VARNA FREE UNIVERSITY
„CHERNORIZETS HRABAR“

FACULTY OF LAW
DEPARTMENT OF SECURITY AND SAFETY

TEODORA KIRILOVA LICHEVA, PhD

TRANSFORMATION OF THE MANAGEMENT CYCLE IN INTELLIGENCE AND COUNTERINTELLIGENCE THROUGH INTEGRATION OF MODERN TECHNOLOGICAL SOLUTIONS

A B S T R A C T

of a dissertation
for the award of the scientific degree „Doctor of Science“,
Professional field 9.1 „National Security“

Varna
2026

VARNA FREE UNIVERSITY
„CHERNORIZETS HRABAR“

FACULTY OF LAW
DEPARTMENT OF SECURITY AND SAFETY

TEODORA KIRILOVA LICHEVA, PhD

TRANSFORMATION OF THE MANAGEMENT CYCLE IN INTELLIGENCE AND COUNTERINTELLIGENCE THROUGH INTEGRATION OF MODERN TECHNOLOGICAL SOLUTIONS

A B S T R A C T

of a dissertation
for the award of the scientific degree „Doctor of Science“,
professional area 9.1 „National Security“

Reviewers:
Prof. Stefan Angelov Simeonov, D.Sc.
Prof. Georgi Vasilev Bahchevanov, Ph.D.
Prof. Boyan Kirilov Mednikarov, D.Sc.

Varna
2026

The presented dissertation covers 475 pages and consists of an introduction, three chapters, a conclusion, contributions and a bibliography. The individual chapters presented in the table of contents are divided into subchapters and end with summaries and conclusions. The main text contains 94 tables and 34 figures.

The literature used consists of 514 sources, which include:

- international and supranational acts (4 sources);
- Bulgarian legislation and strategies (9 sources);
- foreign acts and standards (17);
- literature in Cyrillic (24);
- literature in Latin (61);
- literature in Chinese (5);
- Internet sources (394).

To prepare the dissertation, mainly internet sources and articles were used, due to the rapid change and development of information and communication technologies and innovations, and a significant delay in the legislative framework in the field.

The defense of the dissertation before the scientific jury will be held on August 25, 2026, at 10:30 a.m. in the conference hall of the Varna Free University „Chernorizets Hrabar“. The materials for the defense are available in the Department of Public Order and Security, as well as on the university website www.vfu.bg.

I. General characteristics of the dissertation work

This dissertation explores the transformation of the security management cycle under the influence of modern technological innovations. In the conditions of the Fourth Industrial Revolution, the security environment is characterized by exceptional dynamics, complexity and interconnectedness of threats (Schwab, 2018). Traditional management models are analog, based primarily on human factors, expert judgment, and static p

r

o
- information collection and analysis;

c
- preparation of forecasts, estimates and solution options;

e
- decision making and scenario development

d
- planning;

u
- organizing;

r
- execution;

e
- control and verification of implementation with the planned goal.

s The implementation and use of Big Data, artificial intelligence (AI), cloud technologies, blockchain, drones (UA) and other modern tools is changing the content a

T Traditional, hierarchical management models are proving increasingly inadequate

1. Relevance and significance of the study

e The Fourth Industrial Revolution (Industry 4.0) is laying the foundation for a fundamental transformation in the way national security institutions function (Radulov, 2019). Intelligence and counterintelligence, which are key pillars of the state security architecture, are facing unprecedented challenges posed by the rapid development of digital technologies, globalization, and the overwhelming volume of information flows (World Economic Forum, 2025), as well as the increasing complexity of threats.

The relevance of the study stems from the objective need to adapt national security systems to the new technological environment. The integration of technologies such as artificial intelligence, big data analysis, cloud computing, blockchain and autonomous systems is not just a technical improvement, but a strategic necessity to achieve information and operational superiority. The significance of the topic is determined by several key aspects:

g

f

y

t

h

- **Scientific and theoretical significance:** The study contributes to the development of the theory of security management by offering a new conceptual model for the transformation of the management cycle, which synthesizes and adapts classical management principles with the capabilities of digital technologies.
- **Scientific and applied significance:** The developed models, analyses and recommendations have direct practical value for state institutions in intelligence and counterintelligence of the Republic of Bulgaria. They provide a methodological basis for modernization, digitalization and increasing the effectiveness of intelligence and counterintelligence structures in accordance with the best Euro-Atlantic and global practices.

The topic is extremely relevant given the accelerated digitalization of the public sector, increased international regulatory requirements, and the need to modernize national security institutions.

2. Object of the study

In accordance with the set goal and objectives, the following object and subject of research are defined in the dissertation:

- The object of the study is the management cycle in intelligence and counterintelligence systems - considered in its entirety by interrelated processes, including the phases of information collection and analysis; preparation of forecasts, forecast assessments and decision options; decision-making and scenario preparation; planning; organization; implementation; control and verification of implementation with the planned goal. All stages are implemented in the context of contemporary challenges for national and international security.
- **The subject of the study** is the transformation processes of the management cycle, brought about by the integration of technological innovations. The analysis focuses on the ways in which new technologies change the management activities in intelligence and counterintelligence structures at the national and international levels, as well as on the emerging new management models and strategies.

3. Goals and objectives of the dissertation

The thesis of the dissertation is that modern management processes are inevitably related to technological progress and their development is essentially exponential, as is

the development of modern technologies. Management and the security environment are adequate to the economic development, which also determines their effectiveness.

The security ecosystem is more sensitive to the processes that develop in politics, the economy, and socio-economic processes, which is why the need for rapid digital transition and the use of high-tech solutions is a guarantee not only for efficiency, but also for addressing modern security challenges.

In view of the above, ***the purpose*** of the study is to establish trends in the development and improvement of the elements and essence of security management in the transition from analog to technological digital management. Based on the study of the information available to date, I propose frameworks and concepts for modernizing and increasing the effectiveness of security management. Modeling modern intensive management scenarios facilitates practical activities for effective management in the complex security ecosystem and at the same time creates the opportunity for adequate response to modern threats. Security challenges are closely related to the development of modern technologies and, accordingly, the counteraction and management of crises related to them cannot be other than high-tech.

To achieve this goal, I set the following ***research tasks:***

1. Comparison of classical and digital management to clarify common points and differences;

2. Deriving the role and importance of each of the new technological directions in relation to the elements of the management cycle;

3. Determining the framework and development scenarios of each technology in relation to the individual phases of the management cycle;

4. Research into the synergy of modern technologies in terms of increased efficiency of digital security management.

4. Research methodology

The methodological framework of the dissertation is placed at the intersection of governance, national security, and modern information and communication technologies.

The methods used are selected to provide a systematic, multi-layered and interdisciplinary analysis of the national security system, the transformation of management practices and the impact of innovative technologies on them. The methodological apparatus includes general scientific, specialized and applied methods, which in their entirety form an integrated research framework combining descriptive,

analytical and prognostic elements, as well as scenario development and the creation of descriptive models.

General scientific methods

Analysis and synthesis – in the study of theoretical propositions and summarizing data from various sources;

Induction and deduction – for formulating conclusions from particular cases to general patterns and vice versa

Specialized methods and approaches

Systemic and structural-functional approach – to consider the management cycle as a single system of interconnected elements

Management analysis – for constructing matrices and models that show the applicability of various technological solutions by cycle stages and by management levels (strategic, tactical, operational).

Documentary and legal-analytical method

Documentary and legal-analytical approach – research of the normative and strategic framework of the security system at the national and international level: security strategies and concepts, laws and regulations, regulatory regimes, reports and documents of international organizations.

Content analysis – to extract key concepts, priorities and dominant concepts.

Historical and comparative approaches

Historical-genetic method – to trace the evolution of the security system and governance models in different historical periods.

Historical-comparative and comparative analysis – to compare the development of the Bulgarian security system with similar systems in other countries.

Comparative analysis – to compare management models and practices in countries with highly developed intelligence structures, leading technological countries and Bulgaria.

Scenario and prognostic analysis, scenarios and descriptive models

Scenario analysis and scenario development – to develop alternative possible developments of the security system in the face of accelerated technological evolution.

Modeling – to develop conceptual models for transformation of the management cycle

Prognostic analysis – to outline the most likely trends in the development of technologies, management practices and regulatory regimes in the medium and long term.

Integrated Methodological Matrix

The combination of systemic and structural-functional approaches, management analysis, general scientific methods (analysis, synthesis, induction, deduction), historical and comparative approaches, content analysis, as well as scenario and prognostic analysis, scenario development and creation of descriptive models, forms an integrated methodological model of the dissertation.

The research draws on a wide range of sources - scientific publications, monographs, strategic documents of national and international organizations, regulatory acts and reports from leading research centers.

5. Contributions

The analysis carried out in the dissertation, concerning the management stages in security, is a contribution to Bulgaria, and is based on research that has shown that the country lags significantly in terms of implementing and using new technological capabilities in intelligence and counterintelligence activities.

The main contribution is the formulation of the migration of the elements of the management cycle, characteristic of the security services, from traditional and analog, to modern digital processes, including the specifics of the separate levels of management according to the time horizon and the structural levels in the national security system.

Theoretical and -scientific contributions

1. A concept for digital security management has been formulated;
2. An interdisciplinary model for the integration of new technologies into security management has been developed;
3. Formalized matrix models and templates for the application of key technologies have also been derived;
4. A new reading of the development of the Bulgarian security services is proposed through an in-depth historical -and institutional analysis;
5. An ethical-legal and governance framework for technological transformation in security has been developed;

6. A comprehensive conceptual framework of the security management cycle has been developed in the context of Industry 4.0–6.0 and Security 4.0–6.0;

7. The evolution of security from Security 1.0 to Security 5.0 (and trends towards 6.0) is systematized and comparatively analyzed.

Practical and applied contributions

1. Applicable analytical tools for strategic planning and security reforms have been created;

2. Frameworks have been developed to measure the effectiveness of the management cycle through specific technologies in intelligence and counterintelligence;

3. Directions and models for training and development of human resources in the context of digital transformation have been defined;

4. Guidelines are proposed for improving the regulatory and ethical framework related to the use of new technologies in security;

5. A practical framework has been built for a phased transition from an analog to a digital management cycle;

6. A reference framework has been created for assessing technological lag and national security risks, based on comparative case studies and technological maturity indicators.

6. Practical significance of the study

The practical significance of the dissertation work is multi-layered. It encompasses applications at the national, institutional and operational levels. The practical significance is systematized in the following main areas:

Frameworks for measuring the effectiveness of the management cycle

The study developed specific frameworks and matrix models for measuring the effectiveness of the management cycle through specific technologies in intelligence and counterintelligence. These frameworks can serve as practical guides in the design and implementation of technological solutions in security services, because they show the application of different technological solutions by stages of the cycle and by levels of management - strategic, tactical and operational.

Human resource training and development

Directions and models for employee training and development in the context of digital transformation have been defined. These models can be used in the development

of curricula, in-house training and scenario-based training with elements of virtual and augmented reality (AR/VR), including simulation environments for staff training.

Adaptation of the regulatory and ethical framework

Guidelines are proposed for improving the regulatory and ethical framework related to the use of new technologies in security. They can be used in the preparation of legislative changes, internal policies and mechanisms for independent audit, evaluation and monitoring, taking into account the risks of mass surveillance, algorithmic bias and violation of privacy.

Conceptual model for digital security management

The dissertation proposes a concrete conceptual model for digital security management, applicable in practice. The model envisages the construction of modern digital platforms, predictive analytics systems, digital twins of critical infrastructure, implementation of a zero-trust architecture (ROSE et al. al., 2020) and post-quantum cryptographic solutions.

Contribution to Bulgaria and Euro-Atlantic integration

The practical application in **the Bulgarian context is particularly significant** . The study finds that Bulgaria lags significantly behind in terms of implementation and use of modern technological capabilities in the security sector, due to limited resource capacity, outdated information infrastructure and shortage of highly qualified personnel. The results of the study can serve as a basis for developing a national strategy for digital transformation, in which science, state institutions and the private sector act as partners and work in sync.

Operational advantage and threat management

Modeling modern intensive management scenarios facilitates practical work on effective leadership in the complex security ecosystem. The integration of blockchain, AI and big data into the operational cycle provides concrete tools for moving from reactive investigation to preventive threat prediction, including hybrid and cyber threats, which is crucial for national security.

The practical significance of the study is expressed in the provision of applicable frameworks, models and strategic guidelines through which intelligence and counterintelligence structures can actually modernize their management cycle and gain a lasting operational advantage in the conditions of the modern digital era.

7. Limitations

The study has significant limitations that should be taken into account when interpreting the results and formulating conclusions.

First of all, the limitations are that ***security is considered in a limited format.*** of the security services, namely:

- Intelligence;
- Counterintelligence;

Second, ***the geographical and comparative scope is limited***. The analysis focuses on a limited set of countries, selected based on their leading role in the international system, the availability of sufficient publicly available data, and Bulgaria.

Thirdly, ***the source base used is mainly from publicly available documents,*** academic literature, strategic and regulatory acts, as well as specialized analyses.

Fourth, ***the study has a time horizon limited to processes and data as of 2025,*** due to the rapid development of technologies and the proposed trends should be perceived as a so-called **snapshot,** and not as a final and unchanging picture.

Fifth, ***about Bulgaria, the study encounters specific limitations in the availability and detail of public data.***

Sixth, some ***of the formulated recommendations and models are of a normative and strategic nature***.

II. Main content of the dissertation

1. Structure of the study

Introduction

CHAPTER I. Evolution of security

Section I. Industrial Revolutions and Security Developments

Section II. Security Management

1. Comparative analysis of security management in different countries

2. Security Management in Bulgaria

3. Security management methods

4. Stages of the security management cycle

5. Transformation of the management cycle in the digital environment

6. The Security Management Cycle: Industry 4.0, Industry 5.0 and Industry 6.0

Conclusions

CHAPTER II. New technologies in security

Section I. Big Data

1. Understanding big data and contemporary challenges

2. Comparative analysis: global versus Bulgarian opportunities

Section II. Artificial Intelligence

1. Practical cases

2. Key milestones in the use of AI in security

3. International and Bulgarian experience. Comparison

Section III. Cloud Computing

1. Technological development of security

2. Application of cloud solutions in security. International and Bulgarian experience. Comparison

3. Peripheral computing

4. Confidential calculations

Section IV. Blockchain Technology

1. Integrating blockchain into security

2. Applications in a global perspective and Bulgaria. Comparison

3. Post-quantum protection of blockchain systems

4. Smart contracts in security

5. Official e-files

Section V. Drones

Section VI. Additive technologies

Section VII. Nanotechnology

1. Nano-devices and materials with security applications

2. Applications of nanotechnology in security in a global and Bulgarian aspect. Comparison

Section VIII. Geotechnologies

1. Geotechnologies in special services – global and Bulgarian context. Comparison

2. National legislation and control mechanisms

Section IX. Virtual and Augmented Reality

1. Virtual reality security applications

2. Applications of augmented reality in field operations

3. Comparative analysis and case studies: international experience and Bulgaria

Section X. Space Technologies

1. Applications of space technologies in security

2. Case studies and operational tasks in an international perspective and Bulgaria. Comparison

Section XI. Synergy between security technologies

1. Digital twins

2. Soft robotics

3. Zero Trust Concept

Section XII. Data Security

Conclusions

CHAPTER III. Digital Security Management

Section I. Big Data

1. Information collection, processing and analysis

2. Forecasting and preparing management decisions

3. Management Decision Making: Processes and Frameworks

4. Planning and organizing the implementation of decisions

5. Implementation and control

Section II. Artificial Intelligence

1. Intelligence

2. Counterintelligence

Section III. Cloud Computing

1. Collection, processing and analysis of information in a cloud environment

2. Forecasting and preparing management decisions

4. Planning and organizing

3. Control, audit and constant monitoring

Section IV. Blockchain

1. Intelligence

2. Counterintelligence

Section V. Drones

1. Intelligence

2. Counterintelligence

Section VI. Additive manufacturing

1. Intelligence

2. Counterintelligence

Section VII. Nanotechnology

1. Intelligence

2. Counterintelligence

Section VIII. Geotechnologies

1. Intelligence

2. Counterintelligence

Section IX. Virtual and Augmented Reality

1. Intelligence

2. Counterintelligence

Section X. Space Technology

1. Application of space technologies in the intelligence management cycle

2. Application of space technologies in the counterintelligence management cycle

Conclusions

Conclusion

Contributions

Bibliography

II. Description of the chapters

Introduction

The introduction aims to set the framework of the dissertation work. It justifies the relevance, subject and object of the research, the goals and objectives of the work, the applied methodology. The framework of the research is outlined, emphasizing the practical applicability of new information and communication technologies, with strategic benefits for increasing the efficiency and security of intelligence services. The following 3 chapters logically arise from the boundaries set in it.

Chapter I: Evolution of Security

The first chapter of the dissertation presents a historical and comparative analysis of the evolution of security, examining how technological transformations brought about by the industrial revolutions have influenced the methods and tools of intelligence and counterintelligence. The analysis traces the development from the first mechanized systems to predictive models based on quantum technologies and artificial intelligence.

Chapter I is organized into two main sections: **„Industrial Revolutions and Security Development“ and „Security Management“,** the latter including six subsections covering a comparative analysis of management systems in different countries, institutional development in Bulgaria, the methods and stages of the management cycle, its transformation in the digital environment, and the comparative analysis of security in the context of Industry 4.0, 5.0 and 6.0.

Main theses and scientific results

1. Industrial revolutions as a driving force of transformation

A primary research contribution of the chapter is the systematization of the evolution of security in parallel with the chronology of industrial revolutions. The author proves that each industrial revolution generates a specific type of threat and imposes a corresponding transformation in intelligence and counterintelligence structures.

The first industrial revolution (Industry 1.0) laid the foundations for structured intelligence. During this period, the first agent networks for monitoring labor movements appeared and institutions for protecting industrial secrets were born. The steam engine and railway transport served as tools for deploying intelligence activities and intercepting communications.

The Second Industrial Revolution (Industry 2.0) introduced the telephone and the telegraph as standard tools of intelligence and counterintelligence, and industrial

espionage became international in nature. It is important to note that photography entered the picture as a means of gathering information.

The Third Industrial Revolution (Industry 3.0) is associated with the emergence of electronic intelligence (SIGINT), Big Data analysis, and international security networks. Digitalization imposes cybersecurity as a key component of counterintelligence.

The Fourth Industrial Revolution (Industry 4.0) marks the entry of artificial intelligence (AI), the Internet of Things (IoT), and autonomous systems into security. Intelligence is developing AI-based tools for analyzing data sets, and counterintelligence is focusing on protecting against IoT threats and cyberattacks (Radulov, 2019).

The fifth industrial revolution (Industry 5.0) introduces the symbiosis between humans and intelligent machines. New challenges arise related to genomic espionage, misuse of biometric data, neurotechnology and quantum computers.

2. Evolution of the security concept – from Security 1.0 to Security 6.0

The evolution of security is presented systematically in five consecutive frameworks, each of which reflects the specific needs of the respective technological era:

- **Security 1.0** – physical protection, limited mechanical methods;
- **Security 2.0** – standardized industry protocols and procedures;
- **Security 3.0** – protection of early information systems, cryptography and antivirus programs;
- **Security 4.0** – integrated cybersecurity for connected systems, IoT protection, blockchain and machine learning;
- **Security 5.0** – human-centric , sustainable and flexible protection, in which technologies serve people (Licheva, 2024), and not the other way around, and in which physical and digital security merge into a single system;
- **Security 6.0** is a prognostic stage where both the potential threats from quantum computing to existing cryptographic systems and the opportunities that quantum cryptography offers for creating unbreakable communication channels are analyzed.

A key theoretical contribution is the conceptualization of Security 5.0 as a concept that requires: preemptiveness and predictability through AI and big data; convergence between physical and cybersecurity; improved public-private integration; and human-centric systems aligned with ethical standards and personal data protection.

The author examines in detail the stages of the intelligence and counterintelligence management cycle, including strategic planning, information collection and analysis,

forecasting, decision-making, organization, execution, and control. It is argued that with the advent of digital technologies, each of these stages undergoes a qualitative transformation.

Particular attention is paid to the change in the role of the manager - from an administrator of routine processes to a strategic leader, oriented towards data and technological optimization of the organization. The introduction of "smart analytics" based on AI allows for scenario planning and predictive risk management in real time.

Comparative analysis: Security 4.0 – 5.0 – 6.0

The study developed a detailed comparative analysis of the management cycle in the three successive phases of security development:

Table 1the management cycle from Security 4.0 to Security 6.0

Management stage	***Security 4.0***	***Security 5.0***	***Security 6.0***
Information collection	IoT /SCADA, human analysis	AI, biometrics, automatic validation	Autonomous agents, quantum encryption
Forecasting	Historical data, templates	Machine learning, neural networks	Self-tuning AI models, quantum simulations
Decision making	Centered around the person	AI recommendations validated by humans	Autonomous decisions, human intervention only in borderline cases
Planning	Solid, annual	Dynamic, real-time	Self-correcting , adaptive
Organizing	Hierarchical, static	Hybrid, flexible	Self-governing network structures
Control	Completely human	Interactive AI, automation	Fully autonomous, self- healing

Security Management in Bulgaria

Within the framework of the historical-institutional analysis, the development of the Bulgarian security services is traced - from the centralized apparatus of the State Security (SS) during the Cold War period to the reform and creation of the State Security

Service and the Bulgarian National Security Agency after 1989. A gradual but consistent transition to an architecture compatible with Euro-Atlantic standards is noted, accompanied by increasing investments in technological modernization and cybersecurity.

Head conclusions

The conclusions from Chapter I can be summarized in three key findings.

First, security management is a complex, multi-layered and dynamically evolving system in which historical legacies, legal and ethical frameworks, and technological progress intersect.

Second, the resilience and effectiveness of intelligence services can no longer be thought of outside the context of the implementation of information systems, artificial intelligence, cybersecurity, and the network connectivity of critical infrastructure.

Third, technological integration must be accompanied by sustainable regulatory, ethical and institutional mechanisms with clear accountability regimes, audit systems and independent oversight to ensure a balance between efficiency and protection of civil rights.

The main conclusion is undoubtedly proven that the future of security management depends on the successful combination of three interdependent dimensions: technological innovation, democratic control, and a strategic vision for an integrated, sustainable management cycle, adequate to the challenges of the 21st century.

Chapter II: New technologies in security

Chapter II is the most voluminous and technologically focused part of the dissertation. It includes twelve sections:

- ✓ Big data;
- ✓ Artificial intelligence;
- ✓ Cloud computing (including edge and confidential computing);
- ✓ Blockchain technology;
- ✓ Drones;
- ✓ Additive technologies;
- ✓ Nanotechnology;
- ✓ Geotechnologies;
- ✓ Virtual and augmented reality;
- ✓ Space technologies;

✓ Synergy between security technologies (digital twins, soft robotics, Zero Trust architecture);

✓ Data security.

Main theses and scientific results

1. Big Data – from reactive analytics to predictive intelligence

The author argues that the integration of Big Data represents a structural transformation of intelligence management. The transition from reactive case-based investigation to proactive, predictive intelligence driven by continuous analysis of massive volumes of heterogeneous data in real time is outlined as a strategic goal. The key characteristics of Big Data – Volume, Velocity, Variet, Veracity and Value – are analyzed in the context of the specific challenges facing intelligence agencies (Wired, 2012).

The comparative analysis between global intelligence capabilities (the US NSA processes over 1.7 billion communications daily) and Bulgarian structures categorically shows a structural lag in technological capacity, funding, and regulatory readiness.

2. Artificial Intelligence – a key technological core of security

AI is emerging as the engine of modern intelligence. The author of the study systematizes its historical development into four key stages – from the era of expert systems (1970s–1980s), through biometrics and pattern recognition (1990s), to deep learning and generative AI (2020).

Key applications include: automated OSINT analysis; natural language processing (NLP) for detecting propaganda and threats in cyberspace; computer vision for analyzing satellite and drone imagery; and machine learning for detecting anomalies in financial transactions and network traffic.

Critical limitations are also raised: the problem of the "black box" of AI solutions, the risk of algorithmic bias, the vulnerability of training data to "poisoning", and the increasing difficulty of analyzing encrypted communications. The legislative framework (incl. EU Regulation 2024/1689 on AI) is considered as a prerequisite for legitimate and democratically controlled use (European Parliament and Council of the EU, 2024).

The dissertation systematizes four key areas with prospects until 2030 – explainable AI, generative and multimodal AI, federated learning for system security, and consolidated international regulations.

3. Cloud computing, edge and confidential computing

Cloud technologies have been identified as a critical infrastructure foundation for modern security management.

The study analyzed three complementary concepts in synergy:

Cloud computing provides scalable storage and rapid processing of petabytes of intelligence data, facilitates international interoperability between agencies and allies, and enables rapid deployment of AI models.

Edge computing moves critical functions to the „edge“ of the network. They are close to the physical source of data or threat, eliminating delays in processing sensitive information in real time. Key projects by country are reviewed, including applications in security and surveillance.

Confidential calculations, based on Trusted Execution Environments (TEE), allow processing of classified information even in a public cloud environment, without compromising confidentiality. Confidential computing is a key technology for joint operations with partner services.

4. Blockchain – decentralized trust and data immutability

Blockchain has been analyzed as a fundamental change in intelligence management. Four are fundamental features of the technology (Nguyen et al., 2021) – data integrity, operational transparency, decentralized protection, and smart contracts. They are specifically applied to each stage of the security management cycle.

The author places particular emphasis on post-quantum protection of blockchain systems as an urgent strategic priority (索存口分口存口口口, 2024). Blockchain-based official e-files are also considered as a tool for information security, operational efficiency and chain of evidence protection (Singh and al., 2020).

The paper presents a comparative analysis that shows that while active implementation is being observed worldwide, **Bulgaria is in an initial, primarily research stage** without evidence of operational implementation in intelligence structures.

5. Drones , Additive technologies and Nanotechnologies

The study systematizes drones as a tool with a dual function: intelligence (surveillance, IMINT, mapping) and counterintelligence (detection and neutralization of hostile UAV). The legal and operational challenges are analyzed, including the risk of their use by criminal organizations.

Additive technologies (3D, 4D, 5D printing) are transforming the management cycle through rapid prototyping and decentralized on-demand manufacturing of critical

assets. At the same time, their proliferation creates a serious counterintelligence threat, such as the production of illegal weapons and skimming devices.

Nanotechnology is analyzed as a strategic cooperative technology of intelligence operations capabilities – from hypersensitive sensor networks and nanoarmor to disappearing electronics and quantum cryptography with nanocrystals. The dissertation finds that countries without systemic integration of nanotechnology risk not just technological, but structural intelligence lag.

6. Geotechnologies, VR/AR and Space Technologies

Geotechnologies . These are GIS, satellite intelligence, GNSS and UAV with geospatial analysis. They have been established as a key and indispensable resource for intelligence services. National legislation and control mechanisms have been analyzed.

Virtual (VR) and augmented reality (AR) are revolutionizing employee training, field operations, and situational awareness (Booz Allen Hamilton, 2021): VR for simulated training in a safe environment and AR for providing contextual information in a real operational space (DHS, 2024).

Space technologies are identified as the backbone of modern intelligence because they provide unparalleled capabilities for global and continuous surveillance. Specific applications are analyzed across all seven phases of the management cycle – from satellite IMINT and signals intelligence (SIGINT) to navigation and secure communications.

7. Synergy and system integration of technologies

The dissertation presents and analyzes three synergistic concepts:

Digital twins (Digital Twins) allow for attack simulation, pre-testing of defenses, and predictive analysis of complex systems without risk to real infrastructures. They are expected to become a standard tool for national security in developed countries by 2030 (Gartner, 2024).

Soft robotics offers flexible robotic systems for monitoring and protecting infrastructure in difficult-to-reach environments.

The concept of „Zero Trust“ has been analyzed and defined by the author as a modern standard for cybersecurity. It is based on the principle „Trust no one, verify everything“ (NIST, 2020) (Gartner, 2023). The concept has been applied to the intelligence and counterintelligence environment and analysis shows that when successfully implemented, it reduces the risk of insider attacks by 63%.

8. Data security

The final section of Chapter Two of the study systematizes the entire data life cycle – from its generation to destruction, structuring protection around three key features: confidentiality, integrity and availability. Methods for classification, encryption (symmetric and asymmetric), masking, archiving (3-2-1 strategy) and data loss prevention (DLP) technologies are examined. GDPR principles (European Parliament and Council of the EU, 2016) are presented as a regulatory framework for the responsible processing of personal data by security services.

Head conclusions

The summarized analysis of Chapter II proves that security is entering a stage of complete technological transformation, in which all processes are reorganized around the integrated implementation of diverse but complementary technologies.

There are three key theoretical findings.

First, AI and Big Data are emerging as the core of the new concept of security, enabling a shift from traditional analytics to predictive (Gartner, 2026) intelligence, automated anomaly detection, and dynamic risk management.

Second, blockchain, confidential computing, and zero-trust architecture (Taylor, 2022) are not only tools for greater efficiency, but also for greater verifiability, traceability, and democratic control over the use of powerful surveillance tools, balancing intelligence methods with civil rights.

Third, technological modernization of security cannot be considered in isolation from the legal, ethical, and organizational environment. The risks of mass surveillance, algorithmic bias, and automated decision-making require robust regulatory frameworks, clearly assigned responsibilities, and independent institutional oversight.

The author places a particularly important emphasis on Bulgaria's structural backwardness: it is detrimental and is exacerbated by a chronic lack of funding, qualified personnel, an outdated regulatory framework, and a dominant orientation towards minimizing risks instead of preventive activities and technological advancement.

Chapter III: Digital Security Management

Chapter III is the synthesizing and applied culmination of the dissertation. It contains ten sections, each of which tracks specific technology, namely Big Data, Artificial Intelligence, Cloud Computing, Blockchain, Drones, Additive Manufacturing, Nanotechnology, Geotechnology, Virtual and Augmented Reality, and Space

Technologies, analyzing its specific impact on each of the seven management stages in the intelligence and counterintelligence cycle.

Conceptual frame of the head

The author formulates the starting thesis in the following way: **modern technological transformations are profoundly changing all stages of the security management cycle** – from analysis and planning, through decision-making, to implementation and control. New technologies do not only upgrade individual processes, but **also impose a qualitative systemic change** , in which digitalization, AI, Big Data, cloud services and cybersecurity transform the traditional sequence of management activities into a dynamic, automated system oriented to real-time data.

As an analytical framework, the author introduces **a matrix model** , structured along two axes - **seven management stages** (information gathering; forecasting; decision making; planning; organizing; execution; control) and **three levels** of management (strategic, tactical, operational).

Table 2 Template for creating a framework for the impact of new technologies on the stages of the management cycle and levels of security management

Stages of a management cycle / **Levels of management**	***Information collection and analysis***	***Preparation of forecasts, estimates and solution options***	***Decision making and scenario building***	***Planning***	***Organizing***	***Execution***	***Control and verification of implementation with the planned goal***
Strategic management							
Tactical management							

Operational management							

Each technology considered is mapped to this matrix separately for intelligence and counterintelligence.

Main theses and scientific results by section

1. Big data - transition from reactive analysis to proactive management

The application of Big Data fundamentally transforms traditional, reactive processes into a proactive and highly automated management cycle. At the information collection and analysis stage, integrated platforms allow for the simultaneous processing of heterogeneous, massive data streams, from SIGINT, OSINT, biometrics, and financial transactions, significantly accelerating situational awareness (ODNI, 2022).

At the forecasting stage, the tools generate dynamic assessments and predictive scenarios in real time, replacing intuitive and statistical predictions with machine learning. In decision-making, the author identifies a shift from collegial, experience-based choices to **data-driven decisions supported by analytical frameworks and impact assessment tools** (classification matrices, situation tables, sample structures for cross-functional teams).

At the implementation and control stages, automated monitoring and results tracking systems provide a closer connection between planned goals and actual performance.

2. Artificial Intelligence – digitalization of the management cycle in intelligence and counterintelligence

This part is based on a detailed comparative matrix of three parallel management models: traditional (analog), digitalized without AI, and digitalized with AI. It systematizes the contributions and risks of artificial intelligence at each of the seven management stages.

Table 3the security management cycle

Cycle element	*Traditional (analog) approach*	*A digitalized approach without AI*	*Digitalized approach*	*Key benefits of AI*	*Key risks/limitations*

			with AI (state/trend)		
Collection and analysis	Manual collection, paper media, human analysis	Electronic databases, manual analysis by specialists	Automated OSINT/SIGINT, biometrics, clustering and anomaly detection	Speed, range, detection of hidden dependencies	Data dependency, "black box", vulnerability to manipulation
Forecasting	Intuitive assessments, expert advice	Statistical forecasts	Predictive investigation, cyberattack prediction, simulations	Proactivity, optimization of resources	Algorithmic bias, overconfidence in models
Decision making	Collegial/individual expert selection	Supported by electronic information systems	Solutions powered by explainable AI and predictive models	Better awareness, multi-factor analysis	Transferring responsibility to the “machine”
Planning and organizing	Text plans, hierarchical arrangements	Planning software, electronic workflows	Intelligent optimization systems, adaptive resource reallocation	Flexibility, synchronization between services	Complexity of integration with legacy systems
Implementation	Tactical teams, radio communication, manual reports	Digital communications, GPS, basic sensors	Autonomous systems, drones , smart sensors,	Real-time response, reduced human risk	Technical failures, compromise of AI systems

			cyber defense through AI		
Control	Post factum reports, inspections	Job boards, KPIs without AI	Continuous monitoring, automatic performanc e and risk analysis	Early detection of deviations, learning from experience	Opacity of the basis for AI "assessmen ts"

In intelligence, AI transforms information gathering through automated OSINT/SIGINT and anomaly detection; forecasting through predictive analytics and cyberattack simulations; and decision-making through explainable AI recommendation systems. In the implementation phase, autonomous agents automatically trigger defenses upon detecting an attack.

In counterintelligence, AI is applied to internal threat analysis, profiling of high-risk individuals and units, biometric access control, automated detection of disinformation campaigns, and dynamic "risk profiles" of personnel. Significant emphasis is placed on the challenges: algorithmic bias in profiling, the danger of "legitimizing" erroneous models, and the opacity of AI solutions in counterintelligence surveillance.

The outlook until 2030 outlines four strategic directions: explainable AI, federated learning, multimodal generative AI, and consolidated international regulations.

3. Cloud computing – scalability and management continuity

Cloud technologies are analyzed as the infrastructure backbone of the modern security management cycle. At the information collection and processing stage, cloud platforms enable scalable processing of petabyte arrays (Rashid and Chaturvedi, 2019), integrating multiple disparate intelligence sources. At the predictive stage, they provide computational resources for AI models and real-time simulations.

At the planning and organizing stages, cloud solutions provide centralized control and real-time information sharing, complemented by blockchain to ensure transparency. Of particular importance is the section on control, audit and continuous monitoring, where

cloud environments allow for automated audit trails, continuous monitoring and rapid incident response.

4. Blockchain – decentralized trust in the governance cycle

The author analyzes the application of blockchain as an infrastructure for ensuring integrity, traceability, and automation of processes in intelligence and counterintelligence (中国信息通通研究院, 2020). At the prognostic stage and decision-making, immutable historical records provide access to more reliable data for scenario modeling, and smart contracts automatically signal when certain combinations of risk indicators occur.

A critical emphasis is placed on ethical and legal dilemmas: mass profiling and the construction of dynamic „risk profiles“ via blockchain requires strict segmentation of access, cryptographic protections, and clear legal frameworks to prevent abuse of fundamental rights.

5. Drones, Additive manufacturing and Nanotechnology

Drones are systematized in both directions.

In intelligence, they provide continuous surveillance, IMINT, and real-time implementation coordination, while in counterintelligence they are applied to detect and neutralize hostile UAVs, secure perimeters, and protect critical infrastructure.

Additive technologies are transforming the management cycle through rapid prototyping and decentralized manufacturing, with digital twins and production management systems enabling defect prediction, resource optimization, and workflow automation. Specialized security frameworks based on side-channel monitoring have been introduced in counterintelligence to detect sabotage and intellectual property theft.

Nanotechnology in the governance cycle is presented from the perspective of investment decisions in security technologies, such as cryptography, sensor networks, nano-protective materials, and quantum-secure communication channels. The author strongly emphasizes that these decisions have not only a technical, but also a political and ethical-legal dimension.

6. Geotechnologies – the spatial dimension of the management cycle

Geotechnologies are presented through two detailed matrices, mapping their applications at each management stage in intelligence and counterintelligence. In intelligence, they ensure the organization of decision-making through precise positioning and mapping of the operational space. In counterintelligence, geotechnologies are applied to detect traffic anomalies, protect borders, and monitor critical infrastructure.

7. Virtual and augmented reality – modern digital training and operational context

VR/AR technologies have been identified as a factor for measurable improvement in operational readiness from 15% to 50%. They transform the management cycle through the systematic integration of virtual technologies: VR for training, simulation of crisis scenarios and preliminary assessment of decisions; AR for providing contextual information and data in a real operational space, increasing the situational awareness of performers.

8. Space technologies - an evolving intelligence architecture

Space technologies are conceptualized as fully and systematically integrated into all seven phases of the management cycle, from satellite-based IMINT and SIGINT for information collection, to precision navigation, secure communications, and space-based control over performance. The author builds an analytical model demonstrating how their comprehensive integration has transformed security management from a set of discrete functions into a dynamic, information-centric process that enables proactive shaping of the security environment.

Head conclusions

The summarized analysis of Chapter III confirms three main theoretical findings.

First, the innovation in the proposed conceptual framework lies not in the management cycle model itself, but in its fundamental technological transformation. The traditional sequence of management activities is transformed into a dynamic, data-driven system, in which the transition from reactive to proactive and predictive security management is not a prospect, but an operational reality for the world's leading services.

Second, the proposed model simultaneously covers the three management levels, strategic, tactical and operational, achieving a closer connection between strategic goals and real operational actions. Technologies such as blockchain and advanced data management systems provide a more reliable and secure environment for auditing and evaluating management decisions.

Third, technological superiority and the ability to systematically integrate it throughout the entire management cycle are emerging as a key and determining factor for national security. States and intelligence structures that have managed to turn these technological trends into part of their management model will have a clear informational and operational advantage. Conversely, lagging behind in this integration becomes a strategic vulnerability, putting the overall stability in the security sphere at risk.

The final and fundamental conclusion is that modern security management requires the parallel development of a legal, ethical and organizational framework that guarantees a balance between efficiency and the protection of the rights and freedoms of society. Without such a balance, the concentration of critical data and the dependence on complex algorithms give rise to specific new vulnerabilities, potentially more dangerous than those against which the security system itself is aimed.

Conclusion

Main thesis and summary of the contribution

The conclusion of PhD Teodora Licheva's dissertation „Transformation of the management cycle in intelligence and counterintelligence through integration of modern technological solutions“ is a synthesis of research achievements that formulates strategic guidelines and outlines future security challenges in the digital era.

The main thesis, which is also confirmed in the conclusion, is categorical: **security management can no longer be based on analog, traditional and mostly reactive models.** It requires a complete transformation of the management cycle, which is based on data, automation and predictive technologies, while respecting the rule of law, democratic control and ethical standards. Security is conceptualized not only as an institutional function, but as an integrated system of technologies, people, rules and values, in which technological modernization and management culture are mutually dependent and inextricably linked.

Key findings from the study

The conclusion summarizes three interrelated findings that run like a common thread throughout the dissertation.

First , the traditional security management cycle is no longer functionally viable in the digital age. The reactive, slow and bureaucratic management model is being replaced by a dynamic, data-driven system, in which each of the seven management stages from information collection and analysis, forecasting, decision-making, planning, organizing to execution and control, undergoes a qualitative transformation. Artificial intelligence, Big Data, cloud computing, blockchain, drones , nanotechnologies, geotechnologies and space technologies are not just tools for efficiency – they are architectural elements of a new management model characterized by proactivity , predictability and automation.

Secondly, technological superiority and the ability to systematically integrate it throughout the management cycle is emerging as a key and determining factor for national security in the 21st century. Intelligence structures that manage to turn technological innovations into an organic part of their management model gain a measurable informational and operational advantage. Conversely, lagging behind in this integration becomes a strategic vulnerability, putting the overall stability and reliability of the security sphere at risk.

Third, technological transformation is sustainable only if the legal, ethical and organizational frameworks evolve in parallel. The concentration of vast amounts of sensitive data, the reliance on complex algorithms and automated decision-making give rise to new, specific vulnerabilities, from cyber threats and algorithmic bias to the erosion of civil rights and the right to privacy. Without a clear balance between efficiency and the protection of public rights, the security system itself can become a threat.

Conclusions for Bulgaria

The conclusion pays considerable attention to the specific Bulgarian context, noting a structural lag that risks deepening. Despite the positive institutional and regulatory reforms after 1989 and the establishment of the National Security Agency and the Bulgarian Defense Agency, the adoption of specialized legislation and the introduction of democratic control mechanisms, the security system remains faced with a complex of challenges.

These include: limited resource and technological capacity; fragmented information infrastructure; insufficient integration of modern technologies at the operational level; chronic shortage of highly qualified personnel with digital competencies; and delayed introduction of innovative management models.

The author emphasizes **that Bulgaria's lagging behind is not only technological, but also conceptual,** because the orientation toward minimizing risks and responding to threats that have already occurred dominates, instead of toward preventive, predictive, and technologically advanced activities.

Proposed conceptual model

Based on the research, the dissertation proposes a conceptual model for digital security management, integrating the three management levels – strategic, tactical and operational – into a single, technology-driven system. The model envisages specific strategic measures, united in the following areas:

- Building modern digital platforms and predictive analysis systems for all phases of the management cycle;
- Introducing digital twins of critical infrastructure for risk-free simulation and threat assessment;
- Implementing a „zero trust“ architecture as a cybersecurity standard in intelligence and counterintelligence structures;
- Development and implementation of post-quantum cryptographic solutions as a response to the growing threat of quantum computing.

All of this must be accompanied by a unified regulatory and strategic framework, better coordination between institutions, standardization of processes, and ensuring a balance between national security and civil rights and freedoms.

The role of the human factor

The conclusion also gives special importance to the human factor, conceptualized as an indispensable constant in the process of technological transformation. The main finding is that technological innovations can be sustainably effective only if they are accompanied by the development of the competencies, organizational culture and values of employees in the security system. Managers must evolve from administrators of routine processes to strategic digital leaders, capable of making informed, data-based decisions in conditions of constant uncertainty and technological turbulence.

The dissertation concludes with a fundamental strategic message: ***the technological transformation of security management is not only a necessity, but also a strategic advantage*** , provided that it is driven by a clear vision, adequately resourced, legally regulated and oriented towards sustainability. Only under these conditions will it become a lasting competitive advantage for national security, and not a new and more complex source of instability and vulnerabilities.

IV. Publications on the topic of the dissertation

1. Licheva, T. „Technologies between Industry 4.0 and 5.0“, V. Collection of papers of the 9th International Scientific Conference „Industry 4.0“ - June 26 - 29, 2024, pp. 65-67, ISSN 2535-0161

2. Licheva, T. „Data Security“, V. Sb. XII International Scientific Conference „Technology. Technologies. Education. Security“ - 2 - 5 Sep. 2024, pp. 54-56, ISSN 2535-0323

3. Licheva, T. „Rules and elements of data security“, In the journal Security and Defense, 2024, year III, issue 2, pp. 188-200, ISSN 2815-388X

4. Licheva, T. „Artificial Intelligence and data security“, V. Sb. Doc. of the 8th International Scientific Conference on Security „CONFSEC 2024“ 9-12 Dec. 2024, pp. 69-71, ISSN2603-2953

5. Licheva, T. „Blockchain in Intelligence“, in Collection of papers of the scientific-theoretical conference „Bulgarian Intelligence and Counterintelligence - Challenges, Problems, Prospects“ - April 11, 2025, pp. 167-172, ISBN (pdf) 978-619-7774-26-9

6. Radulov, N., **Licheva, T. „**Digital twins in security”, In Collection of Papers of the 10th International Scientific Conference “INDUSTRY 4.0” June 25-28, 2025, pp. 104-108, ISSN 2535-01-61

7. Radulov, N., **Licheva, T.,** “Security Ecosystem 5.0”, In Collection of Papers of the 10th International Scientific Conference “INDUSTRY 4.0” June 25-28, 2025, pp. 109-111, ISSN 2535-01-61

8. Licheva, T. “Security of e-files with blockchain”, In the journal “Security and Defense, 2025, year IV, issue 1, pp. 114-128, https://doi.org/10.70265/NKYH9976 , ISSN 2815-388X

9. Licheva, T. „Technologies in the management cycle - modern and traditional method“, V. Sb. XIII International Scientific Conference „Technology. Technologies. Education. Security“ - 1 - 4 Sept. 2025, pp. 41-43, ISSN 2535-0323

10. Radulov, N, **Licheva, T**., “Interaction of blockchain with high technologies in the Security 5.0 ecosystem”. V. Sb. XIII International Scientific Conference “Technology. Technologies. Education. Security” – 1 – 4 Sept. 2025, pp. 111-113, ISSN 2535-0323

11. Radulov, N., **Licheva, T.,**“Smart contract in security”. V. Sb. XIII International Scientific Conference “Technology. Technologies. Education. Security” – 1 – 4 Sept. 2025, pp. 117-120, ISSN 2535-0323

12. Licheva, T. „Virtual and Augmented Reality in Security“. V. Sb. Doc. of the 9th International Scientific Conference on Security „CONFSEC 2025“ 8 – 11 Dec. 2025, pp. 76-78, ISSN 2603-2953

13. Licheva, T. „Soft Robotics in Security“ In the journal Security and Defense, 2025, year IV, issue 2: 191-208. https://doi.org/10.70265/UKEY2910

14. Licheva, T. Artificial Intelligence in Counterintelligence Management“. V. Sb. Doc. of the International Scientific Conference „Artificial Intelligence“ March 23-26, 2026

15. Licheva, T. Artificial Intelligence in Intelligence Management“, V. Sb. Doc. of the International Scientific Conference „Artificial Intelligence“ March 23-26, 2026