UDC: 316.624:004.738.5
DOI:10.5937/PDSC26034L

Miloš Lakićević, PhD, Assistant Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad
email: milos.lakicevic@pravni-fakultet.info
ORCID ID: https://orcid.org/0000-0002-0172-1171

Anita Ilić Antanasijević, PhD, Assistant Professor
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad
Professor, College of Applied Studies for Criminology and Security,
Niš, Serbia
email: anita.ilicantanasijevic.kib@gmail.com
ORCID ID: https://orcid.org/0000-0001-9092-9347

RISKS OF INDIVIDUAL SECURITY IN INTERNET INTERACTION

Abstract: Under modern conditions of globalization, the Internet has become an extremely popular information and communication tool with billions of users. Although it brings numerous benefits to contemporary man, it is also frequently abused by malicious actors. Users often present themselves on *online* social networks by posting large amounts of personal information, sharing it not only with friends but also with uninvited users. They tend to overlook that the network of computer communications is ideal for malicious users: the Internet's decentralized nature means it cannot be fully controlled or effectively monitored. This paper demonstrates how the leakage of personal data through social networks and the careless use of Internet services can compromise both privacy and individual security.

Keywords: *interaction, Internet, social networks, security, individual security.*

INTRODUCTION

The rapid evolution of information and communication technologies (ICT) has enabled a vast number of individuals worldwide to proactively exchange messages, data, ideas, and information. Today, the Internet is so deeply integrated into daily life that the prevailing sentiment is: "If you are not online, you do not exist." However, despite the undeniable advantages of these technologies, users often overlook the inherent security risks that threaten their privacy and security in many different ways. Even though social network users have the autonomy to decide what to post, they frequently fail to assess whether their posts are beneficial or detrimental to their personal security. A critical oversight is the lack of awareness that online content is often permanently archived. Given that the Internet-based exchange transcends geographical boundaries and makes information accessible to an unlimited audience, including malicious actors, users could be exposed to unforeseen threats that compromise their privacy and individual security.

Basic Facts About the Internet

The term *Internet* (derived from the Latin *inter*, meaning "between," and the English *net*) refers to the interaction between multiple computers, with the human-computer interface at its core. The characteristic of the Internet is that it has no single owner; instead, individuals, institutions, and states are owners (users) of the interconnected computers and online communication channels. This implies that users independently choose their connection methods, the types of information they access, and the extent of personal data they disclose to other users. Consequently, the Internet has evolved into a new mass medium, enabling individuals to both consume information and broadcast it. Every participant whose computer is connected to the network is a potential user of all circulating information, while simultaneously acting as both a transmitter and a recipient (Milašinović & Jevtović, 2013, p. 131).

The concept of social networks is defined by *nodes* and *links* (Milašinović & Jevtović, 2013, p. 135). A *node* represents an individual participant or member, while a *link* denotes the relationship or interaction between two or more participants. Social networks empower individuals to create personal profiles within bounded systems and establish contact with other users. As the social network's access criteria are low (due to its inherently open architecture, any individual or legal entity that "adheres" to

basic standards of conduct and communication security can have an account[1]), it is a type of (Internet-based) medium that facilitates communication and interaction that traditional media, such as television, cannot provide.

Fundamental Concepts of Individual Security

A social being is inherently characterized by the desire for a peaceful, organized, and secure life within a community with other people, governed by the mutual respect of rights. The establishment of the state created the conditions for achieving comprehensive security for all citizens. In essence, the individual delegates a portion of their self-protection to the state as the supreme authority. Consequently, personal safety becomes largely dependent on the security-related efficiency of others. Still, individual security remains paramount. As a member of society, the individual holds the status of a referent subject of security within their home state, and the status of an object of security, reflecting the process in which they are protected by other entities.

These facts, on the one hand, indicate the necessity of determining the meaning of the concept of *security*, which is primarily related to the individual and human society, their vital values, and the achievement of safety, and on the other hand, the necessity of defining individual security. The term security (*bezbednost*) in the Serbian language[2] is primarily used to assess the state of a subject characterized by the absence of danger. An analytical review of the definitions of security given by some authors[3] indicates that security is among the most fundamental human needs, and its pursuit is a primary motive for human engagement. Within this framework, three key elements of security are identified: the *Object of Security* (the core values or systems being protected), the *Subject of Security* (the individual,

[1] The founder of the social network Facebook, Harvard student Mark Zuckerberg, launched in 2004 a website intended solely for communication among students at his university. Subsequently, other colleges, high schools, and some multinational companies joined the network, making the website the most visited global social network. In October 2007, Facebook had 50 million users, and by 2009, it reached around 300 million users.

[2] To be secure is defined in Serbian as being free of troubles, misfortunes, and worries of various kinds, or accidents, suffering, and various evils. Security, then, is primarily a designation for someone's or something's state characterized by the absence of troubles, worries, accidents, suffering, and other evils, that is, the absence of threats to survival and other values (Ilić, 2011, p. 91, trans. by author).

[3] For more details, see: Bajagić, 2007, pp. 8–22; Mijalković, 2011, pp. 23–49; Mijalkovski, 2009, pp. 17–24.

… or state) providing protection to the Object of Security from the *Subject of Danger* (individual, group) and the *Source of Threat* (natural forces). In a relational sense, the concept of security can be decoded by answering three fundamental questions: What is being protected? Who is providing the protection? And from what or whom is the object being secured?[4]

Answering these questions requires the planned and organized engagement of *Subjects of Security* to optimally protect their values from both current and potential threats. Achieving this goal involves a series of proactive measures designed to establish a secure *state* of one's own values, characterized by the absence of threats, the effective elimination of threats, and the absence of fear of attack. In this context, *security represents the optimal, non-threatening state of the Object of Security, which is established, maintained, and continuously improved by the Subject of Security*. Since absolute security is an impossibility, we must speak in terms of the relative security of the Object of Security. Its optimality depends primarily on the ability of the Subject of Security to provide timely recognition and effective mitigation of threatening activities.

Given the aforementioned definition of the term security and the fact that an individual, as a member of society and the state, simultaneously holds the status of both a referent object and a subject of security, we can define *individual security* as a state within society and the state in which individuals freely exercise and protect their rights and freedoms.[5] Furthermore, *individual security is the optimal protection of a person's physical, spiritual, and material status from real or potential, direct or indirect threats, regardless of their origin or manifestation*.

This definition reflects both the objective and subjective dimensions of individual security within the "individual–society–state–international community" interaction.[6] *Objective security* refers to a state of optimal

[4] Bjorn Møller believes that defining the concept of security requires answering the following: whose security? security of what? security from whom? security from what? security provided by whom? and security by what means? (Møller, 2006, pp. 61–62).

[5] The 1994 UNDP Human Development Report identifies seven components of human security with the individual as the referent object of security: economic security, food security, health security, environmental security, personal security, community security, and political security (UNDP, 1994, pp. 25–33).

[6] Interaction, as a feedback loop in human communication, signifies that the openness of the channel through which a message is transmitted is maintained; this enables a mutual exchange between the communicator and the recipient. It is a mutual or reciprocal influence between two or more systems; social interaction is the relationship between individuals and groups in the process of mutual exchange of messages, ideas, feelings, etc. (Leksikon novinarstva, 1979, p. 95).

protection of an individual's physical, spiritual, and material integrity from threatening activities by other individuals, groups, the state, or the international community. *Subjective security* reflects the individual's internal certainty that their rights and freedoms are secure, characterized by the absence of the fear of attack. In this sense, an individual can be *safe, insufficiently safe*, or *unsafe*. A person is truly safe only when both objective and subjective security are optimal. If objective protection exists but the individual remains in fear of an attack on their values, they are insufficiently safe (subjectively vulnerable despite objective safety). Conversely, an individual is unsafe when they are systematically or continually exposed to threats and are aware of the unattainability of their removal.

The considered facts on individual security primarily relate to threats posed by other entities. The focus is traditionally on the "individual–state" interaction, where the individual's active engagement is crucial, as their rights and freedoms are inherently limited by those of others. The state is responsible for creating conditions for individuals to enjoy the rights and freedoms—to be safe. However, to achieve comprehensive individual security, *the self-threatening aspect* must be addressed. This involves an individual's capacity to assess whether their own careless, reckless, or intentional actions contribute to the compromise of their privacy and security and to the detriment of others. Current findings suggest that the *Internet* has emerged as one of the most significant platforms for the self-endangerment of personal privacy and individual security.

Expansion of Internet Usage and Service Diversity

The inherent advantages of the Internet (cost-effectiveness, decentralized structure, and relative anonymity) have fueled its massive global expansion. In this regard, statistical data reports that the number of Internet users rose from 1.9 billion in 2010 (2.1 billion in 2011, 2.3 billion in 2012, 2.6 billion in 2013) to 2.8 billion in 2014, reaching approximately six billion by 2021.

These figures underscore our existence within a modern *information society*,[7] where *information* serves as the primary driver, and sophisticated technical means enable its instantaneous distribution and processing. In this environment, interaction of people with ICT has become an essential

[7] The working instruments of the information society are computers and telecommunications equipment, while the Internet and mass media are their means of transport. Given the significance of computer networks, the term "network society" is often used in literature (Mimica & Bogdanović, 2007, p. 74).

component of life and social organization, characterized by a global exchange of data accessible from almost any location. What distinguishes social networks is their accessibility: basic computer literacy is sufficient for users to create a visible personal presentation and connect with individuals worldwide—connections that would otherwise be impossible. This explains why social and mobile media platforms have become the dominant technologies in the lives of young people. These platforms allow them to share worldviews with close friends and acquaintances, while simultaneously exposing them to strangers and potentially destructive content. This digital immersion often erodes the caution necessary for safe Internet usage, leading to a variety of risks.

Security Risks within the Interaction of Internet Needs and Services

The volume of data circulating within the information society is unprecedented. Access to information has been simplified and expanded, while the capacity to record, store, and process data is now vast. Similarly, opportunities for electronic communication and interaction are virtually limitless, as are the options to trace anyone: every electronic interaction leaves a persistent digital footprint of the user. In this environment, *individuals* possess the freedom to post an unlimited amount of information about themselves and others. Often, they are unaware that *content shared online can never be truly deleted; the unbounded Internet ensures that once data is posted, it can be archived and potentially misused by third parties at any time.* Furthermore, the modern individual is subjected to constant information overload, which can impair their ability to perceive reality analytically and critically. Consequently, despite national legal frameworks that regulate the right to information, data confidentiality, and personal data protection, Internet users remain exposed to significant risks. Primary among these are threats to *privacy* and *security*. While the goal of privacy is to restrict information access to authorized persons or processes, the *inherent nature of the Internet allows for the collection of sensitive data without the subject's knowledge or consent*.

Although posting information on a website may seem harmless, the absence of an adequate protection system against the exploitation of information resources and personal and business data means that a "mosaic" of an individual's or organization's profile can be reconstructed and exploited. This danger requires Internet users to develop the capacity for risk mitigation, achieving a balance between data disclosure and the protection of their own privacy and security.

Establishing proper dimensions of this relationship requires the understanding that *individual security fundamentally means freedom from danger (risks and threats)*. There is no true freedom in a state of insecurity and lack of security, just as security lacks quality without freedom; both are elementary needs of every individual, guaranteed by national legal orders and international conventions. In this context, state authority occupies a dual position: it must protect the freedoms of its citizens, including protection from its own potential overreach, while simultaneously maintaining its internal functional capacity. To achieve this, the state's preventive and repressive engagements rely heavily on *information* collection, which inherently limits certain rights and freedoms. These restrictions are prescribed by law, and any abuse of such power is subject to sanction. The individual's position in this information process can be summarized as follows: the individual's interest is to know as much as possible about what the government knows regarding public affairs, other citizens, and themselves personally. On the other hand, the government's interest is to protect information it possesses that, if disclosed, would harm the public interest. The privacy interest for the individual is to ensure that the government and other entities remain uninformed about their private life. Moreover, the public/state interest is to know everything about the individual that is justified to know.

However, the individual's position in the context of the Internet is fundamentally different. On the web, individuals often voluntarily surrender personal data and use information at their own peril, frequently ignoring the Internet's inherent absence of responsibility for individual safety. Certainly, *risk* is inherent in most human activities. Recognizing a risk entails considering the common denominator of the definition of risk, which is defined primarily by uncertainty and loss.[8] *Uncertainty* exists when the outcome of an event cannot be predicted with precision. For a situation to be characterized as "risky," it must have at least two possible outcomes, one of which is undesirable—*a loss*. This may manifest as the depletion of an existing asset or a gain that falls short of its potential. Therefore, the essential feature of risk is the possibility of suffering damage.

To fully grasp the risks inherent in the individual–Internet interaction, one must acknowledge the state's inherent limitations in safeguarding the

[8] The concept of risk can be defined as: a) the possibility of loss, b) uncertainty, or c) the possibility of any outcome that is unexpected (Encarta Reference Library, 2005, p. 65); The term risk implies: danger, exposure to danger, or a business venture or stake involving the danger of failure (Vujaklija, 1970, p. 346).

privacy (and security) of its citizens from online abuses. Namely, the state regulates its own collection and use of personal data or ensures individual security through national legislation.

However, it should be emphasized that *these legal frameworks are often insufficient to protect individuals from individual-Internet interaction.* Namely, this protection depends primarily on the individual's IT literacy, analytical skills, and security culture, regardless of whether they are actively promoting themselves on social networks or merely utilizing its services. In this regard, research indicates that these competencies are often lacking, even among adults who frequently share or use personal data online. This results in diverse risks to privacy and security, with the most severe consequences often observed among minors and children. Consequently, the contemporary maxim "whoever is not online does not exist" must be reinforced with a vital caution: "whoever is not sufficiently careful on the Internet jeopardizes their personal safety."

An individual's decision to engage with the Internet presents both a *challenge* and a ***general risk*** to their personal security. The ease of access to any social network often masks the gravity of this choice.[9] Users must remain cognizant that upon joining a platform, the personal information they disclose, as well as data regarding their real-world social circles, effectively becomes the property of the network. In doing so, the user essentially surrenders their privacy, granting the platform a degree of claim over their digital identity and worldview. Furthermore, users expose themselves to the risk of being targeted by malicious actors who may exploit this information for harassment or blackmail. It is also critical to note that while every *online* social network maintains privacy policies,[10] these platforms reserve the right to modify these rules at their discretion. The findings point to the multidimensional nature of the *general risk regarding the individual-Internet interaction*.

Inadequate protection of Internet users' data from unauthorized persons represents an important dimension of the risk involving the individual-internet interaction. A prime example of this ***risk*** is a media-published fact that the personal data of 533 million Facebook users, representing one-fifth

[9] When opening an account, the user must provide their first and last name, date of birth, gender, and email address. Other features (such as location, school, photo, online friends, and activities) are not mandatory.

[10] Facebook's privacy policy contains about 3,752 words and ends with a note that it can be changed at any moment (http://www.FB.com/policy.php, accessed September 20, 2009). However, the question arises) as to how many members have actually read that document, and how many regularly read and familiarize themselves with the changes.

of the platform's total profiles, was exposed on a hacker forum on April 3, 2021, as reported by *Business Insider*. A breakdown of user profiles by country was also published, showing that data were exposed for 162,898 users from the Republic of Serbia, with the largest number (32 million) being from the USA. Because this data was made publicly available for free on the hacker forum, it created a tangible danger of misuse, ranging from unsolicited SMS messages and harassment to extortion and targeted threats. Namely, cybercriminals must invest great effort to obtain this type of data, which can help them launch attacks. However, after such availability in one location, the effort is reduced to just a few clicks. In this regard, Alon Gal, Chief Technology Officer of the Israeli firm *Hudson Rock,* warned that this data had been circulating among cybercriminals for some time.

In October 2021, Frances Haugen, a former Facebook employee, testified before the U.S. Congress, alleging that the company consistently sacrificed user safety for profit. Her testimony was particularly critical of Instagram, stating that the platform failed to take adequate measures to improve user safety, prioritizing astronomical financial gains over the well-being of its users, especially teenagers. Haugen argued that the company has been disingenuous in its fight against hate speech and misinformation, noting that artificial intelligence systems detect only a fraction (10 to 20 percent) of offensive content. This failure allows minors to be exposed to advertisements for drug paraphernalia. She concluded that while the average online experience may be positive, approximately 20 percent of users face "terrible or dangerous experiences."

Digital privacy is protected by national legislation and international conventions from intrusions, sabotage, receiving unsolicited messages, piracy, theft, and espionage. Despite this, scams, fraud, manipulation, identity theft, data destruction, spying, and similar online activities represent a *pronounced risk* to the security of internet users. Cyberattacks can be launched from anywhere in the world, are not immediately noticeable, and their consequences often manifest over long periods, making the attribution of perpetrators, methods, and tools extremely difficult. The actors behind these threats include hackers, insiders, terrorists, corporate spies, and intelligence services. However, practical experience suggests that *the most prevalent threat* to the average individual is posed by cybercriminals. The profile of a *cybercriminal* often reflects an intelligent, unscrupulous, pervasive, technically savvy, and often vengeful individual who is difficult to stop because their obsession and the capacity to easily search through cyberspace give them a sense of power and elusiveness—viewing the computer as the "center of their life." They use various tools to harm the

victim or to gain financial benefit. The "419" or Nigerian Scam[11] is very widespread and quite effective. Another particularly predatory method of money extortion is when the attacker secretly installs malicious software (malware) on the victim's computer to block access to their data and prevent them from using it. The victim is then presented with a ransom demand, typically required in Bitcoin cryptocurrency, to regain access to their files.

Risks of Interaction: Children, Minors, and the Internet

The modern education system introduces children to computers and the Internet as early as the first grade. However, research indicates that children and minors are becoming increasingly preoccupied with the digital world.[12] Their limited capacity to recognize online dangers is often compounded by a lack of necessary parental oversight over their "roaming" through cyberspace. Under these conditions, various forms of self-harm and threats to safety can emerge, ranging from developing internet addiction and cognitive decline to suicide.

The traditional list of *chemical addictions*, such as tobacco, alcohol, narcotics, and gambling, that are dangerous to general and mental health, has been expanded by *behavioral (non-substance) addictions*. These involve excessive hours spent on gaming, social media consumption, and smartphone usage. Findings show that many children spend up to seven hours a day online, primarily via smartphones (www.kurir.rs, Sep 28, 2020). This level of immersion suggests that the youngest populations are living in a "virtual reality," often losing their sense of time and neglecting real-world obligations. The consequences of constant screen exposure are both immediate and long-term. Primarily, a child's physical development is hindered by insufficient physical activity. The core *risk* lies in the development of a dependency—the minors are not capable of understanding that spending hours socializing with friends via social networks and

[11] A cyber attacker sends emails explaining that a money transfer is forthcoming but that there is a problem: a deposit must be paid in advance. If a naive user pays the first installment (for example, $5,000), they are then told that something has become complicated and a subsequent payment is requested, ranging from $10,000 to $50,000. One must pay in order to later receive millions, which never actually arrive. By the time the fraud (theft) is discovered, it is too late; the money has been taken, the account is closed, and all traces are lost.

[12] The results of the international 2018/19 macro-study "EU Kids Online" show that 86 percent of children and youth in Serbia aged 9 to 17 use the internet for an average of three hours a day, while the time spent online doubles during the weekend.

browsing their content cannot replace direct socialization and physical engagement in real space and time.

The essence of a second, more insidious *risk* in the interaction between minors and the Internet is that excessive reliance on digital tools indirectly slows the development of the brain, memory, and other cognitive functions. While the Internet and various IT tools can enable users to obtain and process information and ideas more rapidly, they can also foster a form of cognitive offloading that weakens the brain's ability to utilize and develop its natural associative powers. In fact, there is a danger that a dependency on the Internet manifests (latently) as a gradual atrophy of certain natural mental faculties.[13] The lack of parental oversight, allowing children's unrestricted all-day access to the web, has contributed to a broader decline in academic and professional expertise in the Republic of Serbia. A significant factor in this trend is the total fascination of both youth and parents with social networks and applications (Prvulović, 2021, p. 13). This process is characterized by an "abbreviated" preparation for reading and learning assignments using ready-made solutions or parental assistance, or even unnatural contact with so-called experts—influencers and YouTubers—who captivate young audiences. All of this almost completely neglects standard methods of learning and acquiring knowledge, and leads to projecting life on an unrealistic basis. An even more subtle and far-reaching consequence is that the minor remains permanently dependent on internet search functions, rather than using their own internal capacity for free thought and creative association.

Relevant findings indicate that while today's children and minors possess advanced technical knowledge regarding the functioning of digital technologies, they frequently lack the necessary precautionary skills and methods of self-protection. This knowledge gap makes them increasingly susceptible to *risks* that can trigger aggressive behavior or lead to self-destructive decision-making. There are two prevalent forms of *online aggressive behavior* among youth. The first involves the creation of private groups or profiles on social networks specifically designed to ridicule, belittle, and brutally harass a targeted child/minor. These digital attacks often spill over into physical, real-life confrontations. The second form of

[13] For example, with GPS technology, our ability to memorize and navigate urban spaces (while driving, using maps, etc.) is drastically reduced; with Google, Wikipedia, and similar information sources and search engines, our natural inclination toward research and searching for information is diminished at its inception, while our curiosity is dulled (Lopandić, 2021, p. 12, trans. by author).

teenage aggression that has become almost commonplace is the recording of physical altercations via mobile phones, which are subsequently uploaded to platforms like TikTok or Facebook.

The most devastating impact of certain social media platforms on children and minors is observed in cases of individual suicides. Following the tragic death of a 10-year-old girl in Palermo, Italy,[14] media have published a list of some of dangerous and potentially lethal "challenges" including, but not limited to the *Choking Game* (a child wraps a belt around their neck and tightens it until they lose consciousness, often with fatal outcome), *ingestion of liquid detergent pods, dousing oneself in flammable liquids and self-immolating* to test heat endurance, leading to severe third-degree burns, and *teeth grinding* (filing down teeth to resemble "shark teeth," which causes permanent dental damage, according to dentists). According to data from the U.S. Centers for Disease Control and Prevention, within just over a year of these challenges circulating on TikTok, 82 children worldwide have lost their lives.[15]

CONCLUSION

Based on the preceding analysis, it is evident that today, the self-endangerment of individual security through the careless use of the internet represents one of its important dimensions. Namely, information and communication technologies allow individuals to satisfy a vast array of needs. However, they simultaneously pose a persistent risk to individual security, even in cases where their IT literacy and security culture are

[14] Following the death of the girl, the Italian police held a 48-year-old woman from Syracuse, Sicily, for questioning regarding alleged incitement to suicide by posting videos on TikTok. She had published a video of a man and a woman wrapping adhesive tape around their mouths and noses as part of a challenge. The detained woman had 730,000 followers and was considered an influential TikToker for initiating 20 dangerous challenges, including inhaling cream through the nose, closing eyes with pliers, and breaking an arm with a cooking pot.

[15] In January 2021, in Rakovica, Belgrade, a nine-year-old boy, D.S., was found hanged in his. It was suspected that he died while participating in a "choking game" challenge on TikTok. In late September 2021, the Serbian public was alarmed by videos of children and teenagers from the Stepa Stepanović neighborhood in Belgrade sitting and lying on pedestrian crossings, as well as videos of students in Novi Sad smashing school desks and toilets. It turned out that both cases involved a TikTok "challenge". Media outlets reported that on October 3, 2021, an eleven-year-old student from Stara Pazova jumped from a fourth-floor window at a local elementary school. Reportedly, this was a student who nearly lost his life due to a TikTok challenge.

adequate, and a threat to the security of individuals who use the internet carelessly. This refers to numerous possible threats that often come from virtual space and, in various ways, directly or indirectly, violate human privacy, dignity, and security in real life. The individual's voluntary decision to engage with Internet services often occurs in a space where the influence of society and the state on the content of their communication (self-presentation and use of information) is minimal or excluded. The gravity of a security breach is only realized after the consequences have manifested. It is particularly concerning that interactions between children/minors and the Internet often yield similarly distressing outcomes, despite the assumption of parental supervision, which should make risks negligible. Given that human-computer interaction will only become more integrated and dynamic in the near future, thereby increasing the number and types of risks, it is imperative to constantly evolve the security and self-protection culture of the individual. We must ensure that every Internet user acquires the necessary competencies to prevent the risks inherent in our digital existence.

REFERENCES

1. Bajagić, M. (2007). Osnovi bezbednosti [Fundamentals of Security], Kriminalističko-policijska akademija, Beograd.
2. Džigurski, O. (2002). Informatika [Information Technology], Univerzitet u Beogradu - Fakultet civilne odbrane.
3. Encarta Reference Library (2005). Microsoft DVD.
4. Griffiths, T. R. (2002). The History of Internet, Leiden University, Leiden. http://www.let.Leidenuniv.nl/history/ivh/chap2.html.
5. Ilić, P. (2011). Semantičko-leksikografski aspekti pojma bezbednosti [Semantic-Lexicographic Aspects of the Concept of Security], Vojno delo, Jesen 2011, pp. 85-99.
6. Leksikon novinarstva [Lexicon of Journalism] (1979). IŠKRO, Savremena administracija, Beograd.
7. Lopandić, D. (2021). Da li Gugl zaglupljuje [Does Google Make Us Stupid] (pogledi), Politika, Beograd, 8.3.2021.
8. Meler, B. (2006). Nacionalna, socijetalna i ljudska bezbednost [National, Societal and Human Security], Ljudska bezbednost [Human Security] (zbornik tekstova), Fond za otvoreno društvo, Beograd, pp. 55-90.
9. Mijalković, S. (2011). Nacionalna bezbednost [National Security], Kriminalističko-policijska akademija, Beograd.

10. Mijalkovski, M. (2009). Obaveštajne i bezbednosne službe [Intelligence and Security Services], Univerzitet u Beogradu - Fakultet bezbednosti, Beograd.
11. Milašinović, S. & Jevtović, Z. (2013). Metodologija istraživanja konflikata i krizno komuniciranje u savremenom društvu [Methodology of Conflict Research and Crisis Communication in Contemporary Society], Kriminalističko-policijska akademija, Beograd.
12. Miletić, M. & Miletić, N. (2012). Komunikološki leksikon [Dictionary of Communication Studies], Megatrend, Beograd.
13. Mimica, A. & Bogdanović, M. (2007). Sociološki rečnik [Dictionary of Sociology], Zavod za udžbenike, Beograd.
14. Prvulović, V. (2021). Zaustaviti opadanje stručnosti u Srbiji [Stopping the Decline of Professional Expertise in Serbia], (pogledi), Politika, Beograd, 24.11.2021.
15. Putnik, N. (2009). Sajber prostor i bezbednosni izazovi [Cyberspace and Security Challenges], Univerzitet u Beogradu - Fakultet bezbednosti, Beograd.
16. United Nations Development Program (UNDP), Human Development Report, Oxford University Press, New York, 1994.
17. Vujaklija, M. (1970). Leksikon stranih reči i izraza [Dictionary of Foreign Words and Expressions], Prosveta, Beograd.
18. Zakon o informacionoj bezbednosti [Law on Information Security], Službeni glasnik Republike Srbije, broj 6/2016.
19. Zakon o zaštiti podataka o ličnosti [Law on the Protection of Personal Data], Službeni glasnik Republike Srbije, broj 97/2008, 104/2009, 68/2012.