

Saša Kuzmanović⁵⁹

Professional association of security sector, Belgrade/Serbia

CYBERSECURITY AND DATA PROTECTION IN SOCIETY 5.0

DOI: 10.5937/PIM26208K

Abstract:

Cybersecurity and data protection represent one of the key challenges of modern digital society due to the increasing dependence on information and communication technologies. This paper analyzes the fundamental principles of cybersecurity, the most common forms of cyber threats, and data protection mechanisms, with particular emphasis on technical, organizational, and legal aspects. Special attention is given to the protection of personal data, the role of users in maintaining security, and the importance of regulations in this area. The paper also examines contemporary challenges and future trends, including the application of new technologies in information protection. It concludes that effective cybersecurity requires an integrated approach that combines technology, legislation, and user education.

Keywords: Cybersecurity, data protection, information security, cyber threats, privacy, digital society, regulations

Introduction

In the modern digital age, information represents one of the most valuable resources [1]. With the increasing use of the internet, mobile devices, and digital platforms, the need to protect data and secure information systems is also growing [2]. Cybersecurity has become a key element in the functioning of modern society, as it encompasses measures, technologies, and processes aimed at protecting computer systems, networks, and data from unauthorized access, misuse, and attacks [3].

In this context, the concept of Society 5.0 emerges as a new societal paradigm that integrates cyberspace and physical space through advanced technologies such as artificial intelligence, the Internet of Things, and big data analytics. Society 5.0 aims to create a human-centered, highly intelligent society in which digital technologies are used to solve complex social challenges and improve quality of life. However, this deep integration of digital and physical systems also significantly expands the attack surface and increases dependence on interconnected infrastructures.

Within the Society 5.0 framework, cybersecurity challenges become more complex and multidimensional. The convergence of critical infrastructures (such as healthcare, energy, transportation, and smart cities) with digital

⁵⁹ sasa.kuzmanovic112@gmail.com, ORCID: 0009-0007-6059-3847

networks increases the potential impact of cyberattacks. In addition, the massive collection and processing of personal and sensitive data raises serious concerns regarding privacy protection, data ownership, and ethical use of information. Another significant challenge is the vulnerability of IoT devices, which often have limited built-in security features but play a central role in interconnected systems.

The aim of this paper is to analyze the importance of cybersecurity, the main types of threats, data protection mechanisms, as well as the challenges society faces in this field [4], with a particular focus on the implications of the Society 5.0 paradigm for future security strategies.

1. The Concept and Importance of Cybersecurity

Cybersecurity represents a set of activities, measures, technologies, policies, and procedures designed to protect computer systems, networks, data, and digital infrastructure from unauthorized access, misuse, damage, or destruction, as well as legal aspects of information protection [5].

Three fundamental principles, known as the CIA triad, form the foundation of cybersecurity [6]:

- **Confidentiality** – preventing unauthorized access to data
- **Integrity** – maintaining accuracy and completeness of data
- **Availability** – ensuring access to data for authorized users

The importance of cybersecurity in modern society lies in its critical role due to the growing dependence of society on digital technologies [1], [3].

2. Cyber Threats and Attacks

Cyber threats and attacks are activities aimed at compromising the security of information systems, networks, and data, with the goal of theft, destruction, manipulation, or unauthorized access [2], [7]. They can originate from hackers, criminal groups, insiders (employees), state actors, and others. In practice, there are several types of cyber attacks:

1. Malware – short for *malicious software*, represents any program designed to damage, exploit, or gain unauthorized access to a computer system and its data [3], [7]. It is dangerous because it is often invisible, can remain undetected for a long time, continuously evolves, becomes

more complex, and can lead to significant financial losses. Malware most commonly installs itself silently on a device, runs in the background, and performs malicious activities without the user's knowledge. It can be introduced through infected files, emails and links, internet downloads, and USB devices.

There are several types of malware:

- **Viruses** – attach themselves to files and spread when the file is executed.
- **Trojans** – appear as legitimate software but allow the attacker to access the system.
- **Ransomware** – locks data and demands money (ransom) for unlocking.
- **Spyware** – secretly monitors user activities and steals information (passwords, habits).
- **Adware** – displays unwanted ads and may slow down the system.
- **Worms** – spread independently across networks without user action.

Malware can steal personal and financial information, damage or delete files, take control of devices, monitor users, and use devices to carry out other attacks (e.g., DDoS attacks) [7].

2. Phishing – Scams via email, messages, or fake websites to steal passwords and banking information, often impersonating a bank or company. Unlike system hacking, phishing manipulates people, making it a form of social engineering. It works by sending a fake email, message, or call that appears legitimate. The victim clicks a link or opens an attachment, exposing passwords, data, or files. The attack exploits trust, fear, or urgency.

Types of phishing include: email phishing, spear phishing (targeted), smishing (SMS), vishing (calls), and clone phishing (fake copies of legitimate emails).

Goals include account theft, system takeover, spreading malware or ransomware, and financial fraud.

Basic protections: do not share passwords, verify senders, avoid suspicious links and unknown files. Advanced protections: employee training, phishing simulations, two-factor authentication (2FA), and security policies [3].

3. DDoS Attacks (Distributed Denial of Service) – These attacks overload a server with a large number of requests, causing a website or service to crash. They involve many computers (often infected) simultaneously sending massive requests to a server, aiming to disrupt its normal operation. DDoS attacks are dangerous because they can bring down large systems, are relatively easy to launch (even as “DDoS as a Service”), are hard to trace, and can last hours or days [8].

Types of DDoS attacks:

- Volumetric – consume bandwidth, e.g., UDP flood
- Protocol – exhaust server resources, e.g., SYN flood
- Application-layer – target web applications and are hardest to detect

Common goals: website crashes, service disruption (banks, e-commerce), financial losses, ransom (RDoS), and reputational damage. Basic protections: use CDN and cloud security, rate limiting, firewalls, and traffic filtering. Advanced protections: anti-DDoS systems, load balancing, automated attack detection, and cooperation with ISPs.

4. Man-in-the-Middle (MITM) – A cyberattack where the attacker secretly intercepts, reads, or alters communication between two parties without their knowledge. MITM is dangerous because it is invisible to users and targets communication rather than the system itself. Protection relies on encryption and careful network use [2]. The attack works by intercepting data, passwords, or card information, modifying messages, and injecting malicious content.

5. HTTPS Spoofing / SSL Stripping – An attack that removes HTTPS security while the user believes the connection is safe, allowing attackers to steal credentials, access bank accounts, intercept communications, and modify data.

Basic protection: use HTTPS websites, avoid unsecured public Wi-Fi, use VPN, and keep devices/software updated [7].

Advanced protection: two-factor authentication (2FA), certificates and encryption, and IDS/IPS systems.

6. SQL Injection – One of the most dangerous and common cyberattacks, where attackers insert malicious SQL code into web application input fields to gain unauthorized access to a database [7].

Types:

- Classic (In-band) – immediate results returned
- Blind – no direct response; results inferred from system behavior
- Time-based – uses delays to extract information
- Out-of-band – data sent through another channel (e.g., DNS)

Consequences: data theft, account compromise, data modification or deletion, system control, authentication bypass. Common targets include login forms, search fields, contact forms, and URL parameters.

Basic protection: input validation, prepared statements, avoid direct user input in SQL queries.

Advanced protection: ORM tools (e.g., Hibernate), limited database privileges, Web Application Firewall (WAF), and regular security testing.

7. Brute Force Attacks – Attempts many passwords to break into accounts, exploiting weak passwords. Types: Classic, Dictionary, Credential Stuffing, Hybrid. Consequences: email, social media, banking, business account compromise. Protection: strong, unique passwords, regular updates, 2FA, login attempt limits, CAPTCHA, IP blocking, password managers [6].

8. Zero-Day Attacks – Exploit unknown software/system vulnerabilities with no patch available. Goals: financial theft, identity theft, industrial espionage, political/military targets, ransomware, sabotage. Consequences: financial loss, trust loss, business interruption, legal issues. Protection: strong passwords, 2FA, avoid suspicious links/attachments, regular updates, antivirus, firewall, employee education [8].

9. Social Engineering – A type of cyberattack that targets people rather than technology, exploiting trust, habits, and psychological weaknesses. Attackers manipulate victims into revealing sensitive information or performing actions that compromise security. It is one of the key techniques in cybersecurity, as it is easy to execute, requires little technical skill, is hard to detect, and relies on human psychology.

Instead of hacking systems, attackers impersonate trusted entities (banks, colleagues, IT support), creating a sense of urgency or fear to trick victims into sharing data or clicking malicious links. Victims often unknowingly enable the attack themselves [3].

Common techniques include:

- Phishing – fake emails/messages requesting passwords or card details
- Spear phishing – targeted, personalized attacks
- Pretexting – fabricated scenarios to obtain information
- Baiting – e.g., infected USB devices disguised as valuable data
- Quid pro quo – offering help/services in exchange for credentials

Basic protection: do not share passwords, verify email senders, avoid suspicious links and unknown files.

Advanced protection: employee training, phishing simulations, two-factor authentication (2FA), and security policies.

Social engineering shows that humans are the weakest link in security—awareness and caution are the most important defenses.

3. Data protection

Data protection is a key segment of cybersecurity, involving measures to secure personal and business information. Personal data includes any information related to an identifiable individual: name, address, ID number, phone, IP address [9].

Key principles: lawfulness, transparency, data minimization, purpose limitation, and processing security [9].

Technical measures: encryption, antivirus, firewalls, 2FA, data backup. Organizational measures: employee training, security policies, access control, and risk management [5], [9].

4. Legal framework and regulations

Legal regulations play a vital role in data and cybersecurity protection, including:

- **International standards:** GDPR, ISO/IEC 27001, NIST frameworks.
- **National laws:** Personal Data Protection Act and Information Security Act.

Institutional roles are also significant, including public information commissioners, CERT teams, and regulatory bodies [10].

5. The role of users in cybersecurity

The human factor is both the weakest and most important element of security. Safe user behavior includes using strong passwords, avoiding suspicious links, updating systems regularly, and protecting personal data. Raising awareness of cyber risks is crucial for individuals, organizations, and the state [3].

Future challenges: rapid technological development, complex attacks, lack of experts, global connectivity [6].

Future trends: AI in cybersecurity, automated protection, zero-trust models, quantum cryptography [8].

6. Conclusion

This paper highlights that cybersecurity and data protection represent key pillars of a stable digital society [1]. It particularly emphasizes that effective protection cannot be achieved by relying on individual measures alone, but only through an integrated approach that combines technical protection mechanisms, adequate legal frameworks, and continuous user education [5], [10]. In this regard, the contribution of the paper lies in the systematization of basic security approaches and the emphasis on their interdependence in building a resilient digital environment.

Only by combining these elements can a secure digital environment be created. The future of cybersecurity will depend on society's ability to adapt to new threats and leverage modern technologies [3].

Furthermore, the paper contributes to understanding that contemporary cyber threats are constantly evolving, which requires a dynamic and adaptable security model. In this context, the need for a proactive approach is emphasized, including prevention, early detection, and rapid incident response.

Directions for future research may focus on the development of advanced artificial intelligence-based systems for cyberattack detection and prevention, the improvement of real-time risk management models, as well as a more detailed examination of the human factor in the cybersecurity chain. A particularly important direction is the analysis of the impact of emerging technologies, such as the Internet of Things and 5G networks, on the expansion of the attack surface and the development of new security strategies.

REFERENCES

- [1] Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Hoboken, NJ: Wiley.
- [2] Stallings, W. (2021). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Boston, MA: Pearson Education.
- [3] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W. W. Norton & Company.
- [4] Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Boston, MA: Pearson.
- [5] Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Boston, MA: Cengage Learning.
- [6] NIST. (2022). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). National Institute of Standards and Technology. Retrieved April 1st 2026, from <https://www.nist.gov/cyberframework>
- [7] Bishop, M. (2018). *Computer Security: Art and Science* (2nd ed.). Boston, MA: Addison-Wesley.
- [8] ENISA. (2024). *Cybersecurity Threat Landscape 2024*. European Union Agency for Cybersecurity. Retrieved March 28th 2026, from <https://www.enisa.europa.eu/publications>
- [9] Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer.
- [10] ISO (2018). *ISO/IEC 27001: Information Security Management Systems – Requirements*. Geneva, Switzerland: International Organization for Standardization.