International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 8 Issue 10 October - 2024, Pages: 108-113

Analysis of Personal Information Security Issues in Peacetime and Wartime

Svitlana Sotnik

Department of Computer-Integrated Technologies, Automation and Robotics
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
e-mail: svetlana.sotnik@nure.ua

Abstract: *This study addresses critical issue of personal data protection in both peacetime and wartime, focusing on impact of information warfare on data security. The research is particularly relevant given increasing cyber threats during military conflicts and need for robust data protection systems that can function effectively in various scenarios. The primary hypothesis posits that personal data becomes significantly more vulnerable to cyberattacks during wartime compared to peacetime due to intensification of information warfare. To test this hypothesis, study employs comprehensive methodology. The study introduces novel concept of "dual-purpose" personal data protection systems, designed to be effective in both peacetime and wartime conditions.*

Keywords—cyberattacks; personal data; protection; information; security

1. INTRODUCTION

The protection of personal information has become one of key problems of modern society, especially in context of digital technologies development and widespread use of Internet [1-3]. In peacetime, personal data (PD) protection issues often boil down to need to prevent information leakage, unauthorized access or misuse. However, in times of war, situation changes dramatically. Conflicts and aggravation of international relations become catalysts for cyberattacks aimed at breaking into critical systems that store sensitive information, such as data on citizens, military personnel, or government institutions.

In times of war, risk of PD being used for malicious purposes ranging from information attacks to blackmail or physical threats increases. The urgency of problem lies in fact that many protection systems that are effective in peacetime are vulnerable in wartime, when number and complexity of attacks increases. It should also be borne in mind that during wartime, it may be necessary to transmit confidential information under conditions of limited resources and time, which creates additional risks.

Thus, problem is to develop effective mechanisms for ensuring information security that will be sustainable both in peacetime and during hostilities, and for this purpose it is necessary to analyze issues of PD information security.

The purpose of this paper is to provide comprehensive analysis of personal information security issues in peacetime and wartime to determine impact of information warfare on personal data protection and to develop appropriate recommendations for improving security.

Therefore, to achieve this goal, following tasks are envisaged: analysis of existing approaches to personal data protection in peacetime; study of cyber threats during military conflicts and possible consequences for PD; determination of information warfare impact on personal data protection through analysis of modern cyberattacks used during military operations; developing recommendations for improving level of personal data protection both in peacetime and during military conflicts, taking into account specifics of information warfare and possible cyber threats.

2. RELATED WORK

Today, there is large number of works devoted to protection of personal information, as it is becoming extremely important topic in context of information technology rapid development. Many authors focus on protection of PD in peacetime. Military conflicts often lead to increase in cyberattacks aimed at critical information systems and personal data. The researchers cover various aspects of data protection, emphasizing growing importance of cybersecurity in context of global conflicts. The issues of information security of personal data are actively studied.

Among well-known scholars, we can single out works of V. Bryzhko and V. Pylypchuk, who specialize in legal protection aspects of privacy and individual freedoms in information society [4, 5]. The main focus of their works is on consideration of personal data protection problems exclusively in peacetime, while issues related to information protection during martial law remain unaddressed.

It is also worth mentioning works of Hrytsiuk Y. I. [6, 7], who studies information security issues at state level. In his research, author analyzes information resource protection systems, in particular at enterprise level. However, it is worth noting that Hrytsiuk's work lacks detailed analysis of information protection under martial law, since main focus of his research is on peacetime.

A significant role is played by scientists such as Schneier B. [8, 9], who specializes in cryptography and digital privacy issues, and Richard A. Clarke [10, 11], known for his work in field of cybersecurity. They explore challenges and threats associated with protection of personal data in context of

global cybersecurity. However, his work lacks detailed analysis of PD protection in context of military conflicts, as his main focus is on peacetime and international cooperation in cyberspace.

Modern researchers make important contribution to development of personal data protection strategies in various contexts, but issue of personal information security during martial law remains insufficiently addressed in scientific research. Most existing works on data protection are focused on peacetime and general aspects of cybersecurity. This creates gap in understanding and analyzing challenges related to personal data protection during military conflicts, when cyber threats are growing significantly. Thus, there is need for additional research that would focus on protection of personal data in martial law and during armed conflicts.

3. METHODOLOGY

The information base of study is based on analysis of scientific papers on information security, legal aspects of PD protection, cybersecurity in peacetime and military conflicts. The included sources [4-20] provide data on current methods and strategies for protecting information systems.

Information processing consisted of:

1. Critical analysis of scientific publications.

2. Systematization and comparison of personal data protection existing methods.

3. Identification of trends in cyber threats and their impact on information systems during military operations.

The limitations of study are: lack of access to confidential materials or reports of government agencies related to cyber defense in time of war; insufficient number of published materials on PD protection in wartime; potential dependence of conclusions on current technological capabilities that may change over time.

It is assumed that during wartime, personal data becomes more vulnerable to cyberattacks than in peacetime due to intensification of information warfare.

European legislation, in particular General Data Protection Regulation (GDPR), classifies personal data as those that can directly or indirectly identify person and sets strict requirements for their processing and protection.

3.1 ANALYSIS OF EXISTING APPROACHES TO PERSONAL DATA PROTECTION IN PEACETIME

The main existing approaches to personal data protection in peacetime:

1. The legal approach includes: creation and implementation of legislative framework (e.g., GDPR in EU); establishment of rules and regulations for PD processing; determination of liability for data protection violations.

2. Technological approach includes: use of data encryption during storage and transmission; implementation of access control systems; use of data anonymization and pseudonymization technologies.

3. Organizational approach includes: development of internal data protection policies and procedures; appointment of responsible persons (e.g., Data Protection Officer); regular audits and risk assessments.

4. The principle of «Privacy by Design» is integration of privacy protection at design stage of systems and processes and ensuring highest possible level of privacy by default.

5. The risk-based approach is to conduct data protection impact assessment (DPIA); implement protection measures proportionate to identified risks.

6. Sectoral approach – development of specific standards for different sectors (finance, healthcare, etc.) and implementation of sectoral codes of conduct.

The results of main approaches analysis to PD protection in peacetime in Table 1.

Table 1: Comparison of dynamic and static QR coding

#	*Approaches*	*Advantages*	*Limitations*
1	Law	- creates clear regulatory framework, sets common standards for all and ensures legal protection of data subjects.	- may lag behind technological development; - difficulty in international harmonization; - requires resources to ensure compliance.
2	Technological	- provides technical data protection; - can automate protection processes; - can quickly adapt to new threats.	- requires constant updating; - can be expensive to implement; - depends on human factor when used.

Continuation of Table. 1

#	*Approaches*	*Advantages*	*Limitations*
3	Organizational	- creates culture of data protection in organization; - provides systematic approach to protection; - allows you to adapt measures to specifics of organization.	- requires constant monitoring and support; - may be ineffective without management support; - depends on integrity of employees.
4	Privacy by Design	- ensures data protection at all stages; - reduces risk of breaches; - increases user confidence.	- increase development time and cost; - requires change in approach to system design; - limit functionality.
5	Risk assessment	- allows for efficient allocation of resources; - ensures proportionality of protection measures; - helps to identify vulnerabilities.	- can be difficult for small organizations; - requires constant updating; - depends on quality of assessment.
6	Industry	- takes into account specifics of particular sectors; - provides more precise protection standards; - facilitates exchange of best practices in industry.	- may create heterogeneity of standards; - requires sectoral expertise; - may complicate inter-sectoral cooperation.

No single approach is universal and fully sufficient on its own. The most effective approach is integrated use of different approaches, which allows to compensate for limitations of some approaches with advantages of others. The choice of specific approaches and their combination depends on specifics of organization, industry, type of data processed, and legal environment.

3.2 Study of Cyber Threats During Military Conflicts

Military conflicts significantly increase risk of cyberattacks on critical information systems, which in turn can have serious consequences for personal data security. In such circumstances, attacks are aimed not only at military facilities but also at civilian institutions and infrastructures, which increases risk of leakage or unauthorized access to personal information of citizens. In view of this, study of impact of military conflicts on data security is becoming even more relevant, as large-scale cyberattacks can lead to massive violation of privacy rights, which makes it important to analyze such cyber threats (Table 2).

Table 2: Existing cyber threats and purpose

#	*Cyber threats*	*Purpose*
1	Targeted attacks on databases from hacker groups affiliated with hostile states that may be trying to penetrate government and military databases.	Access to personal data of military personnel, civil servants and civilians.
2	Phishing campaigns are mass mailings of malicious emails that imitate official messages.	Stealing credentials and gaining unauthorized access to personal information.
3	Attacks on identification systems – hacking of electronic identification systems.	Access to wide range of personal data.
4	Mobile device compromise is distribution of malicious software for smartphones.	Gaining access to personal data stored on devices.

The threats listed in Tab. 1 emphasize importance of strengthening cybersecurity and personal data protection

measures at both state and individual levels during military conflicts.

Possible consequences for personal data from cyber attacks are shown in Fig. 1.

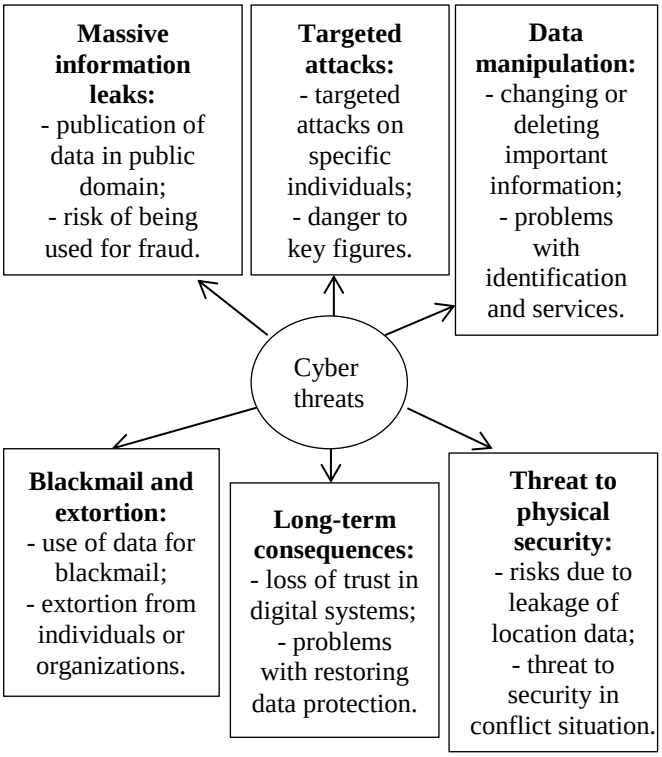

Fig. 1. *Cyber threats during military conflicts and their consequences for personal data*

The analysis underscores critical need for enhanced cybersecurity measures during military conflicts, as these situations create unique vulnerabilities in personal data protection. The threat landscape becomes more complex and dangerous, requiring coordinated responses at both governmental and individual levels to protect sensitive information.

3.3 Determining impact of information warfare on protection of personal data during military operations

In context of information warfare, protection of personal data becomes critical not only for privacy but also for national security. Cyberattacks can be used not only to steal information, but also to manipulate public opinion, disinformation and undermine trust in government institutions. The analysis identified impact of cyberattacks on protection of personal data during military operations (Table 3).

Table 3: The impact of cyberattacks on personal data protection during military operations

Type of cyber attack	***The mechanism of influence***	***Implications for personal data***	***Protection measures***
DDoS attacks	Systems overload, disruption of access to services.	- temporary data unavailability; - risk of compromise during recovery.	- distributed systems; - backup and recovery; - traffic filtering.
Phishing	Deception of users, theft of credentials.	- unauthorized access to accounts and leakage of personal information.	- user training; - two-factor authentication; - anti-phishing filters.
Malicious software	Infection of systems, data theft.	- massive data leakage; - spying on users.	- anti-virus protection; - regular software updates; - network segmentation.
Attacks on control systems	Disruption of critical infrastructure.	- loss of control over data and risk of information manipulation.	- isolation of critical systems; - enhanced monitoring; - backup control systems.
Data manipula-tion	Changing or deleting information in registers.	- violation of data integrity and problems with identification.	- anomaly detection systems; - regular data audits; - secure backups.

3.4 Recommendations for improving level of personal data protection

Given growing threats in today's information warfare, as well as possible cyberattacks both in peacetime and during military conflicts, it is necessary to develop comprehensive measures to improve level of PD protection. It is proposed to introduce concept of «dual purpose» for personal data protection systems, which is reflected in recommendations that should take into account specifics of various cyber threats, including attacks on critical information systems, and ensure resilience of protection systems in both scenarios. The main principles of concept are: improving encryption technologies; raising user awareness; introducing multi-level authentication; regular audits of information systems. Another important aspect is readiness to respond quickly to threats and ability to recover from attacks, especially in wartime. Here are recommendations for improving level of PD protection (Fig. 2).

Fig. 2. *Recommendations for improving level of personal data protection*

Therefore, modern protection of personal data cannot be static or single-purpose, but instead must be dynamic and adapt to different levels of threats and scenarios.

4. Conclusions

The study provides comprehensive analysis of personal information security issues in peacetime and wartime, identifies impact of information warfare on personal data protection, and offers appropriate recommendations for improving security. The tasks were accomplished. A comprehensive approach to analyzing personal data protection in context of peacetime and wartime has been implemented. Most previous studies have focused on only one of these aspects, while this paper offers integrated view of problem. The scientific hypothesis that predicted increased vulnerability of personal data to cyberattacks during wartime compared to peacetime due to intensification of information warfare was confirmed. The study found that in context of military conflicts, number and complexity of targeted attacks on databases increases; risk of massive information leaks and targeted attacks increases; threat to physical security increases due to leakage of location data; and impact of cyberattacks on critical infrastructure and control systems increases. The novelty is that concept of "dual-purpose" for personal data protection systems has been introduced, which should be effective both in peacetime and in military conflicts.

The proposed recommendations allow to:

- Ensure continuity of personal data protection regardless of external circumstances.
- Optimize resources required for information protection, avoiding need to develop separate systems for different conditions.
- Increase overall resilience of information systems to various cyber threats. The work is prerequisite for providing practical recommendations for strengthening protection of personal data and promoting development of more effective cybersecurity strategies.

5. References

[1] Kaponkin, V. et al. (2024). The role of big data in improving functionality of search engines. The 8th International scientific and practical conference "European congress of scientific achievements" (August 12-14, 2024), 69-76.

[2] Nevludov, I.S., et al. (2023). Cloud giants: AWS, Azure and GCP. 2nd International Conference on Innovative Solutions in Software Engineering Ivano-Frankivsk, Ukraine, November 29-30, 18-23.

[3] Deineko, Z., et al. (2022). Confidentiality of Information when Using QR-Coding. International Journal of Academic Information Systems Research (IJAISR), 6(9), 10-15.

[4] Bryzhko, V.M., Pylypchuk, V.H. (2020). Pryvatnist, konfidentsiinist ta bezpeka personalnykh danykh. Informatsiia i pravo, 1(32), 33-46.

[5] Bryzhko, V.M., Pylypchuk, V.H. (2021). Bezpeka personalnykh danykh: pravovi standarty Yevropeiskoho Soiuzu ta suchasni prykladni problemy. Informatsiia i parvo, 1(36), 17-28.

[6] Hrytsiuk, Yu. I., Sivets, O. O. (2016). Obgruntuvannia rozumnoi dostatnosti struktury systemy zakhystu informatsiinykh resursiv pidpryiemstva. Naukovyi visnyk NLTU Ukrainy, 378-388.

[7] Hrytsiuk, Yu. I., Stashevskyi, Z. P. (2015). Modeli ta mekhanizmy formuvannia kompetentnosti personalu dsns ukrainy dlia realizatsii it-proektiv z informatsiinoi bezpeky. Innovatsiini kompiuterni tekhnolohii u vyshchii shkoli: Materialy 7-yi naukovo praktychnoi konferentsii, 136-143.

[8] Schneier, B. (2019). We have root: Even more advice from Schneier on security. John Wiley & Sons, 306 p.

[9] Schneier, B. Schneier on security: privacy and control Journal of Privacy and Confidentiality, 2(1), 3-4.

[10] Clarke, R. A., Knake, R. K. (2010). War C. The Next Threat to National Security and What to Do About It New York. Ecco, 290 p.

[11] Clarke, R. A. (2016). The risk of cyber war and cyber terrorism. Journal of International Affairs, 70(1), 179-181.

[12] Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. Legal Issues in the digital Age, 4(2), 78-121.

[13] Basholli, F. (2022). Cyber warfare, a new aspect of modern warfare. In VI International Scientific Conference on Security «CONFSEC», 52-54.

[14] Whyte, C., Mazanec, B. (2023). Understanding cyber-warfare: Politics, policy and strategy. Routledge, 364 p.

[15] Tikk-Ringas, E. (2023). Evolution of the Cyber Domain: The Implications for National and Global Security. Routledge, 212 p.

[16] Anakhov, P. et al., (2023). Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network. Cybersecurity Providing in Information and Telecommunication Systems, 3550, 240-245.

[17] Sufi, F. (2023). Social media analytics on Russia–Ukraine cyber war with natural language processing: Perspectives and challenges. Information, 14(9), 485.

[18] . Willett, M. (2023). The cyber dimension of the Russia–Ukraine War. In Survival: October-November 2022, 7-26.

[19] Lehto, M. (2023). Cyber Warfare and War in Ukraine. Journal of Information Warfare, 22(1), 61-75.

[20] Jenkinson, A. (2023). Digital Blood on Their Hands: The Ukraine Cyberwar Attacks. Crc Press, 200.