VARNA FREE UNIVERSITY "CHERNORIZETS HRABAR"
FACULTY OF SOCIAL, BUSINESS AND COMPUTER SCIENCES
DEPARTMENT OF COMPUTING AND COMPUTER SCIENCE

RACHELI MENDA SHABAT

THE IMPACT OF REGULATION (EU) 2019/881 (CYBERSECURITY ACT) ON THE EXPANSION OF CYBERSECURITY CERTIFICATIONS

AUTOREFERAT

of a dissertation to award the educational-and-scientific degree PhD,
professional field 4.6 Computing and computer science,
PhD programme “Information Systems and Technologies, Computing and Computer Science”

Scientific supervisors:
Assoc. Prof. Galina Mileva, PhD
Assoc. Prof. Zlatogor Minchev, PhD

Varna, 2026

VARNA FREE UNIVERSITY "CHERNORIZETS HRABAR"
FACULTY OF SOCIAL, BUSINESS AND COMPUTER SCIENCES
DEPARTMENT OF COMPUTING AND COMPUTER SCIENCE

RACHELI MENDA SHABAT

THE IMPACT OF REGULATION (EU) 2019/881 (CYBERSECURITY ACT) ON THE EXPANSION OF CYBERSECURITY CERTIFICATIONS

AUTOREFERAT

of a dissertation to award the educational-and-scientific degree PhD,
professional field 4.6 Computing and computer science,
PhD programme "Information Systems and Technologies, Computing and Computer Science"

Scientific supervisors:
Assoc. Prof. Galina Mileva, PhD
Assoc. Prof. Zlatogor Minchev, PhD

Reviewers:
Prof. Teodora Bakardzhieva, PhD
Prof. Nayden Nenkov, PhD

Varna, 2026

The dissertation is structured into an introduction, three chapters, a conclusion, a bibliography and appendices, and has a total volume of 213 pages. The main text contains 25 tables and 21 figures. The list of references includes a total of 187 sources.
The dissertation has been discussed by the members of the Department of Computer Science and is intended for defense in front of a scientific jury.

The author of the dissertation is a PhD student in an individual form of study at the Department of Computer Science, Faculty of Social, Economic and Computer Sciences, Varna Free University "Chernorizets Hrabar".

The public defense of the dissertation will be held at an open meeting of the scientific jury on 07.07.2026 at 11:00 in the Conference Room of Varna Free University "Chernorizets Hrabar".

The materials for the defense are available in the office of the Department of Computer Science at the Faculty of Social, Economic and Computer Sciences of Varna Free University "Chernorizets Hrabar" and on the Internet: www.vfu.bg, section "PHD".

I. GENERAL DESCRIPTION OF THE DISSERTATION

1. **Introduction**

In today's hyper-connected environment, cybersecurity has evolved from a supplementary concern into a critical necessity. The growing reliance on digital infrastructure has exposed individuals, businesses, and public institutions to increasingly complex security risks - from infrastructure attacks and large-scale data breaches to ransomware and cyber-enabled financial crime.

The EU's Common Criteria (CC) framework (ISO/IEC 15408) long dominated security certification. However, its exclusive reliance on public certification bodies created structural bottlenecks constraining scalability, increasing costs, and delaying market entry, particularly for the rapidly expanding Internet of Things (IoT) sector.

The EU Cybersecurity Act (CSA) 2019/881 marked a pivotal shift by opening certification processes to private Conformity Assessment Bodies (CABs), followed by mandatory obligations under the RED Delegated Act (EU) 2022/30 and the Cyber Resilience Act (CRA) (EU) 2024/2847. This hybrid landscape raises fundamental questions about the role, trustworthiness, and legitimacy of private CABs within the European certification system.

Additionally, the impact of private CABs entering the ecosystem on market adoption trends for security certifications needs to be checked.

2. **Topicality and Relevance of the Research Topic**

The topicality of this dissertation is determined by the urgent need to scale cybersecurity certification for IoT devices in response to the rapid proliferation of connected products, the evolving EU regulatory landscape, and the structural limitations of traditional public-body-led certification. Most IoT devices remain uncertified, largely due to cost, time, and procedural complexity. Yet, increasingly they handle sensitive or critical data.

At the same time, there is a lack of scientifically grounded research addressing the conditions under which private CABs can be reliably integrated into a domain historically governed by public

authorities. This dissertation addresses that gap by providing both a theoretical framework and empirical validation. Filling a critical need for policymakers, manufacturers, and certification authorities.

3. **Object and Subject of the Research**

The object of this dissertation is the European cybersecurity certification framework for IoT devices, with an emphasis on the mechanisms through which CABs, both public and private, assess and validate the security of connected products.

The subject of the study focuses on the influence of three key EU regulatory instruments: the Cybersecurity Act (CSA) 2019/881, the RED Delegated Act 2022/30, and the Cyber Resilience Act 2024/2847. Specifically, the dissertation examines how these regulations shape the adoption and legitimacy of private cybersecurity certification schemes and how they affect trust, quality assurance, harmonization, and market uptake.

4. **Problem Researched**

The problem researched is a six-dimensional discrepancy between the rapidly growing need for scalable and cost-effective cybersecurity certification of IoT devices and the capacity of the current framework to deliver it:

(1) Can private CABs ensure the same quality of evaluation as public schemes?

(2) Does their involvement risk regulatory non-compliance?

(3) How can private and public schemes be harmonized for mutual recognition?

(4) How can private schemes gain legitimacy without undermining government authority?

(5) Can cybersecurity compliance be achieved without degrading IoT product performance or market adoption?

(6) Which criteria and methodological approaches should guide CAB selection to ensure certification success?

5. Author's Argument

The core argument defended is twofold:

First, that recognizing private CABs as legitimate entities within the EU's cybersecurity certification framework, governed through accreditation standards, transparency mechanisms, and the CSA/RED/CRA regulatory architecture can significantly enhance the scalability and effectiveness of IoT security certification without compromising quality or harmonization.

Second, that IoT products certified under recognized cybersecurity schemes exhibit measurably higher levels of implemented security features compared to equivalent non-certified products, without incurring significant performance penalties.

These arguments are operationalized through two novel models: the Private Scheme Forecasting (PSF) model, providing macro-level systemic foresight on certification adoption, and the Private Scheme Selection (PSS) model, offering a structured micro-level decision-making tool for CAB selection.

6. Objective and Tasks of the Dissertation

The main goal of this dissertation is to develop scientifically grounded, harmonized models that facilitate the prediction of successful integration of private certification schemes within the broader certification ecosystem, and to formalize these models into a robust decision-making framework for CAB selection.

To achieve this goal, the following six tasks were formulated:

Task 1: Evaluate quality and effectiveness.
Task 2: Analyze regulatory impact.
Task 3: Develop harmonization strategies.
Task 4: Investigate trust mechanisms.
Task 5: Assess market adoption and scalability.
Task 6: Formulate a CAB decision-making model.

7. Research Methodology

This dissertation employs a multidisciplinary methodology combining regulatory analysis, comparative studies, case studies, and quantitative modelling across two integrated approaches:

Theoretical and Analytical: In-depth legislative review; comparative analysis of certification frameworks; and case studies from sectors where private schemes supplement public oversight.

Empirical and Modelling: A Private Scheme Forecasting (PSF) model using Multi-Phase Scenario-Based Modeling - incorporating morphological analysis, Cross-Consistency Matrix, Prognostic Analytical Modeling, and sensitivity analysis to assess macro-level adoption dynamics; and a Private Scheme Selection (PSS) model based on the Fuzzy Prioritization Method (FPM) for structured CAB decision-making. Both models are validated through empirical evaluation.

8. Limitations of the Problematic Scope of the Ph.D. Work

The limitations of this research include: reliance on publicly available technical documentation for the empirical product comparison; restriction of the experimental validation to three representative IoT product categories; the exclusion of proprietary cost data for certification procedures; and focus primarily on the EU regulatory context. The rapidly evolving nature of cybersecurity threats and regulations also means that some findings may require updating as new legislative instruments mature, particularly the CRA which was still at an early implementation stage at the time of writing.

II. SIZE AND STRUCTURE OF THE DISSERTATION

The dissertation is structured into an introduction, three chapters, a conclusion, a bibliography, and appendices, totalling 213 pages. The main text contains 25 tables and 21 figures. The list of references consists of 187 sources, including international, and internet sources. In addition, there are 2 appendices (an acronym list and cybersecurity standards classification tables):

CONTENTS

III. DISSERTATION SUMMARY

INTRODUCTION

The Introduction justifies the topicality and relevance of the research problem by tracing the evolution of cybersecurity from a niche technical concern reserved for defense and governmental systems into a critical societal necessity affecting every dimension of modern economic, political, and social life. The growing reliance on digital infrastructure has fundamentally transformed the threat landscape: digital attacks such as large-scale data breaches, ransomware incidents, infrastructure sabotage, industrial espionage, and cyber-enabled financial crime have become more frequent, more sophisticated, and more consequential across sectors ranging from banking and healthcare to energy and public administration.

Central to this transformation is the unprecedented proliferation of Internet of Things (IoT) devices. The global IoT sector is projected to achieve a Compound Annual Growth Rate (CAGR) exceeding 25% between 2020 and 2025, generating billions of interconnected devices that process and exchange vast volumes of sensitive data. Yet a significant proportion of these devices enter the market without robust security features, and most remain uncertified - largely because the dominant certification framework, the Common Criteria (ISO/IEC 15408), was designed for governmental and defense contexts and relies exclusively on public certification bodies even at low assurance levels.

This structural mismatch between the scale of the IoT ecosystem and the capacity of the certification apparatus forms the core tension that motivates this research.

The Introduction defines the object and subject of the dissertation: the European cybersecurity certification framework for IoT devices, and specifically the influence of three landmark EU regulatory instruments - the Cybersecurity Act (CSA) 2019/881, the RED Delegated Act 2022/30, and the Cyber Resilience Act (CRA) 2024/2847 - on the adoption and legitimacy of private Conformity Assessment Bodies (CABs).

It formulates the research problem as a six-dimensional challenge: quality assurance, regulatory compliance, harmonization, legitimacy and trust, market adoption and scalability, and structured CAB selection decision-making.

It presents the dual research argument - that private CABs can deliver quality-neutral or quality-superior certification compared to public schemes, and that certified IoT products exhibit measurably higher levels of implemented security features without incurring performance penalties.

The Introduction specifies the six research tasks aligned with these dimensions, describes the multidisciplinary methodology combining legislative analysis, comparative case studies, mathematical forecasting, and empirical product evaluation, and outlines the dissertation's three-chapter structure culminating in two original models - the Private Scheme Forecasting (PSF) model at the macro level and the Private Scheme Selection (PSS) model at the micro level - as the dissertation's primary scientific contributions.

FIRST CHAPTER: CYBERSECURITY CERTIFICATIONS - EXAMINING THE REGULATORY LANDSCAPE, STANDARDS, AND CABS THROUGH THE CHALLENGES OF PRIVATE SCHEME ADOPTION AND THE LENS OF LEGITIMACY THEORY

The First Chapter establishes the regulatory, theoretical, and institutional foundation of the entire dissertation through a comprehensive and systematic analysis of the cybersecurity certification landscape.

It begins by tracing the historical roots of cybersecurity certification: from the U.S. Department of Defense's Trusted Computer System Evaluation Criteria (TCSEC, the "Orange Book," 1983), through Europe's ITSEC and Canada's CTCPEC, to their unification into the globally recognized Common Criteria (CC, ISO/IEC 15408) framework in 1999. Initially tailored for governmental, defense, and financial systems, certification schemes later expanded to telecommunications, identity management, and payment infrastructures.

Industry-driven standards such as ISO/IEC 27001 for information security management and FIPS 140-2 for cryptographic modules also gained prominence, reinforcing certification's role in trust-building and regulatory compliance.

By the 2010s, cybersecurity certification had become a key instrument in sectors handling sensitive data or operating critical

infrastructure, yet its accessibility remained limited due to complexity, cost, and the structural constraint of public-sector exclusivity.

A comprehensive classification and analysis of cybersecurity standards was conducted across four key dimensions.

First, type of coverage - distinguishing between environmental standards (securing the development, testing, and manufacturing environment, such as ISO/IEC 27001) and functional standards (securing the security capabilities embedded within the product itself, such as Common Criteria and FIPS 140-3) - recognizing that these two domains are deeply interdependent: a product's functional security features can be rendered ineffective if the development environment is compromised.

Second, governance level - differentiating international standards developed by globally recognized bodies such as ISO/IEC, regional standards such as those developed within the EU framework, and national standards tailored to country-specific infrastructure, threat landscapes, and regulatory priorities.

Third, applicability - distinguishing horizontal standards designed for universal cross-industry application using risk assessment-based approaches (such as ISO/IEC 27001 and ISO/IEC 15408) from vertical standards tailored to specific market segments such as automotive (ISO/SAE 21434, UNECE R155), industrial control systems (IEC 62443), and IoT (ETSI EN 303 645, SESIP).

Fourth, evaluation methodology - categorizing standards by whether they require self-declaration, a formal Declaration of Conformity (DoC), or independent third-party evaluation.

Twenty standards were analyzed and classified using this framework, including ISO/IEC 27001, ISO/IEC 15408 (Common Criteria), ISO/IEC 19790, FIPS 140-3, IEC 62443, EN 18031, ETSI EN 303 645, SESIP (EN 17927:2023), ISO/SAE 21434, UNECE R155, PSA Certified, and national schemes from Japan (JC-STAR), Singapore (CLS IoT), the United States (NIST IR 8259, NIST IR 8425A), Germany (BSI TR-03109-1), Spain (LINCE), China (GB/T 18336.1), and Taiwan (SSIPS). This classification revealed significant diversity in evaluation methodologies and governance approaches, and importantly confirmed significant gaps in IoT-specific certification pathways at the international level - a finding that directly motivated the dissertation's focus on private CABs as a scalability solution.

Essential factors driving the certification challenge for IoT devices were systematically outlined. The Common Criteria framework's reliance on public Certification Bodies (CBs) even for low-assurance EAL1 evaluations created structural bottlenecks that constrained scalability, increased cost, and delayed market entry for fast-moving consumer IoT products. The ENISA 2019 gap analysis confirmed the absence of adequate IoT-specific standards. At the same time, the IoT sector's complexity - spanning hardware components, infrastructure devices, and consumer electronics - demands evaluation expertise that public bodies, operating under governmental structures and resource constraints, often cannot provide at the pace and granularity the market requires.

The EU's regulatory response across three complementary legislative instruments was examined as an opportunity for scaling cybersecurity certification. The Cybersecurity Act (CSA) 2019/881 introduced a structured pan-European framework establishing three voluntary assurance levels - basic, substantial, and high - and, crucially, opened certification processes to private CABs for the first time, thereby enabling broader market participation and more flexible certification ecosystems.

The RED Delegated Act (EU) 2022/30 established mandatory cybersecurity requirements for specific classes of radio equipment, primarily through manufacturer self-declaration of conformity under harmonized standards such as EN 18031, creating a compliance obligation without requiring third-party evaluation for most products.

The Cyber Resilience Act (CRA) (EU) 2024/2847 extended the scope of mandatory cybersecurity compliance to a much broader range of digital products with network connectivity, requiring third-party evaluation for high-risk categories and significantly expanding the operational role of CABs within the certification ecosystem. Together, these three acts create a layered regulatory architecture that moves from voluntary (CSA) to mandatory self-declaration (RED) to mandatory third-party evaluation (CRA), producing a hybrid landscape that places increasing structural demand on private CAB capacity.

The theoretical context of public versus private regulatory schemes was analyzed through the lens of Legitimacy Theory, examining how organizations and regulatory actors derive social acceptance and

authority. Three dimensions of legitimacy were particularly relevant: pragmatic legitimacy (derived from the practical benefits private CABs deliver to manufacturers and markets), moral legitimacy (derived from adherence to recognized standards of conduct and impartiality), and cognitive legitimacy (derived from taken-for-grantees within the sector over time).

Considerations in accrediting private CABs for cybersecurity were analyzed in depth, highlighting the unique challenge that cybersecurity CABs face compared to those in other regulated domains: they handle cryptographic algorithms and security methodologies that may be classified as national security assets, subject to export control regulations such as the U.S. EAR and EU Regulation No. 428/2009. This creates a fundamental tension between the need for private sector agility and the governmental imperative to protect sensitive security knowledge.

Case studies from analogous regulated sectors were examined to draw parallels and extract best practices: the food safety sector, where private accredited bodies conduct product inspections and audits under regulatory oversight with demonstrably high compliance outcomes; the fire safety and environmental compliance sectors, where private testing laboratories operate within mandatory accreditation frameworks; and the financial services sector, where private auditing firms conduct assessments of systemic importance.

Across all these cases, the pattern that emerged was consistent: properly governed private actors, operating under mandatory accreditation and subject to market accountability, can uphold and in many cases exceed the regulatory outcomes achieved by purely public mechanisms.

A systematic analysis of the advantages (sector-specific expertise, operational agility, faster evaluation cycles, market responsiveness, ability to attract specialized talent) and disadvantages (risk of commercial pressure on standards, limited transparency without oversight, potential for conflicts of interest, reduced governmental control over cryptographic security knowledge) of private certification schemes was presented. The need for specialized requirements for cybersecurity CABs, going beyond general ISO/IEC 17065 accreditation to address impartiality in cryptographic contexts, personnel security clearances, and information security management within the CAB itself, was established.

FIRST CHAPTER FINDINGS

Based on the analysis conducted, the regulatory framework for EU cybersecurity certification is evolving from a purely public, centralized model toward a hybrid public-private ecosystem, driven by the convergence of market demand, regulatory modernization, and technological evolution.

The classification of 20 cybersecurity standards across four dimensions confirmed the significant diversity of evaluation methodologies and governance approaches currently in use globally, and highlighted material gaps in IoT-specific certification pathways at the international level.

It was shown that the convergence of the CSA, RED Delegated Act, and CRA creates both opportunities and structural tensions for private CAB integration: the CSA opens the door, the RED creates mandatory compliance demand that strains public body capacity, and the CRA amplifies that demand further by requiring third-party evaluation for high-risk categories.

The central challenges - trust, legitimacy, quality assurance, regulatory harmonization, market scalability, and structured CAB selection - were identified, theoretically grounded, and framed as the six research tasks addressed in the subsequent chapters.

The cross-sector case study analysis established the foundational evidence base that private regulatory actors, when properly governed, can achieve regulatory outcomes comparable or superior to their public counterparts - providing the theoretical warrant for the dissertation's core argument.

SECOND CHAPTER: PRIVATE SCHEME MICRO-MACRO ADOPTION SUCCESS MODEL - OPTIONAL MODELS EVALUATION AND MODEL DEVELOPMENT

The Second Chapter develops the theoretical and methodological framework for the dissertation's two original models, proceeding through three stages: evaluation of candidate modeling approaches, selection and justification of the most suitable approaches, and the formal development of the PSF and PSS models.

The chapter opens by establishing why mathematical modeling is essential to this research. The decision to integrate private schemes into cybersecurity certification involves a wide range of variables - institutional credibility, standardization capabilities, market dynamics, technical responsiveness, regulatory alignment - that interact in complex, non-linear, and evolving ways.

An overly narrow model would produce flawed conclusions; an insufficiently rigorous one would fail to capture the systemic interdependencies that determine real-world certification outcomes. The selection of appropriate modeling frameworks is therefore a foundational methodological decision.

` Three candidate modeling approaches were evaluated in depth:

1. The House of Quality (HoQ) - rooted in Quality Function Deployment (QFD), provides a structured matrix-based methodology that translates customer or stakeholder needs into technical design requirements. While intuitive and well-established in product development contexts, its static structure and limited capacity to accommodate probabilistic uncertainty or non-linear interdependencies make it insufficiently flexible for the dynamic and evolving threat landscape of cybersecurity certification.
2. The Fuzzy Analytic Hierarchy Process (Fuzzy AHP) - combines the hierarchical structuring and criteria prioritization of classical AHP with fuzzy set theory, allowing decision-makers to express judgments using linguistic variables (e.g., "moderately more important," "strongly more important") mapped onto triangular fuzzy numbers rather than requiring precise crisp values. This approach enhances reliability in group decision-making under uncertainty and enables the prioritization of intangible or qualitative criteria - making it particularly well-suited to the multi-criteria CAB selection problem. However, its computational complexity and potential for subjective bias in defining fuzzy scales make it less appropriate as a macro-level forecasting tool.

3. Multi-Phase Scenario-Based Modeling - integrating morphological analysis, cross-consistency matrix evaluation, prognostic analytical modeling, and 3D sensitivity analysis, was selected as the primary macro-level tool for its superior capacity to handle complex, multi-dimensional, and evolving risk environments. A systematic comparison across criteria of flexibility, uncertainty handling, multi-dimensionality, computational tractability, and applicability to cybersecurity certification was conducted and presented, confirming the selection rationale.

The Private Scheme Forecasting (PSF) model was developed as a macro-level framework using Multi-Phase Scenario-Based Modeling to forecast the systemic success of private cybersecurity certification adoption across the IoT ecosystem. The PSF was structured around four analytical phases:

In Phase 1, the problem space was defined by identifying ten key dimensions and factors influencing certification outcomes, extending beyond conventional technical metrics to encompass human-centric considerations, economic and market pressures, cross-sector interdependencies, and global standards alignment - including Security Measures, Secure Storage, Keys Securing, System Protection, Smart Grids, IoT, Communications Protection, User Data Protection, Human Factor, and Cyber Resilience.

In Phase 2, Morphological Analysis created a structured morphological matrix mapping relationships between security assurance levels, technological domains, assessment methods, and implementation types using fuzzy logic principles, enabling systematic generation of plausible certification scenarios and cross-consistency evaluation of their internal coherence.

In Phase 3, Prognostic Analytical Modeling built on the morphological analysis by introducing predictive techniques - probabilistic simulation and fuzzy logic - to assess long-term certification success probabilities under different scenario configurations, using directed graph representations and Dirichlet distribution to model evolving risk profiles.

In Phase 4, 3D Sensitivity Analysis employed three-dimensional modeling to ascertain scenario sensitivity and identify potential hidden threats that could undermine certification schemes - including supply chain vulnerabilities, AI-driven attacks, and quantum computing risks.

The Private Scheme Selection (PSS) model was developed as a micro-level structured decision tool to address the sixth research task: defining the criteria and methodological approach that should guide the decision to engage a private CAB. The model is built on the Fuzzy Prioritization Method (FPM), which addresses the gaps inherent in purely crisp AHP approaches by incorporating expert uncertainty through linguistic judgment mapping.

Five selection criteria were defined on the basis of the dissertation's theoretical analysis:

- Legitimacy - the CAB's recognition, accreditation scope, and demonstrated impartiality across regions and assurance levels.
- Quality - the clarity, consistency, and credibility of issued certification reports.
- Effectiveness - operational capacity, expert depth, evaluation duration, and innovative assessment processes.
- Enforcement - scope of accreditations held and coverage across regulatory segments.
- Trust - stakeholder confidence as evidenced by volume and diversity of certifications issued and security levels assessed.

Pairwise comparisons across these five criteria were established based on theoretical analysis and field experience, translated into triangular fuzzy numbers (TFNs) using the mapping Saaty(k) → (k−1, k, k+1), geometric means were computed per criterion, fuzzy weights were normalized, and defuzzification was performed using the centroid method ($w_i = (L_i + M_i + U_i) / 3$).

The resulting normalized criteria weights - Trust (38%), Enforcement (23%), Legitimacy (16%), Quality (11%), Effectiveness (11%) - reflect the primacy of stakeholder confidence and regulatory authority in CAB selection for cybersecurity contexts, where the sensitivity of cryptographic materials and the national security implications of certification make trust the foundational prerequisite for legitimacy.

A six-step PSS tool was formalized for practical application, enabling any manufacturer or scheme owner to input CAB performance scores on a 1–10 scale, compute weighted totals, normalize to percentages, and derive a ranked selection recommendation.

SECOND CHAPTER FINDINGS

The comparative model evaluation confirmed that Multi-Phase Scenario-Based Modeling offers the most rigorous and flexible analytical basis for forecasting complex, multi-dimensional certification adoption dynamics, while Fuzzy AHP provides the most appropriate methodology for structured CAB selection under expert uncertainty.

The PSF model development identified three key conditions for effective private scheme integration: innovative risk-based assessment strategies that go beyond checklist compliance, realistic and internally consistent scenario construction that balances comprehensiveness with plausibility, and systemic integration across technological, regulatory, and methodological dimensions rather than narrow focus on individual certification pathways.

The PSS model formalization demonstrated that fuzzy logic successfully addresses the inherent subjectivity and imprecision of expert judgment in multi-criteria CAB evaluation, producing stable, defensible, and transparent priority weights that can guide both individual certification decisions and broader policy design.

Together, the PSF and PSS models establish a complementary macro-micro system: the PSF provides the forecasting perspective on the overall systemic role and value of private certification schemes, while the PSS delivers the operational methodology to implement those insights through structured, evidence-based CAB selection.

THIRD CHAPTER: PRIVATE SCHEME MICRO-MACRO ADOPTION SUCCESS MODEL - MODEL IMPLEMENTATION AND RESULTS VALIDATION

The Third Chapter implements and empirically validates both models, translating the theoretical and methodological frameworks developed in Chapter Two into concrete analytical results and actionable insights. The chapter proceeds through the full implementation and validation of the PSF model, followed by the implementation and validation of the PSS model, and concludes with an integrated analysis connecting the macro and micro perspectives.

The PSF model implementation proceeded across four analytical phases. In the Morphological Analysis phase, a morphological matrix was constructed mapping ten key certification dimensions against their possible states, generating 324 total scenario combinations.

Cross-consistency analysis using the Cross-Consistency Matrix (CCM) evaluated the internal plausibility of each combination, assigning scenario weights based on the coherence and mutual compatibility of their dimensional states. Only approximately one-fifth of the 324 combinations - roughly 65 scenarios were deemed plausible and internally consistent.

Dominant high-weight scenarios with weights of 210 or above were identified as strategically aligned pathways for certified product deployment, characteristically featuring hardware-centric protection architectures, compliance-based regulatory alignment, nanotechnology integration, and third-party evaluation methodology.

This finding powerfully illustrates the complexity of constructing coherent certification paths across the full spectrum of technical and regulatory domains: the vast majority of theoretical scenario combinations are incompatible in practice, underscoring the need for structured analytical tools like the PSF to identify viable pathways.

The Prognostic Analytical Modeling phase employed directed graphs and probabilistic links to reveal systemic interdependencies among the ten key certification dimensions. The modelling demonstrated that small shifts in human factor considerations or user data protection practices propagate meaningfully across the system, influencing overall security posture in ways that purely technical certification assessments would miss.

The analysis identified strong interdependencies among Secure Storage, Keys Securing, System Protection, and Cyber Resilience - confirming that certification approaches must address dynamic systemic resilience rather than static technical compliance.

The 3D Sensitivity Analysis phase mapped each of the ten dimensions onto a three-dimensional risk space defined by direct risk (X-axis), indirect risk (Y-axis), and arrangeable risk level (Z-axis), classifying components into Critical and Non-Critical zones. Security Measures (0.8, 0.69, 0.86), Keys Securing (0.42, 0.59, 0.71), and System Protection (0.25, 0.22, 0.88) were positioned in or near the critical zone, while Secure Data and Key Securing were identified as hidden threat areas - dimensions where vulnerabilities may not be immediately visible in standard certification assessments but carry significant systemic risk implications.

PSF model validation was conducted through a systematic empirical evaluation of three representative IoT product categories, selected to span hardware components, infrastructure devices, and consumer electronics.

The Flash Memory IC category was represented by the Winbond TrustME W75F Secure Serial Flash Memory, certified at EAL5+ under Common Criteria - a high-assurance product designed for embedded systems requiring data confidentiality and integrity, supporting secure boot, secure firmware update, and hardware-based encryption.

The Infrastructure Device category was represented by the EFR GmbH Secure SGH-S Smart Grid Hub, certified at EAL4+, providing secure and reliable data transfer between energy consumers, grid operators, and service providers.

The Consumer Electronics category was represented by the Dahua Network Camera IPC-HDBW4200E, certified at EAL2+, designed for video surveillance with core security features including encrypted video transmission and user account control.

Each certified product was compared against an equivalent non-certified product in the same functional category, with product identities of non-certified devices withheld to avoid reputational sensitivities.

Six cybersecurity parameters were assessed for each product pair: Data Encryption, Secure Default Passwords, Network Protections / Secure Channel, Tamper Detection, User Account Protection, and System Protection / Initialization.

Assessment was conducted on a relative basis using publicly available technical documentation and security target documentation, with cybersecurity feature scores reflecting the strength and depth of implementation relative to the associated EAL level.

Certified products consistently demonstrated substantially higher implementation levels across all six parameters in all three product categories: The Secure Flash device (W75F) scored between 90% and 100% across all criteria - with Data Encryption and User Account Protection achieving 100%, Network Protections and Tamper Detection at 95%, Secure Default Passwords at 90%, and System Protection / Initialization at 95% - compared to scores consistently at or below 40% for the non-certified Flash counterpart (Data Encryption 5%, Secure Default Passwords 5%, Network Protections 5%, Tamper Detection 20%, User Account Protection 35%, System Initialization 40%). Statistical analysis using a t-test confirmed these differences to be highly statistically significant ($p < 0.001$).

The certified Smart Grid Hub showed gaps of 30 to 75 percentage points over the non-certified version across the six parameters, with statistical significance confirmed at $p < 0.01$.

The IP Camera showed security improvements in five of the six parameters, the exception being Tamper Detection where both certified and non-certified models scored minimally at 5%, reflecting an industry-wide gap in physical intrusion detection for this product class at the evaluated assurance level.

Performance evaluation was conducted using quantitative metrics (read/program time, erase/write cycles, data retention, energy efficiency for Flash Memory; real-time data collection latency, remote control responsiveness, scalability, reliability and redundancy, energy management for Smart Grid Hub; image quality, megapixels, protection class, frame frequency for IP Camera) and qualitative dimensions where direct numerical comparison was not available.

The results confirmed that cybersecurity certification does not universally lead to performance degradation. For the Flash Memory, no statistically significant performance difference was found between certified and non-certified variants ($p > 0.05$), with the certified model showing marginal improvements in energy efficiency in deep power-down mode (40% versus 30%) and equivalent or slightly better endurance

metrics. For the Smart Grid Hub, the certified product performed equal to or better than the non-certified version across all five performance dimensions, with a particularly notable advantage in Reliability and Redundancy (95% versus 60%), and aggregated performance showing a statistically significant advantage for the certified product ($p < 0.05$). For the IP Camera, no statistically significant overall performance difference was found ($p = 0.0943$), with the only notable discrepancy being a megapixel advantage in the non-certified model (80% versus 40%) offset by the certified model's superior security architecture – a finding consistent with market prioritization of image specification over embedded security design in the consumer surveillance segment.

The PSS model implementation proceeded through the six formalized steps. Criteria definition established the five selection dimensions – Legitimacy, Quality, Effectiveness, Enforcement, and Trust – grounded in the theoretical findings of Chapter One.

Pairwise comparisons reflecting field experience and theoretical priorities were established using Saaty's scale, with Trust assigned the highest comparative importance relative to all other criteria, followed by Enforcement.

Fuzzy comparisons translated the crisp Saaty values into triangular fuzzy numbers per the mapping formula, generating a full fuzzy pairwise comparison matrix. Geometric means were computed per criterion, yielding fuzzy geometric mean vectors (L, M, U): Trust (1.516, 2.221, 2.862), Enforcement (0.803, 1.320, 1.933), Legitimacy (0.608, 0.922, 1.351), Quality (0.488, 0.608, 0.871), Effectiveness (0.488, 0.608, 0.871).

After normalization and centroid defuzzification, the final normalized priority weights were: Trust 38.1%, Enforcement 22.8%, Legitimacy 16.3%, Quality 11.4%, Effectiveness 11.4%. The PSS tool was demonstrated with three hypothetical CABs assigned performance scores on a 1–10 scale per criterion, producing weighted totals of 6.47 (CAB A), 5.11 (CAB B), and 7.43 (CAB C), normalized percentages of 34.0%, 26.9%, and 39.1% respectively, with CAB C ranked first.

PSS model validation was conducted in two steps:

1. The Consistency Ratio (CR) was calculated on the defuzzified crisp pairwise comparison matrix following Saaty's classical AHP procedure: computing the geometric mean of each matrix

row, normalizing to obtain crisp AHP weights, multiplying by the original matrix to compute the weighted sum vector, deriving λ_i per criterion, and averaging to obtain $\lambda_{max} = 5.087$. The Consistency Index $CI = (\lambda_{max} - n)/(n - 1) = 0.0218$, and the Consistency Ratio $CR = CI/RI = 0.0218/1.12 = 0.0195$ – well below the 0.10 threshold, confirming that the expert pairwise judgments are logically consistent and the model is validated.

2. Sensitivity analysis across six predefined scenarios (Base, Trust +5%, Trust −5%, Enforcement +5%, Enforcement −5%, Quality +5%, Effectiveness +5%, and Equalized equal weights) confirmed that CAB rankings remain entirely stable under ±5% weight perturbations across all scenarios – with CAB C consistently ranked first, CAB A second, and CAB B third. Trust and Enforcement were confirmed as the most influential criteria: variations in their weights produce the largest shifts in total CAB scores, while Quality and Effectiveness (both 11%) exert minimal influence. The equalized scenario, where all criteria are forced to equal weight (20% each), produced results identical to the base case in terms of ranking – demonstrating that the weighted model reinforces rather than distorts the underlying evaluation.

THIRD CHAPTER FINDINGS

The empirical validation confirmed the PSF model's core assumptions with statistical rigor: certified IoT products consistently and significantly outperform non-certified counterparts on critical security metrics across all product categories and all six cybersecurity parameters, without incurring statistically significant performance penalties in any of the three product categories tested. The morphological and risk-based modeling confirmed the viability of a targeted subset of aligned private certification scenarios - approximately one-fifth of all possible combinations - while identifying systemic weak points in Key Securing and Secure Data that require explicit attention in certification scheme design.

The PSS model demonstrated practical applicability as a structured, transparent, statistically validated, and robust CAB selection

tool, producing consistent rankings under all tested weight perturbation scenarios.

Together, the PSF and PSS models form a closed-loop macro-micro system in which macro-level systemic forecasting provides the strategic rationale and boundary conditions for private scheme adoption, while micro-level structured decision-making operationalizes that strategy into concrete, defensible, and market-relevant CAB selection outcomes - bridging the gap between theoretical modeling and applied governance in cybersecurity certification.

CONCLUSION

An analysis of the prospects for private CAB integration into EU cybersecurity certification was performed, conclusions are as follows:

- **Topicality substantiated** - The rapid expansion of the IoT market (CAGR >25%, 2020–2025), the structural bottlenecks of public-only certification under Common Criteria, and the EU's landmark regulatory shift via the CSA, RED Delegated Act, and CRA collectively confirmed the urgency and relevance of researching private CAB integration into the cybersecurity certification ecosystem.
- **Quality and effectiveness of private CABs confirmed** - Contrary to initial concerns, private CABs do not compromise evaluation quality. Their sector-specific expertise, operational agility, and market-driven accountability - governed by ISO/IEC 17065 accreditation - produce certifications that are compliant, rigorous, and in many cases more responsive to emerging threats than traditional public mechanisms.
- **Regulatory risk mitigated** - The involvement of private CABs does not increase the risk of non-compliance. Mandatory accreditation standards, ongoing audits, peer reviews, and the competitive pressure of the market collectively serve as robust safeguards against quality degradation or regulatory erosion.
- **Harmonization maintained by law** - The EU's three-act framework (CSA, RED, CRA), coordinated by ENISA, preserves regulatory coherence across member states. Mutual recognition between public and private CABs is legally grounded and

practically feasible, as confirmed by cross-sector use-case analysis.

- **Trust identified and addressed as the central challenge** - Private CABs are currently limited to low and substantial assurance levels. Trust must be actively built through ISO/IEC 17065 accreditation, impartiality controls, transparency mechanisms, and demonstrated certification track records - a process that is underway and accelerating with growing market participation.
- **Security uplift without performance penalty** - empirically proven - Across all three IoT product categories tested (Flash Memory IC at EAL5+, Smart Grid Hub at EAL4+, IP Camera at EAL2+), certified products consistently outperformed non-certified counterparts on all six cybersecurity parameters (Data Encryption, Secure Default Passwords, Network Protections, Tamper Detection, User Account Protection, System Initialization), with statistically significant differences ($p < 0.05$ to $p < 0.001$), while showing no statistically significant performance degradation.
- **Market adoption supported** - The experimental results directly address and dismiss the concern that cybersecurity compliance degrades product attractiveness. Certified products maintain operational performance parity, removing the primary market barrier to certification adoption among IoT manufacturers.
- **PSF model - macro-level innovation delivered** - The Private Scheme Forecasting model, built on Multi-Phase Scenario-Based Modeling, provided a novel systemic framework for forecasting private certification adoption. From 324 morphological scenario combinations, the model identified the ~20% of plausible, high-weight pathways - confirming that hardware-centric, compliance-based, and nanotechnology-aligned scenarios yield the most viable and secure certification outcomes.
- **PSS model - micro-level innovation delivered** - The Private Scheme Selection model, built on the Fuzzy Prioritization Method, operationalized CAB selection into a six-step structured decision process. The model produced stable, validated criteria weights (Trust 38%, Enforcement 23%, Legitimacy 16%, Quality

11%, Effectiveness 11%) with a Consistency Ratio of 0.0195 - well within acceptable bounds - and rankings confirmed robust under ±5% sensitivity perturbations.

- **Integrated PSF–PSS framework** - original scientific contribution - The joint macro-micro system represents the dissertation's primary contribution to the field: PSF provides systemic foresight on private scheme adoption, PSS delivers the operational methodology for implementation, and together they form a closed-loop evidence-based roadmap - bridging theoretical modeling and applied decision-making in cybersecurity certification for the first time.

IV. DISSERTATION CONTRIBUTIONS

Contribution at the Macro Level - The Private Scheme Forecasting (PSF) Model:

1. An original model has been developed for assessing the credibility of private cybersecurity schemes: With the theoretical validation of certification efficacy and the empirical results, the model confirmed that certified products consistently outperformed non-certified counterparts on critical security measures across all

three IoT product categories, without incurring performance penalties. This provides strong evidence that certification enhances resilience while preserving operational efficiency.

2. System-level determinants of success: The PSF identifies three key conditions for effective private certification - innovative risk-based assessment strategies, realistic scenario construction balancing comprehensiveness with plausibility, and systemic integration of technological and methodological components.

3. Market implications: By demonstrating that strong compliance need not undermine competitiveness, the PSF reframes certification as a simultaneous driver of trust and market viability.

Contribution at the Micro Level - The Private Scheme Selection (PSS) Model:

4. An algorithmic model has been developed to support IoT manufacturers in selecting a CAB: As a methodological innovation: The PSS integrates fuzzy logic and optimize it via the Fuzzy Prioritization Method (FPM) to translate expert linguistic judgments into robust, quantitative priorities - addressing uncertainty and subjectivity more effectively than conventional AHP methods.

5. Operational strictness: Through six structured steps - criteria definition, pairwise comparisons, fuzzy translation, geometric mean optimization, defuzzification, and decision application - the PSS establishes a transparent, replicable, and validated decision process for CAB selection with Trust and Enforcement as the dominant criteria.

6. To facilitate practical application, the PSS model was implemented in a simple Excel-based tool; this implementation operationalizes the selection criteria and substantially simplifies

decision-making regarding CAB selection, thereby improving usability for practitioners.

Integrated Contribution - Linking PSF and PSS:

7. A strategy has been proposed for harmonizing private and public schemes within the European Union framework. With A dual-perspective framework connecting strategic foresight (PSF) with operational execution (PSS), forming a closed-loop system in which macro-level forecasting informs micro-level decision-making and micro-level methodology validates macro-level assumptions - providing an original, evidence-based roadmap for advancing private cybersecurity certification schemes that strengthen security resiliency, preserve performance efficiency, and sustain market viability.

V. PUBLICATIONS RELATED TO THE DISSERTATION

1. Menda-Shabat-More, R., & Veselina, S. (2026). Private schemes for cybersecurity certifications: Experimental modelling and forecasting for success. In W. Ding, A. Chakrabarti, M. Chakraborty, & S. Chakraborty (Eds.), *Proceedings of the Second International Conference on Advanced Computing and Systems. AdComSys 2025*. *Lecture Notes in Networks and Systems, 1887*. Springer, Cham. https://doi.org/10.1007/978-3-032-20253-6_15
2. Menda-Shabat-More, R. (2023). *Private schemes for cybersecurity certifications: An experimental modeling and*

forecasting for success. BISEC 2023 Conference, Belgrade Metropolitan University, Serbia, 24 November 2023. https://bisec.metropolitan.ac.rs/agenda-2023/
3. Menda-Shabat-More, R. (2023). *IoT cybersecurity certification: A multicriteria assessment approach*. 18th Annual Meeting of the Bulgarian Section of SIAM, BGSIAM'23, 11-13 December 2023, Sofia, Bulgaria. http://www.math.bas.bg/bgsiam/docs/bgsiam_2023_program.pdf
4. Menda-Shabat-More, R. (2024). *Cybersecurity regulations and standards: Best practices and the future challenges of the cybersecurity regulations evolvement*. International Conference: Technological Challenges to Security, Defence and Innovations in the New Digital Age. https://securedfuture21.org/int_sec_conf_iict_aora_apr_26_27_2024/int_sec_conf_iict_aora_apr_24_files/Int_Conf_PC_Sofia_April_26_27_2024.pdf
5. Menda-Shabat-More, R. (2024). *Private schemes for cybersecurity certifications: An experimental modeling and forecasting for success*. International Conference: Technological Challenges to Security, Defence and Innovations in the New Digital Age.
https://securedfuture21.org/int_sec_conf_iict_aora_apr_26_27_2024/int_sec_conf_iict_aora_apr_24_files/Int_Conf_PC_Sofia_April_26_27_2024.pdf
6. Menda-Shabat-More, R. (2026). *Designing secure-by-default IoT products: What will actually change under the CRA?* EU Cyber Act Conference, March 2026; GlobalPlatform CRA Summit, April 2026.
7. Menda-Shabat-More, R., & Veselina, S. (2025). *Private schemes for cybersecurity certifications: Experimental modelling and forecasting for success*. AdComSys 2025, 2nd International Conference on Advanced Computing and Systems, 26-27 June 2025. https://adcomsys.uemkcstcsit.in/past-editions