officers were most frequently assaulted while exercising their power to keep order and carry out detention (14.5% in both cases); in 2015, they were most frequently assaulted while issuing a payment order (13.75%);
- in 2016 and 2015, officers were most frequently assaulted while dealing with road traffic offences – 42.5% (33.3%), while maintaining peace and order – 30% (32.5%) and while handling criminal offences – 24.4% (30.8%);
- in 2016, officers were most frequently assaulted during interventions – 39.3% of cases, and in 2015 43.25% assaults happened to officers while on patrol;
- in 2016 and 2015, officers were most frequently assaulted while carrying out their usual duties. In 2016, the total share of these assaults was 53.8%, and in 2015 it was 56.9%. Assaults that happened during the course of normal duties were followed by assaults while performing sensitive procedures (35% in 2016 and 25% in 2015); officers were most rarely assaulted while conducting dangerous procedures (11.1% in 2016 and 18.1% in 2015);
- suspects in 2016 most frequently assaulted officers via other means of assault (37.2%), which was followed by using physical force – pushing, holding and strangulation (19.6%), blows with the hand (12.8%); in 2015, suspects most frequently used physical force as a means of attack – pushing, holding and strangulation (30.2%), then by other means of assault (29.7%) and blows with the hand (17%);
- in 2016, officers tried most frequently to protect themselves against assaults and manage suspects' resistance by using physical force, accounting for 28.3% (40.7%) of all coercive means applied; as a form of physical force, officers most frequently used an unarmed technique (23.3% in 2016 and 34.7% in 2015); the second-most frequently used means of coercion were cuffing and binding, i.e. 27.8% (23.7%), and coercive means were not used by officers during 27.8% (31.4%) of assaults on them. The 12.4% decline in the share of the use of physical force by officers when protecting themselves and managing the resistance of suspects and the respective 7.1% and 3.8% increases in the share of the use of gas sprays and use of batons could also be due to officers feeling threatened after some extremely dangerous assaults on them in the past because the concept of police training on this matter and practical self-defence procedures (PSDP) in cases when serious means of coercion are used did not change in 2016;

- compared to 2015, in 2016 the number of injured officers dropped by almost one-half (by 29 or 47.5%); in 2016, 30 officers (17.3% of assaulted police officers) were seriously injured in 115 criminal offences of assaults on police officers; one officer was severely physically injured, two were killed (one assault with a knife and one with another type of weapon) (1.2% of assaulted police officers); in 2015, six officers were physically injured in 149 criminal offences of assaults on police officers (25.5% of assaulted police officers); one officer was severely physically injured, and one was killed during an assault (using a vehicle). Such a significant drop in the number of injured officers, besides the fact that in 2016 compared to 2015 62 fewer officers were attacked, i.e. the 26.4% decline was most probably partly due to the fact that in 2016 officers performed approximately 70% fewer interventions in road traffic due to having been on strike, and this is the area where most assaults on officers occur (the latter is confirmed by the drop in the number of assaults on officers issuing payment orders – from 22 to 0;
- that approximately 10% of the assaulted officers in 2016 and 2015 were women; in 2016, 89.6% of assaults were against male and 10.4% against female officers; in 2015, the figures were 90.2% male and 9.8% female; the threat to female officers is approximately the same in both years since in 2016 the share of assaulted female officers grew by 0.6%, but the share of female officers also grew by 0.4%;
- in 2016, the majority of officers attacked were between 35 and 40 years old – 69 police officers or 39.9%; in 2015, the majority of officers attacked were between 30 and 35 years of age – 69 officers or 29.4%;
- in the considered period (2016 and 2015), most officers who were attacked had worked for the police for 5 to 10 years; officers with 10 to 15 or 15 to 20 years of active service were endangered to approximately the same degree; officers with 20 to 25 years of active duty and from 25 to 30 years of active duty were attacked less often; officers with active duty of 30 and more years were attacked very rarely (four times in 2016 and two times in 2015); the least frequent assaults happened on officers with less than 5 years of active service – three times in 2016, or never in 2015;
- in 2016, the officer ranks most frequently assaulted were: police constable (30.6%); in 2015: senior police officer (40.8%); officers of these ranks are by far at greatest risk among all officers since assaults on constables and senior officers comprise the large majority of all assaults on police officers – 60.1% in 2016 and 73.6% in 2015;
- in 2016 and 2015, most criminal offences/assaults involved assaults on a single officer, i.e. 62.6% (51.7% in 2015); the most frequent assaults on officers were committed under Article 299 of the Criminal Code; in 2016, the number of assaults compared with 2015 dropped to 1, 2 and 3 officers, the number of assaults on four or more officers remained the same – 4;
- by analysing the records of events involving the Operation and Communication Centre, it was found that 83 (105) events in 2016 involved assaults on officers, while 123 (133) officers were attacked; of whom in 9

(13) cases 1 officer was attacked, and it was established that the officer was on duty alone in 6 (4) cases, in 2 (1) cases on patrol; in other cases, the events involved neighbourhood police chiefs, detectives and officers on duty. In other instances, when only one officer was attacked or injured – 3 (9), offences involved threats against the officer – there was a suspicion of a criminal offence of obstructing an official act or of taking revenge against an official under Article 299 of the Criminal Code or an assault on an official performing security tasks under Article 300 of the Criminal Code. Two (3) threats were made directly – in 2016, no such offence was subject to criminal proceedings (only 1 in 2015); 2 (2) threats were made directly to officers during their free time; other threats were made indirectly when the suspect was in a police procedure – by phone (4 in 2015) and 1 (3) on online social networks.

Despite the drop in the number of offences of assaults on police officers, the rise in the number of most dangerous assaults on officers is concerning. Therefore, assaults on officers that ended in their deaths in 2015 and 2016 were analysed. In 2015, one such assault had a tragic outcome, and there were two in 2016. In all three events, the officers were on duty with another officer, but in only two cases did the assaulted officers face the perpetrator alone (Ministry of the Interior of the Republic of Slovenia, Police, 2016b).

In an assault using a vehicle in 2015 the perpetrator intentionally ambushed and collided with a police car used by officers for intervention purposes. It was later found that the perpetrator had made a false report of the violation of public order and peace with the intention of entrapping officers and assaulting them.

During an assault using a knife in 2016 the perpetrator used the knife to attack an officer who had approached the perpetrator to identify him; the other officer was moving the police car off the carriageway at the time.

In an assault with weapons in 2016, the attacker shot an officer who had coincidentally come to the scene of an assault where the perpetrator had already shot a doctor, while the other officer was located outside the area of the assault.

5 DISCUSSION

It was shown that the number of criminal offences of assaults on police officers, as presented in Figure 1, actually started to drop in 2014. The number of assaults in 2014 was the same as in 2008. Between 2008 and 2014, the numbers varied greatly. By examining the reports, we found several measures used by police management to reduce assaults, and that the number of assaults is now actually lower than in the mentioned years. The reason for these measures being taken were the serious consequences of assaults, especially for police officers, since deaths also occurred. The police management's finding in 2017 was that emphasis should be placed on the safe implementation of practical procedures for protection with short and long firearms while training instructors in practical self-defence procedures. It is also appropriate to focus on the procedures for purchasing protective shirts, vests and body cameras for recording police procedures. Another part of the solution is to use a newly legalised means of coercion, i.e. electroshock weapons.

While establishing or comparing findings from 2016/2017 reports with the research by Krope et al. (2013), there were differences with regard to the days of assaults and ages of attackers. Both comparisons spanned a 2-year period. Krope et al. (2013) considered the 2005/2006 period where it was found that most perpetrators are 25 years old. Police reports for 2017/2016 show that the perpetrators were aged 33 to 44 years. There is also a difference of 10 years in the age groups of attackers who were considered in the aforementioned age group, and the comparison considered age in a specific year. The age limit of attackers had risen compared to 10 or 11 years before.

The trend in criminal offences of assaults on officers has constantly declined in the past 11 years, with the exception of 2012 when there was an increase in the number of criminal offences when suspects attacked officers while policing the mass protests erupting across the Republic of Slovenia. Although the number of criminal offences of assaults on officers is falling, the rise in the number of the most dangerous forms of assaults on officers is a concern. Of five attacks that ended in an officer's death in the period since Slovenia's independence, four happened in a 2-year period – on 1 August 2014 (attack with firearms), one in 2015 (attack with a vehicle) and two in 2016 (attack with a knife and attack with firearms/gun).

We can see that between 2014 and 2016 a unique contradiction emerged, i.e. officers were actually in greater danger despite the statistical decline in the number of offences of assaults on them. Since Slovenia gained its independence, officers were most brutally attacked in the mentioned period, when four officers lost their lives during assaults. The methods of the assaults show the attackers did not choose the means for carrying out their assaults (use of firearms, knife, vehicle) and they attacked officers suddenly and unexpectedly. While attacking, the perpetrators showed extreme deviousness and thoughtfulness, as emphasised when an attacker made a false report about the serious violation of public order and a threat to people's safety so that he could ambush officers, watched them with binoculars and then deliberately attacked them using his vehicle. In this attack, the perpetrator murdered one officer and caused serious physical injuries to another.

This shows the statistical data on the number of criminal offences of assaults on officers are only an indicator of the trend of such offences in a certain period, and do not paint a comprehensive 'picture' of the actual threat to officers from assaults. Therefore, while monitoring the threat to police officers we should always analyse the forms and methods of assault on them, and plan appropriate activities and measures to improve the situation.

All of the recent activities conducted should be supplemented by continuing the following measures:

- practical self-defence training with the method of situation exercises should be intensified, whereby officers should practise scenarios prepared in advance, and also dangerous procedures which appear to be usual but where they are normally less careful and thus more vulnerable in the event of sudden and unexpected assaults on them;
- the Catalogue of Enforcement Proceedings Standards should be updated so as to rank relevant procedures among procedures with a higher risk rating (from normal to usual and from usual to dangerous procedures);

- additional equipment for protection, equipment for using force and other equipment should be added to help improve officers' safety during police procedures;
- shirts or vests with ballistic and anti-stabbing protection should be purchased for officers, especially for use in the performance of police tasks and police procedures where armed assaults on officers occur;
- after a test period of using cameras for video and audio recording of police procedures, such cameras should be permanently used by all police units on the local level and in some units on the regional (CPD PD, UPD PD) and national levels (CPD GPD, PSD GPD …); and
- following adoption of the Police Tasks and Powers Act (Zakon o nalogah in pooblastilih policije, 2013), systemic training should start immediately of police officers on the use of new police powers, the use of electroshock weapons and other equipment and means that may help improve the safety of officers during police procedures.

Some of the aforementioned activities and measures to improve officers' safety are already being used in practice – for instance, the intensification of practical self-defence training with situation training; the Catalogue of Enforcement Proceedings Standards has been updated, and some means of coercion will be supplemented (purchase of new gas sprays for all officers who directly exercise police powers); officers who exercise police powers have received shirts with soft ballistic protection and partial protection against cuts and stabs; other activities and measures are already in preparation. Some activities depend on the financial resources available. Officers will soon receive electroshock weapons to fill the gap between batons and firearms (seen from the aspect of the means of coercion officers carry on their belts) and to more effectively, safely and from a greater distance prevent assaults on themselves and others. Police officers will also receive body cameras for video and audio recording of police procedures, proven abroad to greatly impact the decline in the number of assaults on officers since many latent or prospective attackers cease an assault after receiving a warning from an officer that they are recording the procedure. The Ministry of the Interior and the Police have prepared tender documentation for the purchase of electroshock weapons and cameras for video and audio recording of police procedures, and the purchasing procedure will start in the near future.

In all cases, we must be aware that this technical equipment (means of coercion, protective gear) is only considered as passive protection. It ensures only limited protection for officers and, in certain circumstances (e.g. where an assault using firearms is directed exactly at the part that is ballistically protected etc.). Officers will be able to much better protect themselves with so-called active protection. This kind of protection comprises officers' comprehensive professional and proper conduct to reduce the risk of assault and, in the event of an assault, they enhance the chances of stopping it. This conduct comprises the maximum self-protective conduct of officers, consistent observation of police rules referring to active protection during police procedures, the implementation of police procedures falling within the so-called safety triangle, the protection of police procedures from cover, the protection of police procedures with firearms in permissible cases and so on.

These are only some of the activities and measures that can be used by the Police, but many activities and measures to improve officers' safety in the performance of police tasks cannot be affected by the Police. One of these is an appropriate punitive policy, a policy that would ensure general and special prevention of assaults on police officers.

REFERENCES

Bele, I. (2001). *Kazenski zakonik s komentarjem* [Criminal Code with commentary]. Ljubljana: Gospodarski vestnik.

Bristow, A. (1963). Police officer shooting – A tactical evaluation. *Journal of Criminal Law, Criminology and Police Science, 54*(1), 93–95.

Chapman, S. G. (1986). Reducing attacks on police. *The Police Journal: Theory, Practice and Principles, 59*(4), 300–320.

Deisinger, M. (2002*). Kazenski zakonik s komentarjem*. *Posebni del* [Criminal Code with commentary: Special part]. Ljubljana: GV Založba.

Dempsey, J., & Forst, L. (2005). *An introduction to policing*. Belmont: Wadsworth/Thomson Learning.

Gomboc, L. (1996). *Vzroki napadov na policiste* [Causes of assaults on police officers] (Diploma thesis). Ljubljana: Visoka policijsko-varnostna šola.

Ignjatović, D. (2006). Research on violent attacks on policeman in Serbia. In G. Meško, & B. Dobovšek (Eds.), *Policing in Central and Eastern Europe. Past, present and futures* (pp. 80–82). Ljubljana: Faculty of Criminal Justice and Security.

Kazenski zakonik RS (KZ) [Criminal Code]. (1994). *Uradni list RS*, (63/94).

Kazenski zakonik (KZ-UPB1) [Criminal Code]. (2004). *Uradni list RS*, (95/04).

Kazenski zakonik (KZ-1) [Criminal Code]. (2008). *Uradni list RS*, (55/08).

Krope, S. (1998). Standardizacija in tipizacija policijskih postopkov kot dejavnik kakovosti policijskih storitev [Standardization and typification of police procedures as a factor in the quality of police services]. *Organizacija*, *31*(5), 280–287,

Krope, S., & Ilić, V. (2017). Uporaba prisilnih sredstev v slovenski policiji za obdobje 2008–2016 [The use of coercive means in the Slovenian police for the period 2008–2016]. *Varstvoslovje*, *19*(3), 293–312.

Krope, S., & Lobnikar, B. (2015). Assaults on police officers in Slovenia – the profile of perpetrators and assaulted police officers. *Revija za kriminalistiko in kriminologijo*, *66*(4), 300–306.

Krope, S., Lobnikar, B., & Pagon, M. (2013). Elaborating an organizational model for managing criminal acts of assault on police officers. In Z. Balantič et al. (Eds.), *Pametna organizacija: Talenti, vitka organiziranost, internet stvari: Zbornik 32. mednarodne konference o razvoju organizacijskih znanosti* (pp. 480–491). Kranj: Moderna organizacija.

Lester, D. (1985). The murder of police officers in American cities. *Psychological Reports*, *57*(2), 101−113.

Ministry of the Interior of the Republic of Slovenia, Police. (2008). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2007* [Report on the use of coercive means and assaults on police officers in 2007]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2009). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2008* [Report on the use of coercive means and assaults on police officers in 2008]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2010). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2009* [Report on the use of coercive means and assaults on police officers in 2009]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2011). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2010* [Report on the use of coercive means and assaults on police officers in 2010]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2012). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2011* [Report on the use of coercive means and assaults on police officers in 2011]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2013). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2012* [Report on the use of coercive means and assaults on police officers in 2012]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2014). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2013* [Report on the use of coercive means and assaults on police officers in 2013]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2015). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2014* [Report on the use of coercive means and assaults on police officers in 2014]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2016a). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2015* [Report on the use of coercive means and assaults on police officers in 2015]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2016b). *Primerjalna analiza napadov na policiste v prvih 9 mesecih 2016* [Comparative analysis of assaults on police officers in the first 9 months of 2016]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2017). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2016* [Report on the use of coercive means and assaults on police officers in 2016]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Ministry of the Interior of the Republic of Slovenia, Police. (2018). *Poročilo o uporabi prisilnih sredstev in napadih na policiste v letu 2017* [Report on the use of coercive means and assaults on police officers in 2017]. Ljubljana: Ministry of the Interior of the Republic of Slovenia, Police.

Mravlja, M., & Krope, S. (2007). Poškodbe policistov z vidika napadov na policiste v letih 2004 in 2005 [Police officers' injuries in terms of assaults on police officers in 2004 and 2005]. In B. Lobnikar (Ed.), *Dnevi varstvoslovja.* Maribor: Fakulteta za varnostne vede.

Novak, G. (1996). *Obrambne tehnike v policijski praksi* [Defense techniques in police practice] (Diploma thesis). Ljubljana: Visoka policijsko-varnostna šola.

Pinizzotto, A. J., Davis, E., & Miller, C. (2000). Officer s perceptual schoorthand: What messages are offenders sending to law enforcement officers? *FBI Law Enforcement Bulletin, 69*(7), 1–6.

Terrill, W., Leinfeld, F. H., & Kwak, D. (2008). Examining police use of force: A smaller agency perspective. *Policing: An International Journal of Police Strategies & Management, 31*(1), 57–76.

Vidmar, J. (1993). *Vrste in oblike napadov na policiste kot indikator pri programiranju samoobrambe* [Types and forms of assaults on police officers as an indicator in self-defense programming] (Diploma thesis). Ljubljana: Višja šola za notranje zadeve.

Zakon o kazenskem postopku (ZKP) [Criminal Procedure Act]. (2012). *Uradni list RS* (32/12).

Zakon o nalogah in pooblastilih policije (ZNPPol) [Police Tasks and Powers Act]. (2013, 2015, 2017). Ljubljana. *Uradni list RS,* (15/13, 23/15, 10/17).

Zakon o prekrških (ZP-1) [Minor Offences Act]. (2011, 2013, 2016). *Uradni list RS*, (29/11, 21/13, 111/13, 32/16).

Zakon o prekrških zoper javni red in mir [Act on Criminal Offences against Public Order and Peace]. (1974). *Uradni list RS* (16/74).

Zakon o varstvu javnega reda in miru (ZJRM-1) [Protection of Public Order Act]. (2006). *Uradni list RS*, (70/06).

Žaberl, M. (2001). *Policijska pooblastila* [Police powers]. Ljubljana: Visoka policijsko-varnostna šola.

About the Authors:

Srečko Felix Krope, PhD, senior lecturer at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: srecko.krope2@fvv.uni-mb.si

Vlado Ilić, senior independent police inspector at the General Police Directorate of the Police, Slovenia. E-mail: vlado.ilic@policija.si