D. A. TSENOV ACADEMY OF ECONOMICS
DEPARTMENT OF STRATEGIC PLANNING

Raphael Röttinger

SECURITY MANAGEMENT OF PUBLIC SPORT EVENTS: A CASE STUDY ON FOOTBALL STADIUMS IN GERMANY

ABSTRACT

of a dissertation for awarding the educational and scientific degree of doctor, Doctoral programme “Public Administration” at the “D. A. Tsenov” Academy of Economics – Svishtov, Department of Strategic Planning

Scientific adviser: Assoc. Prof. Evelina Parashkevova-Velikova,PhD
Assoc. Prof. Hristo Sirashki, PhD

Svishtov
2025

The dissertation was discussed and proposed for defense at a meeting of the Departmental Council of the Department of Strategic Planning at the Faculty of Management and Marketing at the D. A. Tsenov Academy of Economics – Svishtov.

Details of the dissertation:
Number of pages – 337.
Number of figures – 11.
Number of tables – 5.
Number of literary sources – 321.
Number of publications of the doctoral student – 6.

The defense of the dissertation will take place on 08.05.2025 at 13:00 hrs. in the Rectorate Conference Hall at the D. A. Tsenov Academy of Economics – Svishtov.
The materials for the defense are available in the PhD and Academic Development department at the D. A. Tsenov Academy of Economics – Svishtov.

I. GENERAL CHARACTERISTIC OF THE DISSERTATION

1. Relevance of the Research

The dissertation examines the public-private security dynamics surrounding EURO 2024 by documenting operational failures in German football stadiums. Despite security being deployed, from June to July 2024, there were 2,340 crimes recorded, including 700 cases of physical assault and 140 cases against police officers. Therefore, the research inspects why standardized protocols failed. In Munich, for instance, security personnel identified 50 unauthorized drones but could prosecute only 14 cases due to unclear jurisdiction between private contractors and police. In the EURO 2024 matches, security staff reported communication breakdowns with law enforcement, leading to delays in responding to incidents. The necessity of preventing such failures in the future constitutes the source for the dissertations' relevance.

The study characterizes German stadium security from the early National Concept of Sport and Safety of 1992 up to the EURO 2024 period. This includes new issues such as modern drone flights above the venue or cyber-attacks against its infrastructural foundation as well as the risk of concerted terror attacks. Furthermore, the dissertation documents how past and possible future threats, for instance climate protests, exposed or could expose the gaps in existing security frameworks. Indeed, an analysis of 115,000 police measures during EURO 2024 revealed jurisdictional confusion between private security contractors operating inside stadiums and police forces responsible for surrounding areas. Finally, this research is relevant, as there have been documented incidents where ill-defined boundaries of authority between public and private security actors led to either late or uncoordinated responses to security incidents. Only a

thorough investigation of these incidents can inform future frameworks to prevent mishappenings.

2. Degree of Development of the Problem

Research on stadium security in Germany has repeatedly pointed to weak coordination, gaps in training, and legal ambiguities. One recurring issue involves communication failures between private security services and law enforcement. **Kubera et al.** (2019) found that in 28% of deployment briefings, private security was not present, which limited coordination with the police. Although security personnel largely meet formal certification standards—98% passed the required exams, according to **Eisenmenger** (2023)—these qualifications often lack stadium-specific training, leaving personnel unprepared for the environments in which they work.

Private security also plays a role in broader crisis management, although inconsistencies remain. During the 2015-2016 refugee crisis, **Schütte et al.** (2022) observed that private security firms ranked as the third most relied-upon partner in reception facilities. Despite this, they were excluded from 76% of coordination meetings, following the same pattern seen in stadium security. Legal authority creates further complications. **Müller-Eiselt** (2015) documented multiple disputes between government agencies and security firms, particularly regarding the limits of private personnel's detention powers outside stadium zones.

Security threats have also changed over time. **Mengistu and Getu** (2022) group stadium-related risks into health and safety concerns, alcohol-related disturbances, and crowd control failures. While these risks remain relevant, they do not account for all emerging problems at large events. Unauthorized drone activity, for example, has become a growing concern—Munich alone recorded 50 such incidents during EURO 2024. Security responses to these violations remain inconsistent, with no clear

division of responsibilities between public and private actors. Although **Soomro et al.** (2016) outlined security tasks related to information management, their study did not clarify jurisdictional questions on data-sharing. **Künzer and Hofinger** (2021) examined security risks across event types, infrastructure setups, and human behavior but did not analyze how these factors connect when private firms and state institutions coordinate their efforts.

3. Research Thesis

The dissertation argues that stadium security succeeds or fails based on institutional mechanisms governing public-private collaboration. The argument rests on data from EURO 2024, where venues with clear operational protocols between security contractors and police reported fewer incidents than those lacking standardized procedures. The research demonstrates this through three connected propositions:

First, multi-stakeholder operations depend on well-defined structural boundaries. At EURO 2024 venues, communication failures exposed the risks of poor coordination: private security teams operated without direct radio links to police command centers, slowing response times. Second, jurisdictional overlap further complicates decision-making. During pitch invasions, neither private security nor police intervened in some cases, as authority limits remained unclear. Third, large crowds introduce additional vulnerabilities that only integrated approaches can manage. Comparative data from EURO 2024 show that venues with joint public-private command centers handled crowd control more effectively than those relying on fragmented management structures.

The dissertation maintains that new threats require security frameworks to evolve. Drone activity at EURO 2024 underscored this point, as Munich reported 50 incidents where detection systems were in place, yet intervention protocols were absent. To examine how structural

approaches influence security outcomes, the research compared responses at venues following the National Concept of Sport and Safety (NKSS) guidelines with those implementing venue-specific protocols. While NKSS ensured consistency, its rigid procedures delayed adaptive decision-making. In contrast, venues with flexible frameworks identified and mitigated threats more rapidly. Security models designed for single-threat scenarios proved inadequate when attackers combined cyber intrusions with physical breaches, thereby proving the limitations of rigid, threat-specific planning.

4. Object and Subject of the Research

The *object* comprises institutional frameworks governing German stadium security between 2022-2024. This includes the National Concept of Sport and Safety (NKSS), state-level security regulations across 16 federal states, and venue-specific protocols at 10 EURO 2024 stadiums. Furthermore, the research inspects formal coordination mechanisms—from joint deployment briefings to standardized communication protocols—documenting their implementation across 51 EURO 2024 matches. Resource distribution procedures were specifically tracked, documented through 800 Technical Relief Agency (THW) personnel deployments across staging areas accommodating 100-200 staff each. The research mapped command structures at five coordination centers in Cologne alone, thereby analyzing how public-private partnerships managed technical equipment, workshop facilities, and emergency response units. These frameworks determined information flow between 580 international police forces and 22,000 security officers active during EURO 2024.

The *subject* revolves around actual interactions between public authorities and private contractors during EURO 2024 operations. For this, the research discussed the daily deployments of 800-1,300 security personnel per stadium, analyzing their coordination with municipal offices,

emergency services, and law enforcement. This includes the study of communication patterns between the International Police Coordination Centre in Neuss and security contractors as well as investigating how information flowed during 1,112 arrest warrant executions and 8,300 unauthorized entry preventions. Finally, the subject encompasses operational decisions made by security managers regarding resource allocation, threat response, and inter-agency coordination during actual security incidents.

5. Aim and Objectives of the Dissertation

The *aim* of this dissertation is to determine optimal frameworks for public-private security collaboration by analyzing EURO 2024 operations across 10 German stadiums. Four concrete objectives guided this investigation:

The concrete *objectives* are:

- evaluating coordination efficiency by tracking communication patterns, response times, and incident resolution rates among 22,000 security officers and 580 international police forces, thereby assessing how effectively public-private security entities collaborate;
- measuring framework adaptability, through the examination of responses to 50 drone incursions in Munich, to evaluate how security frameworks adapt to emerging threats and whether predefined security protocols can accommodate real-time risks;
- assessing regulatory oversight, by analyzing qualification standards that allowed 98% of security personnel to pass despite insufficient stadium-specific training, to scrutinize the effectiveness of licensing frameworks governing security professionals;
- extracting lessons from past incidents, by comparing EURO 2024 security management to historical failures such as the Hillsborough

disaster, and thereby identifiying structural weaknesses in public-private partnerships and regulatory enforcement.

6. Research Methods

This dissertation employs a mixed-methods approach that integrates the following qualitative and quantitative research techniques: a systematic literature review, expert interviews, a quantitative survey and four case studies.

The study begins with a systematic literature review based on the Paré & Kitsiou (2017) framework. A total of 321 scholarly and regulatory documents, where examined to present current security governance models and situate EURO 2024 within broader security management developments. Particular focus is given to inconsistencies in security policies, limitations in crisis response frameworks, and challenges in coordinating private and public sector efforts.

To capture and include the realities of stadium security, structured interviews were conducted with seven professionals who each had at least a year of experience in stadium operations. Their responses displayed communication obstacles, regulatory blind spots, and the practical constraints of adapting security protocols to unpredictable threats.

A survey of 361 security personnel working at EURO 2024 stadiums supplements these qualitative findings. Participants assessed the adequacy of training programs, the clarity of communication channels, and the efficiency of real-time decision-making. Their responses provide a basis for measuring preparedness levels and identifying patterns in operational strengths and weaknesses across different venues.

Finally, the study also investigated four historical events as case studies—Hillsborough, Heysel, the 2015 Paris attacks, and CTE 2024—to draw comparisons with contemporary security practices. These cases

expose recurring failures, including breakdowns in communication, overlapping jurisdictional responsibilities, and regulatory shortcomings.

7. Structure

The dissertation is divided into five main sections: introduction, argument in four chapters, conclusion, works cited list, and appendixes. The introduction presents the main thesis and hypotheses. Subsequently, the four chapters are structured by the level of analysis: conceptual (chapter 2), practical and applied (chapter 3) as well as prospective (chapter 4).

8. Research Limitations

While this dissertation provides an elaborate analysis of security governance at EURO 2024, several limitations must be acknowledged. First, the scope of case studies is restricted to four historical events: Hillsborough, Heysel, the Paris attacks, and CTE 2024. Although these cases did indeed allow for deriving understanding of public-private security coordination failures, additional comparative studies could further strengthen the generalizability of findings.

Another limitation relates to survey sample constraints. Despite the study surveyed 361 security personnel, this represents only a fraction of the 22,580 security staff deployed at EURO 2024. Certain security roles, such as emergency medical personnel and municipal law enforcement, were underrepresented in the sample. As a result, the findings may not fully capture the perspectives of all relevant security stakeholders.

Furthermore, the research is bound by jurisdictional specificity. The analysis is based on German regulatory frameworks, particularly the NKSS, and thus may not be directly applicable to countries with different legal and operational models for stadium security. Its recommendations must be contextualized for international applications.

Finally, emerging threats present a moving target. The study assesses security responses to drone incursions, cyber threats, and protest

disruptions, but these risks continue to evolve. Security governance models must remain dynamic and adjust to new threats beyond the study's timeframe.

II. CONTENT OF THE DISSERTATION

INTRODUCTION

The relevance of security management in contemporary society and its increasing importance in public and private sectors is presented, focussing on public events such as those in football stadiums. Furthermore, the research thesis regarding the integration of security frameworks and management methodologies is formulated. Additionally, the subject, object, aim and objectives concerning security management and large-scale event security are defined. Finally, the methodology of the study is described, including descriptive and empirical research approaches.

CHAPTER ONE: CONCEPTUAL DIMENSIONS OF SECURITY MANAGEMENT

1.1. Security Management – Areas of Application

This chapter contextualizes security management according to its areas of application. Security management operates where public and private domains converge. Public security, administered by state authorities, is designed to uphold societal order, while private security primarily focuses on asset protection and client-specific risk management. The increasing interdependency of public and private security actors has resulted in hybrid security models, where private firms directly complement law enforcement agencies. This integration is evident in areas such as infrastructure protection, corporate security, as well as event management.

Security management also encompasses indirect applications, where non-security personnel perform security-related functions. These include

transport operators acting as situational monitors and architectural designs that deter criminal activity through structural modifications. A critical area within security management is *event security*, particularly for large public gatherings such as EURO 2024. Security strategies for mass events incorporate *access control, surveillance*, and *risk mitigation measures* to ensure public safety.

1.2. Security Management Strategies — Cooperation Between Public and Private Sectors in Security Management

The increasing complexity and novelty of security challenges necessitates structured *collaboration between public and private security actors*.

This cooperation is classified into three levels: 1. Cooperation — informal, ad hoc interactions; 2. Coordination—formalized but independent operational structures; 3. Collaboration—fully integrated security frameworks.

Security partnerships often encounter challenges, including:

- *Jurisdictional ambiguities* regarding the legal authority of private security personnel.
- *Trust deficits* stemming from historical tensions between public and private security actors.
- *Training disparities* that affect the standardization of security competencies.

Empirical research, including findings from the *SiKoMi project*, indicate *role conflicts* and *communication barriers* in public-private security partnerships. Therefore, it can be concluded that *clear regulatory frameworks* and *operational integration mechanisms* are needed.

1.3. Security Management Methods

Security management methodologies draw from *criminology, risk analysis,* and *management science*, including:

- *Routine Activity Theory*—implying effectiveness and necessity of situational crime prevention through environmental modifications.
- *Rational Choice Theory*—focusing on offender decision-making and deterrence strategies.
- *Social Control Theory*—incentivizing benevolent behavioral regulation through normative enforcement.

Risk management in security planning integrates *predictive analytics, surveillance systems,* and *digital security frameworks*. Artificial intelligence and big data analytics enhance threat detection but require regulatory oversight to balance security efficiency with privacy considerations.

Cybersecurity governance plays a growing role in *preventing digital threats and securing critical infrastructure*. The expansion of AI-driven risk assessment tools presents both *opportunities for enhanced security* and *challenges* related to *data protection* and *algorithmic bias*.

1.4. Security Risks and Their Impact on Society

Security risks encompass a broad spectrum of threats that impact *societal stability and institutional resilience*. These risks range from *localized security breaches* to *large-scale emergencies*, necessitating *proactive risk management strategies*.

Security governance must address both *conventional threats*, such as property crime and terrorism, and *emerging risks*, including cyber-attacks and environmental hazards. The *integration of public and private security actors* is critical in mitigating the societal impact of security threats.

1.4.1. The Chaos Phase as a Critical Phase in Security Management

Security crises often follow a *predictable pattern*, beginning with an *initial chaos phase* characterized by *disruptions in communication, coordination failures, and situational uncertainty*. During this phase, *misinformation spreads rapidly*, and institutional responses may be *delayed or fragmented*. Security management must incorporate *structured crisis response mechanisms* to restore order and prevent escalation.

1.4.2. Current Threat Situation in Germany

Germany's current security landscape is shaped by *internal and external threats*, including: Cybersecurity vulnerabilities affecting critical infrastructure; Political extremism and radicalization trends; International terrorism concerns.

Government agencies and private security firms must *adapt risk assessment strategies* to counter these evolving threats, integrating *intelligence-sharing mechanisms with advanced surveillance technologies,* bounded by the law.

1.4.3. Large-Scale Emergencies and Their Impact on Society.

Large-scale emergencies, such as *terrorist attacks, natural disasters, and industrial accidents*, pose *unpredictable security challenges of high complexity*. Crisis management frameworks must ensure preparedness through training and simulation exercises, response with the deployment of emergency personnel and resources, recovery via post-crisis assessment and security reinforcement, and mitigation through long-term risk reduction strategies.

1.4.4. Attack Situations as Emergencies

Attack situations, whether *terror-related or large-scale security breaches*, require *immediate containment measures* to prevent escalation. Security responses must integrate *real-time intelligence analysis,*

interagency coordination, and *emergency response mobilization*. Some large-scale security breaches target security personnel, which then must prioritize *self-protection* as a means to stabilize the situation. Furthermore, attacks vary with regards to spatial and organizational complexity, not only determined by their number but primarily by the training of perpetrators. Appropriate response pathways to attacks on every part of the complexity spectrum are required.

1.4.5. Types of Simple and Complex Attack Scenarios

Security threats range from *simple, isolated incidents* to *coordinated multi-target* attacks. Simple attacks—often spontaneous and require immediate containment. Complex attack scenarios—involve strategic planning by adversaries, requiring advanced countermeasures and preemptive intelligence gathering.

1.4.6. Security Challenges of the EURO 2024

Major international events, such as *EURO 2024*, present *heightened security challenges*, including: Crowd management risks, Terrorism threats, Cybersecurity vulnerabilities.

EURO 2024 was a high-profile sporting event necessitating *comprehensive security planning*. Key concerns included *crowd safety, cyber threats,* and *intergovernmental security coordination*.

Security strategies originally planned for EURO 2024 included: Advanced surveillance and monitoring systems, Access control measures at stadiums and public spaces, Counter-terrorism protocols and rapid response teams.

Past major sporting events have witnessed *security breaches, including hooligan violence, unauthorized entry, and cyber-attacks*. The security management for EURO 2024 had to integrate *lessons learned from previous incidents* to enhance *preparedness* and *response capabilities.* Notable security incidents during EURO 2024 included: a violent fan-

security clash at Portugal vs. Slovenia (Frankfurt), with two German fans attempting to enter the pitch and an investigation into alleged mistreatment by stewards; five streakers disrupting Turkey vs. Portugal; a masked climber accessing the stadium roof during the Round of 16 (Dortmund), leading to a special police intervention and a penalty order; YouTuber Marvin Wildhage infiltrating the Munich Arena disguised as the mascot; riots and fan clashes before Serbia vs. England (Gelsenkirchen), with multiple arrests and the controversial sale of only light beer; multiple streakers at Spain vs. France, one of whom collided with a security guard, causing an impact with Spanish captain Morata.

Government agencies and security organizations reiterated *the necessity of multi-agency coordination, intelligence-sharing, and strategic planning* to be guarantors of the security at EURO 2024.

Public statements represent the importance of *technological innovations, emergency preparedness, and interagency cooperation* in managing event security.

An incident where a knife altercation in a fan zone left four people injured during EURO 2024 in Stuttgart was quickly resolved due to drone surveillance. This lead to explicit endorsements for such technologies.

CHAPTER TWO: PRACTICAL AND APPLIED ASPECTS OF SECURITY MANAGEMENT IN THE PUBLIC SECTOR

2.1. Strategic Dimensions of Security – Concept of National Security and Sport

Stadium security governance historically has been defined by the *Heysel* (1985) and *Hillsborough* (1989) disasters. Statistical analysis of 1,719 fatalities across 39 stadium incidents between 1946-2001 showed several interacting risk factors for disasters: *mass panic* (666 deaths), *riots*

(511 deaths), and *infrastructure failures* (166 deaths). These incidents lead to *divergences in European approaches* to stadium security management.

2.1.1. The National Concept of Sport and Safety as a Special German Feature

Germany's approach to stadium security was formalized through the NKSS implementation of 1992. While other European nations adopted primarily repressive measures, German policy combined security enforcement with socio-pedagogical interventions through mandatory fan projects.

2.1.2. Preventive and Repressive Measures in the National Concept of Sport and Safety and Their Legal Context

Legal frameworks governing stadium security distinguish between preventive and repressive measures within Germany's federal system. *Hazard prevention law* enables short-term protective measures, while *preventive criminal protection* combines deterrence with enforcement. Other European models diverge from this separation. Germany maintains a sharp separation between preventive and repressive state responses to violence, while in England these measures are scattered across various statutes. Additionally, Germany's federal system creates state-by-state variations in security regulations (e. g., reliability checks), whereas other nations tend to have more uniform national frameworks.

2.1.3. Relevant Infringements of Fundamental Rights in the Stadium.

Stadium security measures necessitate the consideration of constitutional rights and upholding their protections, especially *informational self-determination*, *physical integrity*, and *freedom of movement*. Surveillance technologies and data collection protocols require particular scrutiny, with legal frameworks needing to define acceptable limitations on privacy in service of security objectives.

2.1.4. Tasks of Security Staff in the National Concept of Sport and Safety

The NKSS mandates *hierarchical command structures* in stadiums, with operational managers heading security teams through section leaders. Security tasks revolve around *entrance control*, *facility protection*, and *unauthorized person removal*. Personnel must submit clean criminal records, though qualification standards remain vaguely defined by personality and appearance. Basic instruction covers property rights, bystander rights, and stadium-specific protocols.

2.1.5. Reform of the National Concept of Sport and Safety in 2012

NKSS reformation in 2012 addressed novel, emerging security challenges, in particular the rise of *ultra fan culture* and evolving threat patterns. Innovations central to the reform included enhanced network dialogue protocols, standardized qualification requirements through QuaSOD e-learning certification, and refined coordination mechanisms between security stakeholders.

2.1.6. Thirty Years of the National Concept of Sport and Safety: Development of Safety in German Football Stadiums

Three decades of NKSS implementation resulted in measurable impact through *increased stadium attendance* and *enhanced security protocols*. Contemporary challenges persist, including annual violence-related costs reaching 44 million euros. Security threats continue evolving, requiring adaptive response mechanisms and continuous framework refinement.

2.1.7. NKSS and Security Management in Football Stadiums

Overall, the NKSS centers around *infrastructure requirements*, *security protocols*, and *socio-pedagogical interventions*. Fan projects are such socio-pedagogical interventions that evolved from autonomous 1980s

initiatives to integrate security partners by 1992. The 1998 *Nivel attack* triggered *intensified hooligan countermeasures* within the NKSS.

2.2. Key Factors for Security Management at Public Sporting Events

Football stadiums, as enclosed spaces with controlled entry and exit points, large crowds, the presence of high-profile athletes, and the potential for fan violence necessitate multi-layered security approaches. Core factors influencing stadium security are: *Structural Design & Infrastructure*, shaping crowd control and evacuation; *Public-Private Security Coordination*, ensuring risk mitigation through cooperation; *Behavioral Risk Factors*, as football culture tolerates deviant behavior, with historical links to subcultures reinforcing territoriality; *Crowd Management & Conflict Prevention*, addressing risks like overcrowding and substance abuse through structured policing; *Trust & Communication Deficits*, as tensions between police and fans necessitate transparent enforcement.

German football security policy evolved ahead of the 2006 World Cup, by adopting a more repressive stance against hooliganism. Despite the associated efforts, empirical research shows ongoing tensions between security actors and fans, consequently requiring continued refinement of communication and enforcement frameworks.

Chapter Three. Empirical Study of the Practice of Providing Security at Public Sporting Events

The thesis uses a *multi-method approach*, by integrating the following four research methodologies:

1. Systematic Literature Review (SLR)—examines existing research on stadium security and security management best practices.
2. Qualitative Interviews—aim to capture expert perspectives from security personnel and event organizers.

3. Quantitative Survey—analyzes security personnel's experiences at UEFA EURO 2024.
4. Case Studies—investigate historical security failures of 4 selected disaster events.

3.1 Systematic Literature Review (SLR)

The literature review consolidates empirical findings from security studies, criminology, and legal analysis, where central aspects include:

- Variability in Security Standards: *lack of uniform training* and *qualification requirements* for private security personnel; calls for national certification frameworks are supported by studies on inter-agency coordination gaps.
- Comparative Security Strategies: differences between Germany, England, and France in the balancing of surveillance, fan engagement, and private security delegation.
- Monopoly vs. Oligopoly of Violence: increasing reliance on *hybrid security models*, where private firms operate alongside state actors.

3.2 Methodological Part 2: Qualitative Interviews.

A total of *seven expert interviews* were performed with professionals working in German Bundesliga stadiums. In the initial phase, *four interviews* were conducted with *personnel from a commercial security company* responsible for stadium operations. To complement this practitioner perspective, *three additional interviews* were conducted with *security managers and operations managers* overseeing IT and physical security at Bundesliga clubs.

The qualitative interviews follow a *semi-structured format*. Respondents include both security staff and operational managers, thereby offering perspectives from different hierarchical levels to approximate a statistically representative sample.

The interview questions are adapted from *Kubera et al.* (2019), structured into seven thematic blocks, covering premises, operational workflows, inter-agency cooperation, training protocols, and subjective assessments.

Interviews were conducted in *controlled environments* (security offices), avoiding post-match scenarios to promote respondent clarity. Transcriptions follow *content-oriented methods*, eliminating non-verbal data to maintain analytical focus.

Participants include security *executives* and *frontline staff*, coded as: IP1F, IP2F, IP5F, IP6F, IP7F (Executives), IP3M, IP4M (Frontline staff)

3.3 Methodological Part 3: Quantitative Survey

A *structured survey* was distributed among UEFA EURO 2024 *security personnel*, later expanded to include *municipal security agencies*, *emergency services*, and *public order offices*.

The study targeted 22,580 security professionals, with a minimum sample size of 384 respondents required for statistical validity.

The survey is divided into seven sections, each addressing:Background & role classification; Security strategy assessments; Critical security challenges; Public-private security cooperation; Best practices & case-specific observations (EURO 2024); Recommendations for future events.

A two-iteration approach allows for targeted expansion, thereby including underrepresented groups in the second round.

Responses are categorized by:

- Experience Level: differentiating seasoned vs. new personnel.
- Role Classification: identifying sector-specific security perceptions.

With greater experience, perceptions of security scenarios may become more accurate, which is why the experience level was chosen as a category. Role classification was included as a differentiator as

perspectives vary based on assigned responsibilities, and domain-specific vulnerabilities become more apparent. Numerical and open-ended responses are analyzed separately, to ensure contextual interpretation alongside statistical evaluation.

3.4 Case Studies.

The study includes four case studies, that historically represent major security failures and futile, yet partially adaptive response strategies.

Case studies in general provide depth and contextual specificity, compensating for the generalizability limitations of quantitative surveys.

A total of four case studies are selected, based on historical relevance, as well as scope and scale of the disaster:

1. Hillsborough (1989): A case of crowd management failure, compounded by infrastructural insufficiencies.
2. Heysel (1985): A Clear demonstration of the consequences of inadequate fan segregation, poor stadium infrastructure, and weak security planning.
3. Paris Attacks (2015): An example for the risk of external security threats, that necessitate counter-terrorism preparedness.
4. Counter-Terrorism Exercise (CTE) 2024: A real-world security drill simulating multi-target attacks, simultaneously evaluating inter-agency coordination and crisis response strategies.

3.5 Research Results

Results of all qualitative, empirical subcomponents (qualitative interviews & case studies) of the research methodology are presented in this chapter.

This chapter introduces the expert interview results.

The introductory question block identified participants' roles and security responsibilities: managing directors and senior staff from stadium security firms, security officers with operational duties, security managers

from Bundesliga clubs, and IT security operations managers. Of the interview participants, specific responsibilities span overall *security coordination*, *personnel management*, *access control*, and *emergency response*. Most participants expressed *confidence in Germany's preparedness for EURO 2024*, though some anticipated *challenges* related to *terrorism, hooliganism*, and *crowd management*.

All interview partners confirm compliance with the NKSS regarding dedicated spaces for security personnel. These areas serve multiple functions: Preparation and debriefing center, Break room for staff, Central operations hub, Shared space with other service providers.

The shared nature of these spaces is meant to *incentivise inter-agency communication and coordination*, particularly during fast-paced, high-stakes security incidents.

Work operations performed by the interviewed professionals encompass multiple security dimensions:

- Access control at entrances/exits
- Crowd management throughout events
- Emergency response protocols
- Conflict de-escalation
- Collaboration with police and authorities

According to the professionals, legal requirements generally provide clear operational frameworks, though *moral or legislative challenges exist* in areas such as: Data protection regulations (DSGVO); Temporary employment limitations; Physical intervention protocols; Surveillance technology deployment.

According to the professionals, security operations need internal briefing structures that work well and employ several methods: Teams meet before events to talk about how many people will come and what might go wrong (*pre-event briefings*); they give each person their own job

to do (*task distribution and responsibility allocation*); leaders join these meetings (*leadership team participation*); after events, teams meet again to talk about what happened (*post-event debriefings*) and they use phones and apps to stay in touch (*mobile communication systems*).

According to the interviewees, external communication networks incorporate multiple stakeholders such as:

- Club security officers
- Other security service providers
- Federal Police
- Deutsche Bahn (German railway)
- Local authorities
- Fan projects

Furthermore, communication methods mentioned by the interviewees were:

- Email and telephone for pre-event coordination
- Radio systems during events
- Joint deployment briefings
- Network-wide debriefings

Collaboration with fan projects proves particularly valuable for conflict resolution and de-escalation due to the prevention of hooliganism and the development of trust.

Security personnel undergo differential, comprehensive training programs covering:

- Security protocols and access control
- Evacuation procedures
- Fire safety
- Conflict management
- De-escalation techniques
- Legal compliance

- Communication coordination

Equipment allocation varies by deployment location and responsibility level. Training is primarily company-led rather than club-organized, with some participants advocating for increased frequency and joint training sessions with network partners.

3.6 Survey Results

Results of the quantitative survey of 361 security professionals are presented. Participants were distributed over a range of operational/occupational roles: security personnel (39.89%), law enforcement (18.84%), fire services (7.76%), emergency medical services (6.93%), team leaders (6.65%), event coordinators (6.65%), disaster management (4.15%), municipal public order office directors (1.94%), and municipal security services (7.20%). Experience levels varied significantly, with 21.88% having 1-3 years experience, 10.80% with 4-7 years, 21.61% with less than one year, and 13.30% with over eight years. Important implications derived from the results were:

- NKSS effectiveness evaluations showed large differences between experienced and inexperienced groups.
- Role-specific perceptions of public authorities' coordination were consistent with varying levels of satisfaction.
- Integration challenges between private and public security services were mentioned and represent systemic issues.
- Assessment of security measures during EURO 2024 was heterogeneous.
- Recommendations for future improvements were centered around training, communication, and technology integration.

Several patterns in public-private collaboration for stadium security governance can be identified from the quantitative survey:

1. Divergent Perceptions: Significant gaps exist between public sector actors and private security personnel in assessing governance framework effectiveness. Law enforcement rated NKSS-effectiveness substantially higher (23.5%) than security personnel (9%).
2. Resource Constraints: Public authorities consistently identified resource limitations as a primary obstacle, with over 50% citing inadequate funding and manpower.
3. Strategic Oversight: Role delineation emerged as a critical concern, with 33% of private security personnel reporting lack of operational clarity.
4. Training Importance: 32.18% of experienced participants identified regular training as the primary improvement area.
5. Emerging Threats: Technological advancement and geopolitical tensions require proactive governance approaches.
6. Communication Challenges: Significant disparities in communication satisfaction levels between law enforcement (50% positive) and private security providers (34% positive).

Concluding the findings of the quantitative survey validates the central thesis of this research regarding institutional framework importance in stadium security governance. Important details uncovered were:

1. Governance Framework Analysis:
    a. Strengths: Public authorities' regulatory authority and crisis management experience
    b. Shortcomings: Inconsistent implementation and resource allocation issues
2. Resource Management:
    a. Municipal authorities report significant staffing and financial constraints

b. Technology infrastructure gaps affect operational effectiveness

3. Communication Effectiveness:
    a. Information flow breakdowns between public and private sectors
    b. Need for centralized communication platforms
4. Security Threat Response:
    a. Lack of standardized protocols for emerging threats
    b. Resource limitations impacting technological adoption
5. Training Programs:
    a. Joint simulation exercises underutilized but highly valued
    b. Inconsistent training standards between sectors
6. Strategic Leadership:
    a. Public authorities' unique position as governance leaders
    b. Need for greater private sector inclusion in decision-making

In total, the quantitative analysis concludes that effective stadium security governance requires: Strategic alignment between stakeholders; Adaptive capacity for emerging threats; Collaborative partnerships; Optimized resource allocation.

3.7 Discussion of Results

Equipment and *operating standards* remain *inconsistent across Germany*. Technology use varies widely between venues, while protective gear often falls short of requirements set by the 1992 NKSS guidelines.

Analysis of past incidents, like Hillsborough, shows *serious flaws* in *accountability* and *emergency response times*. These cases ought to further inform current security officer training.

Public and private security forces require different equipment based on their roles. Less restrictive approaches have reduced violence, while

clear uniform distinctions affect how fans interact with staff. The legal framework gives security personnel certainty in their actions.

Communication between law enforcement agencies remains weak, according to our survey. Security incidents occur frequently, based on staff reports. Risk assessment directly affects management effectiveness. Security teams *lack clear protocols* for *communicating with families* during incidents.

The public generally *distrusts facial recognition systems* at venues. Protecting fan data while maintaining security remains a conflicting dichotomy to this day. EURO 2024 raised concerns about tracking spectators. A *mixed public-private security model* works best.

The *QuaSOD program* tried to *standardize training*, but current *regulations under § 34a GewO fall short*. Stadium alliances in NRW show progress. The system of service and event stewards needs updates.

Debate continues over who should pay for police operations. Clubs fund private security services. *Security quality depends* partly *on costs*. Laws need revision regarding club-owned versus commercial security forces.

Main arguments of the thesis about institutional structures, adaptation, and accountability in stadium security are supported. In total, the following are specific needs for future stadium security governance:Standard equipment and training rules; Better communication systems; Clear public-private security roles; Careful use of technology; Updated qualification rules; Fair cost sharing.

Chapter Four. Applied Aspects of Security Management in the Public Sector

4.1 Best Practices for Security Management

This chapter evaluates case studies of security crises to develop optimization frameworks for large-scale events that are similar to EURO 2024.

4.1.1 Overview

This chapter provides an overview of the case studies' central features:

1. Hillsborough Disaster – Overemphasis on hooliganism prevention; physical barriers worsened crowd dynamics; delayed emergency response due to poor communication; infrastructure failures amplified human errors; community response exposed planning gaps.
2. Heysel Stadium – Infrastructure deficiencies and poor crowd management; ticket allocation errors led to failed fan segregation; confirms research hypotheses on strategic alignment, framework evolution, and social context adaptation.
3. Paris Attacks – Highlights rising security complexity; rational choice theory in target selection; multi-target strategy strained resource allocation; emphasizes need for stronger public-private security cooperation.
4. CTE 2024 – Demonstrates benefits of proactive security; underscores high resource demands of comprehensive preparation; reveals controlled environment limitations and operational coverage challenges during training.

4.1.2 Hillsborough

Several factors made this tragedy preventable. The stadium's *documented safety issues* were well known, yet officials proceeded with unprecedented police decisions that proved fatal. The situation worsened due to *poor communication with hospitals* and a stark *lack of basic equipment and supplies*.

The accountability failures compound the tragedy. Officials initially *blamed the fans*, while *police* systematically *falsified their statements*. The *weak public oversight structures* enabled a *cover-up*, as officials tightly controlled information flow. These actions point to necessary *reforms*: *mandatory independent documentation*, *immediate public disclosure requirements*, *direct legal accountability for officials*, and *clear standards for essential resources*.

4.1.3 Heysel

At Heysel Stadium, the breakdown occurred at multiple operational levels. Authorities *mishandled ticket allocation* and *failed to* properly *separate rival fan groups*. Security personnel showed *limited awareness of potential risks*, while adherence to societal norms complicated crowd behavior patterns.

4.1.4 Paris

The Paris attacks exposed specific vulnerabilities in modern security frameworks: The rise of *foreign agents* created new threats that existing intelligence systems struggled to track, especially regarding cross-border movement. Consequently changes in security approaches occured, demanding *proactive coordination* and *integrated intelligence* across agencies. The attacks also had negative societal effects, as in the promotion of negative sentiments toward immigration, eroding trust in institutions, and fundamentally altering public perceptions of safety.

4.1.5 CTE 2024

As a counter-terrorism exercise, the CTE 2024 presented progress in security preparation. It successfully tested *cross-border cooperation* and developed wide-ranging scenarios involving multiple stakeholders, thereby proving the legitimacy of iterative simulation exercises.

4.1.6 Summary and Comparison of Results

All events make clear the fundamental necessity for *robust emergency response systems* and *adequate private-public security cooperation*. Emergency preparation has improved, stakeholder integration has increased, and security scope has broadened.

Yet, each type of threat raises idiosyncratic demands: hooliganism requires different tactics than terrorism, crowd management varies by context, and modern threats often emerge from multiple directions simultaneously. Effective security frameworks therefore must *incorporate historical lessons* while adapting to emerging threats in an increasingly complex security landscape.

4.2 Prospects for the Security Management of Public Sport Events

The first two chapters lay a robust foundation for comprehending the intricate tapestry of security management, highlighting the diverse areas of concern, the interplay of prevention and response strategies, the importance of inter-agency collaboration, the influence of legal frameworks, the necessity of comprehensive personnel training, the valuable contributions of theoretical frameworks, and the imperative of adaptability in the face of dynamic security landscapes. This was complimented by focusing on security and security management in the context of football events, by highlighting the importance of both internal and external security factors. However, the technology has faced criticism from civil rights groups over data privacy and constitutionality concerns.

4.3 Holistic Security Concepts

The research uncovers evidence of *long-standing mistrust* between *fans* and *police forces*: In 1988, only 3 out of 28 police officers stated conversations with fans were possible, while 22 reported fan aversion. This led to SOD deployment in stadiums operating between police intervention

thresholds and tolerated violence. The findings prove that, in a holistic security concept, both conflict parties must calculate each others' behavior through *information exchange* about causes of violence, *fan culture codes*, and *police measure purposes*. When repressive measures exceed the 'intermediate phase between civilization and escalation,' situations deteriorate. The NKSS as an attempt for framework holism, specifically mandates *clear communication about security restrictions* affecting peaceful fans.

4.4 Recommendations for Action in Providing Security

Research results and theoretical groundwork yield four main recommendations:

- Training and Education: building modular training programs combining technical skills with social abilities
- Technology Integration: surveillance systems with privacy protections need to be implemented
- Public-Private Cooperation: creating standardized qualifications through joint exercises
- Emergency Response Plans: the rehearsal and subsequent application of industry standard practices through regular drills

4.4.1 Developing a Guideline and Recommendations for Action Concerning Stadium Security

The summative analysis of expert interviews and case studies produce specific operational guidelines: Risk assessment must account for *crowd size variations* and *potential escalation triggers*. Access control requires *layered verification* at *predetermined checkpoints*. Emergency protocols must specify *first responder roles* and *evacuation routes*. The research determines that communication systems between security teams require *redundant backup channels*. Technology integration guidelines

mandate *data protection compliance* while maintaining *rapid threat detection capabilities*.

4.4.2 The Scope of Recommendations

EURO 2024 functions as the contextual backdrop for these recommendations. The tournament's security measures involved substantial investment (250 million euros across host cities), specialized personnel, as well as technological systems.

4.5 Conceptual Model for Public-Private Cooperation in Security Management

Hybridization of security tasks since the 1970s created *interdependency between public and private forces*. The SiKoMi project results showed formal structures like coordination meetings proved indispensable, while informal networks enabled flexible crisis response. Private security forces reported feeling unequal to public counterparts, reducing cooperation effectiveness. Joint training strengthened both technical and social competencies. The Safety II concept application improved organizational resilience against unexpected challenges. Digital real-time information exchange shortened response times and reduced misunderstandings.

4.6 Critical Success Factors for Security Management

Preventive measures must include *risk analysis*, *target hardening*, and *environmental design modifications*. Response strategies require *rapid deployment protocols* and *coordinated multi-agency efforts*. Legal frameworks delineated *precise operational boundaries* between police and private security powers. Training gaps persist particularly in the private sector despite standardization attempts. Routine activity theory, rational choice theory, and situational crime prevention provide evidence-based intervention strategies. The findings prove that security management strategies require *continuous evaluation cycles* to maintain effectiveness.

CONCLUSION

The dissertation investigates the optimization of governance frameworks for public-private collaboration in stadium security management, with particular emphasis on EURO 2024. Four key hypotheses are systematically analyzed, enabled by the employment of a hybrid research approach utilising four different qualitative and quantitative strategies. By this, the study generates knowledge regarding strategic alignment, emerging threats, regulatory oversight, and historical lesson integration. The NKSS, established over thirty years ago, proves generally effective as evidenced by declining violence rates and successful EURO 2024 operations. Despite this, quantitative analysis shows varying perceptions of its effectiveness: among experienced security personnel, only 11.3% rated it as effective and 17.9% as very effective, while 19.6% deemed it very ineffective and 35.1% ineffective. Notably, inexperienced participants show different response patterns, with 48.6% rating it neutrally and 29.7% ineffectively. Regional variations emerge as an additional consideration, especially in North Rhine-Westphalia, where 15 of 56 professional teams operate, requiring more elaborate security networks than regions like Bavaria with only six teams. The research concludes that standardized solutions must account for local factors including fan demographics, infrastructure conditions, and available personnel resources. Furthermore, the dissertation identifies several areas for future improvement in public-private security collaboration:

- Training and Qualification: The QuaSOD e-learning program represents progress in standardization, though limitations of virtual training in high-risk environments were acknowledged. Current qualification standards under §34a GewO prove inadequate, with documented failure rates of 1-2% resulting from systemic deficiencies.

- Personnel Management: The security industry is confronted with enduring, significant staffing challenges, requiring improved working conditions and reduction of marginal employment. Thus, the research advocates for expanding full-time positions to address personnel shortages and simultaneously enhance professional development.
- Operational Integration: During EURO 2024, emerging threats like drone incursions (with 50 identified drones in Munich alone, resulting in 14 legal charges) and cyber risks demonstrated the need for adaptive security frameworks. Therefore, the research concludes that traditional structures struggle to address these evolving challenges.
- Communication Networks: The research proves the importance of regular joint scenario exercises and mandatory training sessions. Trust-building between public and private security forces is similarly necessary, with evidence showing improved spectator relations where security personnel maintained consistent presence.

Analysis of historical cases provide additional support for the given hypotheses: The Hillsborough disaster (1989) influenced modern crowd management protocols, while the Heysel Stadium tragedy (1985) shaped fan segregation strategies. The 2015 Paris attacks led to enhanced information sharing and specialized counter-terrorism units, elements tested during CTE 2024. In total, the research validated all four hypotheses:

- H1: Strategic alignment through governance frameworks enhances operational effectiveness
- H2: Emerging threats disproportionately impact traditional security structures
- H3: Enhanced regulatory oversight improves private security integration

- H4: Historical lessons provide crucial foundations for future-proof strategies

Methodological limitations of the research include restricted access to EURO 2024 security measures due to confidentiality requirements and the relatively small sample of seven expert interviews. Future research opportunities include expanding stakeholder perspectives through broader surveys, most importantly incorporating fan perceptions of security measures. The study concludes that effective stadium security governance requires frameworks that balance standardization with local adaptation, integrate emerging technology responses, and maintain strong public-private coordination. Success depends on continued professional development of security personnel, enhanced communication networks, and systematic application of historical lessons to contemporary challenges.

III. REFERENCE OF SCIENTIFIC AND SCIENTIFIC-APPLIED CONTRIBUTIONS IN THE DISSERTATION

First. The dissertation empirically documents security framework failures during EURO 2024, contextualizing them within the history of stadium security. It provides a unique, broad analysis by incorporating statistical data on 2,340 criminal incidents, including 700 cases of physical assault and 140 against police officers. The study highlights standardized security protocol failures, such as jurisdictional confusion in Munich, where 50 unauthorized drones were detected but only 14 cases prosecuted. Additionally, it examines communication breakdowns between law enforcement and private security, emphasizing the operational gaps exposed by emerging threats like drone activity. On this basis, the dissertation presents a framework for integrating emerging security technologies with legal compliance. The framework standardizes security

surveillance, ensuring interoperability between private and public security forces. Empirical validation through EURO 2024 data shows that structured technological integration improves coordination. A large quantitative survey further supports findings, identifying inter-agency communication gaps, role-specific risk perceptions, and collaboration challenges. The study quantifies areas for improvement, with 32.18% of experienced personnel recommending frequent drills and 25.29% emphasizing better technology adoption.

Second. The research highlights how ill-defined authority boundaries between public and private security actors resulted in delayed or uncoordinated responses. This analysis is supported by examination of 115,000 police measures during EURO 2024 that showed jurisdictional confusion between private security contractors operating inside stadiums and police forces responsible for surrounding areas. Furthermore, this scientific contribution encompasses exemplary information about how emerging threats exposed gaps in existing security frameworks

Third. The dissertation makes a methodological contribution through a validated mixed-methods security analysis framework, applicable to other large-scale events. This framework integrates a systematic literature review, structured interviews, quantitative surveys, and historical case study comparisons. The literature review, based on the Paré & Kitsiou (2017) framework, identifies research gaps in security policies, crisis response frameworks, and public-private coordination. Interviews document communication barriers and regulatory blind spots, featuring managing directors, security officers, Bundesliga security managers, and IT operations managers. The structured interviews with seven security professionals who each had at least a year of experience in stadium operations provide context for understanding the operational realities behind the statistical data gathered via the survey. The survey

component, with 361 respondents across security roles, provides statistical validation. Comparative case studies—Hillsborough (1989), Heysel (1985), Paris Attacks (2015), and CTE 2024—enable pattern identification in security failures and response strategies. The mixed-method approach effectively cross-validates findings, revealing disparities in inter-agency communication satisfaction, with 50% positive ratings from law enforcement versus 34% from private security.

Fourth. The dissertation develops an evidence-based framework for integrating public and private security at major sporting events. Empirical validation shows that venues with standardized security cooperation had fewer incidents. A comparative analysis of venues following the National Concept of Sport and Safety (NKSS) versus those with venue-specific protocols highlights structural factors influencing security outcomes. The study maps command structures in Cologne, examining interactions among five coordination centers and security information flow between 580 international police forces and 22,000 security officers.

IV. LIST OF PUBLICATIONS OF THE DOCTORAL STUDENT

Scientific articles:

1. **Sicherheit im Fußballstadion – Mehr Standardisierung beim Einsatz gewerblicher Ordnungsdienste erforderlich**
   In: Der Sicherheitsdienst, Bd. 76, 2024, Nr. 01, S. 6–7.
2. **Gewalt gegen privatrechtlich und hoheitlich handelnde Sicherheitskräfte bei Fußballveranstaltungen**
   In: Die Kriminalpolizei, 4. Dezember 2024, S. 7–9, ISSN 0938-9636..
3. **The Current Security Situation at Major Events from an Official Perspective**
   In: IJASOS – International E-Journal of Advances in Social Sciences, 25. Dezember 2024, Vol. 10, No. 30, S. 407–414.
4. **Cooperative Strategies in Security Management**
   In: e-Journal VFU, 2025, Vol. 23, S. 133–149, ISSN 1313-7514.
5. **Prevention Strategies against Violence in German Football Stadiums: A Public Administration Perspective**
   In: Народностопански архив (Narodnostopanski Arhiv), 2025, Vol. 1, ISSN 0323-9004, ISSN 2367-9301 (im Druck).
6. **Kritis (Critical Infrastructure) and Current Threats: Challenges and Opportunities for Public Administration in Modern Crisis Management**
   In: e-Journal VFU, 2025, Vol. 23, ISSN 1313-7514.

V. RERENCE OF MEETING THE MINIMUM NATIONAL REQUREMENTS FOR OBTAINING THE EDUCATIONAL AND SCIENTIFIC DEGREE OF DOCTOR UNDER THE REGULATIONS ON THE IMPLEMENTATION OF THE LAW ON ACADEMIC STAFF DEVELOPMENT IN THE REPUBLIC OF BULGARIA

National requirement in number of points: 30,00

Number of **articles**, published in non-refereed peer-reviewed journals or published in edited collective volumes:
Number of points for the author: **55,00**

Number of **papers**, published in non-refereed peer-reviewed journals or published in edited collective volumes:
Number of points for the author: 0,00

Total points: **55,00**

VI. DECLARATION OF ORIGINALITY OF THE DISSERTATION

The presented dissertation in a total volume of 337 pages on the topic:

SECURITY MANAGEMENT OF PUBLIC SPORT EVENTS: A CASE STUDY ON FOOTBALL STADIUMS IN GERMANY

is an original author's work.

It uses author's ideas, texts and visualization through graphics, schemes, tables and figures, and all the requirements of the Copyright Act and related rights are complied with by proper citing and referring to other authors' opinions and data, including:

1. The results and contributions in a dissertation work are original and are not borrowed from research and publications in which the author has no participation.

2. The information presented by the author in the form of copies of documents and publications, personally compiled references, etc. corresponds to the objective truth.

3. The scientific results obtained, described and/or published by other authors are duly cited in the text and included in the bibliography.

10. March 2025

Doctoral Student:……

(Raphael Röttinger)