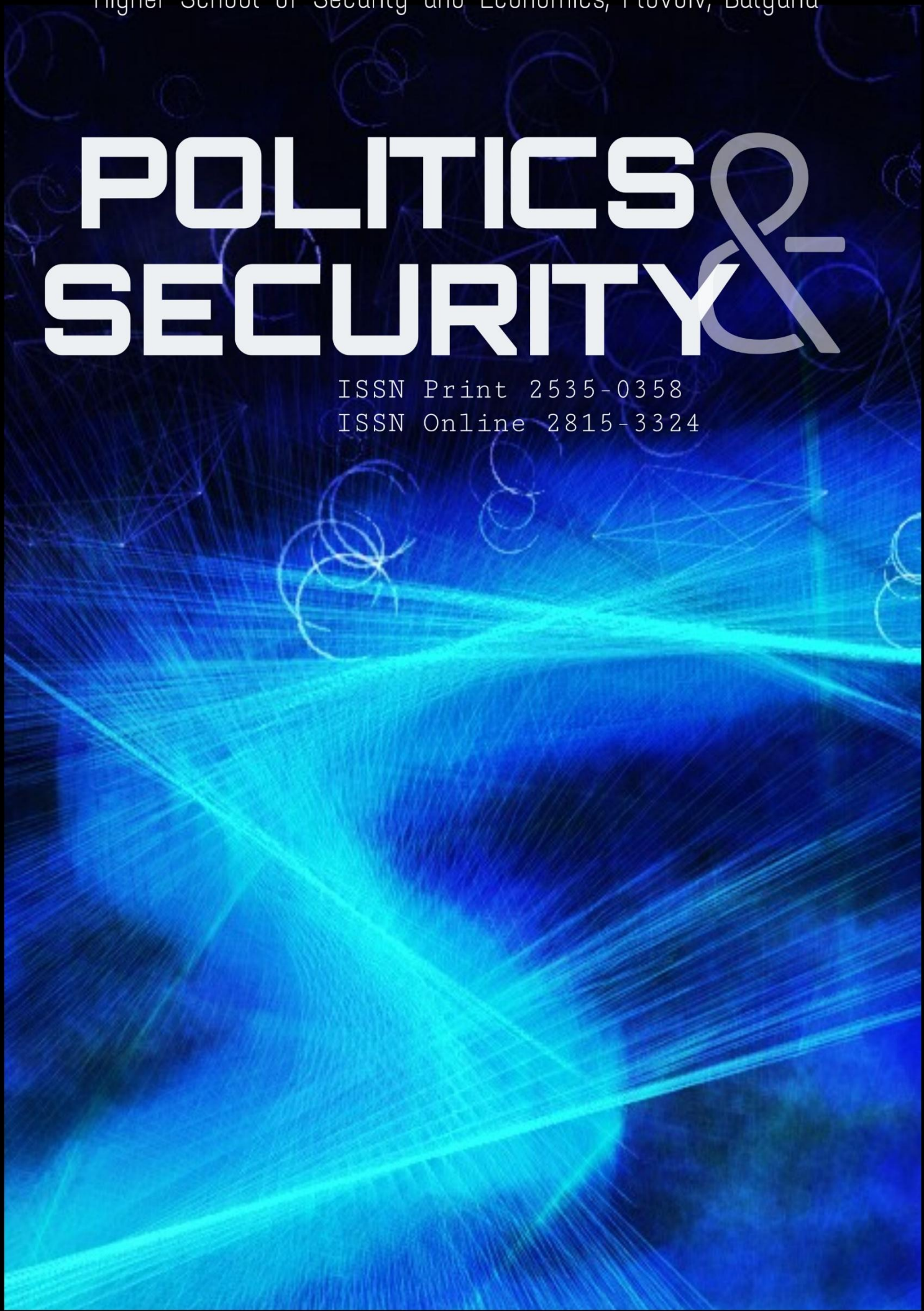
Higher School of Security and Economics, Plovdiv, Bulgaria

POLITICS & SECURITY

ISSN Print 2535-0358
ISSN Online 2815-3324



EDITORIAL BOARD

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

FOREWORD

Vol. 13 No. 3 (2025)

Dear Readers,

The publication of Volume 13, Issue 3 (2025) of Politics & Security arrives at a pivotal moment, as the global security system is undergoing a profound transformation. The familiar unipolar architecture of the world order is increasingly giving way to a more complex, volatile multipolar world, characterized by growing geopolitical competition and deep ideological polarization. This transition is not abstract; it is manifested daily in rising instability—from the elevated risk of military clashes in regions like Eastern Europe, the Middle East, and the Asia-Pacific, to the sobering fact that interstate armed conflicts are now considered the main global risk in the near future.

This issue fully reflects our mission to foster interdisciplinary research and dialogue in the face of these contemporary global challenges. The studies presented herein cover a wide and critically important spectrum of topics, underscoring that complex threats demand the integration of knowledge from political science, international relations, military affairs, information technology, and law.

This volume offers timely and in-depth analysis across four critical areas:

- Geopolitical Shifts and Alliance Dynamics: We explore the dramatic recalibration of power, from the fracturing of the Visegrád Group in the wake of the Ukraine war to the intensifying US-China rivalry that is reshaping the Indo-Pacific into a complex, networked strategic arena.
- The Digitalization of Defense and Critical Infrastructure: The rapid digitalization of defense processes is altering the nature of security. Our contributors explore the new vulnerabilities created by the integration of Internet of Things (IoT) systems in critical national infrastructures. They emphasize the urgent need for a comprehensive approach, combining technical defenses with organizational and legal measures to counter evolving cyber threats.
- Governance, Security, and Accountability: A key theme is the challenge of ensuring security without eroding fundamental rights and freedoms. Papers address this by examining the political and institutional failures in managing strategic intelligence in Nigeria, where issues like politicization of findings and public distrust significantly impede law enforcement, and by analyzing how the ambiguity of extremist rhetoric challenges legal oversight frameworks like those of the European Court of Human Rights.
- The Privatization of Coercion: Finally, we confront the escalating role of Private Military Companies (PMCs), demonstrating how the rise of the state-proxy model—such as the Wagner Group—exploits a persistent vacuum in international law to project geopolitical influence with near-total impunity.

The international composition of our authors and the diversity of their topics attest that scientific analysis is more important than ever for developing effective solutions. I am confident that the in-depth, interdisciplinary analysis presented here will help to develop sound approaches to strengthening security in the face of our contemporary global challenges.

Igor Britchenko

Editor-in-Chief

Politics & Security

CONTENTS

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

STRATEGIC INTELLIGENCE MANAGEMENT AND LAW ENFORCEMENT IN NIGERIA: FIXING THE GAPS

Ngboawaji Daniel Nte
Department of Intelligence and Security Studies
Provost, College of Management and Social Sciences
Novena University, Ogume, Delta State, Nigeria
https://orcid.org/0000-002-331-3511
profdnte@novenauniversity.edu.ng

Ben Robert Eyororokumoh
Department of Intelligence and Security Studies
Novena University, Delta State, Nigeria
albenny90@yahoo.co.uk

Abstract: *This study focuses on important issues in how strategic intelligence is managed within Nigerian law enforcement agencies, with the goal of improving national security. It looks at the current situation of intelligence collection and analysis, looking at the structures, processes, and abilities in place. The study identifies key obstacles to effective sharing and cooperation among security agencies, exploring institutional, operational, and cultural challenges. It also evaluates the quality of training and technology available for intelligence work, looking at the effectiveness of training programs and the state of technological resources. The research also looks at how socio-political issues like political influence, corruption, and public attitudes affect the objectivity and success of intelligence agencies. Based on these findings, the study offers practical advice and strategies to close these gaps and improve the security system in Nigeria, ultimately making law enforcement more effective.*

Keywords: Strategic Intelligence, Law Enforcement, Nigeria, Intelligence Management, National Security, Intelligence Sharing, Training, Technology, Socio-political Factors, Crime Control.

1. INTRODUCTION

1.1 Background of the Study

Strategic intelligence management is essential for effective national security and law enforcement around the world. It involves collecting, analyzing, and sharing information to make informed decisions, predict threats, and use resources better against different types of crime and instability. In today's complex security environment, intelligence is not a side function but a key part of planning and taking action ahead of threats rather than just reacting to them. Integrating intelligence into all areas of law enforcement ensures that agencies work with foresight, targeting the causes of crime and reducing emerging security risks. This approach focuses on understanding the criminal environment, identifying key players, and predicting how they operate, allowing law enforcement to use resources wisely and effectively (Handel, 2005).

Nigeria, a country facing many complex and changing security issues, heavily depends on strong strategic intelligence management. The nation deals with ongoing threats from terrorism, especially groups like Boko Haram and ISWAP, which have caused devastation and displaced millions in the North-East. Beyond terrorism, widespread banditry in the North-West and North-Central regions has resulted in mass kidnappings, violence, and economic damage. Kidnapping for ransom has become a widespread issue across the country, affecting both urban and rural areas, while organized crime groups continue to engage in illegal activities such as oil theft, human trafficking, and financial fraud. These problems together weaken national stability, economic growth, and public safety (Amnesty International, 2023). Tackling these complex security threats requires a smart and well-planned intelligence system. Good intelligence gives the foresight needed to stop attacks, break up criminal networks, rescue victims, and bring criminals to justice. Without it, law enforcement remains reactive, chasing incidents instead of preventing them, which reduces public trust and worsens insecurity (Ochonu, 2018).

1.2 Statement of the Problem

Even though strategic intelligence is very important, there are big gaps in how it is managed and used by Nigerian law enforcement agencies, greatly affecting their ability to fight the country's many security challenges. A major issue is the lack of collaboration and information sharing between agencies. Many security agencies exist in Nigeria and often have similar duties and responsibilities, yet there is a strong culture of competition and reluctance to share important intelligence. This creates isolated pockets of information, preventing a full understanding of threats and weakening coordinated responses. Important intelligence, spread across different agencies, often doesn't reach the right people at the right time, leading to missed chances and operational failures (Obasi, 2017).

In addition, there is a major lack of training and development for intelligence personnel. Many intelligence officers don't have advanced training in modern methods like data analysis, human intelligence collection, and cyber intelligence. This limits their ability to process complex information, find useful insights, and deal with new threats. Along with this is the limited technological support and tools available to agencies. Old equipment, lack of secure communication channels, and few advanced analytics software hinder the efficient gathering, processing, and interpreting of large data sets, which are essential for generating strategic intelligence (Adebayo, 2020).

The politicization of intelligence is another big challenge. Sometimes, intelligence findings are altered or hidden to serve political goals rather than national security. This can lead to wrong threat assessments, misusing resources, and a loss of objectivity within the intelligence community, ultimately harming its integrity and effectiveness. Also, public distrust and reluctance to share information with law enforcement agencies hinder intelligence gathering from the local level. Past abuses, lack of accountability, and perceptions of corruption reduce public confidence, making communities less willing to give important information, thereby cutting off a key source of intelligence (Human Rights Watch, 2022).

Finally, limited resources, including insufficient funding and inadequate equipment, greatly restrict the operational abilities of intelligence agencies. Staff often lack basic tools, vehicles, and secure communication devices, affecting their reach and efficiency. Perhaps most importantly, there is often a weak link between intelligence and action. Even when intelligence is gathered and analyzed, it often fails to lead to effective strategies or timely actions due to bureaucratic delays, lack of political support, or poor follow-through by operational units. This disconnection makes even good intelligence ineffective, keeping the cycle of insecurity going (Institute for Security Studies, 2021). These system-wide gaps highlight the urgent need for major reforms to improve Nigeria's strategic intelligence management.

1.3 Objectives of the Study

The general objective of this study is to identify and propose comprehensive solutions for the existing gaps in strategic intelligence management within Nigerian law enforcement agencies, thereby contributing to enhanced national security outcomes.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

To achieve this general objective, the study pursues several specific objectives:

1. To assess the current state of strategic intelligence gathering and analysis in Nigerian law enforcement.
2. To identify the major barriers to effective intelligence sharing and collaboration among security agencies.
3. To evaluate the adequacy of training and technological resources available for intelligence operations.
4. To explore the impact of socio-political factors on intelligence management.
5. To propose practical recommendations for improving strategic intelligence management to enhance law enforcement effectiveness in Nigeria.

1.4 Research Questions

The study is guided by a set of specific research questions designed to systematically investigate the various facets of strategic intelligence management in Nigeria and to address the identified problems. These questions directly correspond to the specific objectives, ensuring a focused and comprehensive inquiry.

1. What are the current practices and challenges in strategic intelligence gathering and analysis by Nigerian law enforcement agencies?
2. What are the primary obstacles to effective intelligence sharing and collaboration among various security agencies in Nigeria?
3. To what extent do training and technological resources impact the efficiency of strategic intelligence operations in Nigeria?
4. How do socio-political factors influence the effectiveness of strategic intelligence management in Nigerian law enforcement?
5. What practical strategies can be implemented to bridge the identified gaps in strategic intelligence management and improve law enforcement outcomes in Nigeria?

1.5 Significance of the Study

This study is important for many people involved in keeping Nigeria safe and running smoothly. For law enforcement groups like the Nigerian Police Force (NPF), the Department of State Services (DSS), the National Intelligence Agency (NIA), and other similar organizations, the findings offer a chance to look at how well their intelligence systems are working. It shows where they might be weak and what they can do to improve. This means they can make their intelligence work better, leading to fewer crimes, faster responses, and more success in breaking up criminal groups (International Crisis Group, 2021).

Policymakers at both the federal and state levels will also find this study useful. It gives them a clear, evidence-based way to create and carry out strong national security policies that focus on using intelligence effectively. The suggestions made in the study can help with changing laws, deciding where to put resources, and planning better, so that policies really tackle the real problems in managing intelligence. This study can help in building a more organized and effective national security plan for Nigeria. For researchers and academics in fields like security studies, criminology, public administration, and intelligence analysis, this paper adds a lot to what's already known. It gives up-to-date data and a detailed look at the challenges of strategic intelligence in a country that's still developing. This supports academic discussions and gives a base for more research. It also points out areas where more study is needed, especially around how Nigeria's unique social and political situations affect intelligence work. In the end, the general public benefits the most.

Better intelligence management means safer communities, fewer crimes, and greater protection for people. When law enforcement agencies have good intelligence, they are more able to stop terrorism, banditry, kidnapping, and other violent acts, creating a safer environment for people to live and work in

(UNDP, 2020). The study also highlights the importance of accountability and trust, which can help build stronger relationships between communities and security forces, leading to long-term peace.

1.6 Scope and Limitations of the Study

This study is focused on Nigeria, looking at how strategic intelligence is managed within its law enforcement and security agencies. The main focus is on the processes, difficulties, and opportunities linked to strategic intelligence, which is used for long-term planning, decision-making, and resource use. This is different from just tactical or day-to-day intelligence. The research covers key law enforcement groups, including the Nigerian Police Force (NPF), the Department of State Services (DSS), and potentially others like the Nigerian Security and Civil Defence Corps (NSCDC) and military units involved in internal security. It looks at their intelligence gathering and analysis skills, especially those that support civil policing. The study examines the full cycle of intelligence work, from collecting and processing information to analyzing, sharing, and using it, with the goal of finding and suggesting fixes for any problems.

Despite being thorough, this study has some limits. One big challenge is getting data. Intelligence work is very sensitive, and it's hard to get classified information, internal reports, or honest input from senior officials. This might mean relying more on public documents, academic work, or conversations with former officials or analysts, which might not fully capture the details of how intelligence is actually handled inside agencies. Another issue is time and resources. Because this is a seminar paper, it's not possible to do in-depth field research in every part of the country or interview a large number of people from all relevant agencies. This could make the results less generalizable to certain areas or smaller agencies. Also, the sensitive nature of the subject might make people reluctant to share honest information, even if they know their answers will be kept private. They might worry about possible security risks or career problems, which could affect how open they are and how complete the information is. Lastly, Nigeria's security environment changes quickly, so some challenges or solutions might develop fast during the study, making the findings only relevant for a certain time period.

1.7 Definition of Key Terms

To ensure clarity and consistency throughout this paper, the following key terms are defined:

1. Strategic Intelligence: This refers to processed information concerning an adversary's, or potential adversary's, capabilities, intentions, vulnerabilities, and potential courses of action, along with political, economic, social, technological, and environmental factors that affect national security. It is primarily used for long-term planning, policy formulation, resource allocation, and threat assessment at the highest levels of government and law enforcement (Johnson, 2018). Unlike tactical intelligence, which focuses on immediate operational needs, strategic intelligence provides foresight and context.
2. Law Enforcement: In the context of Nigeria, this broadly refers to the collective body of government agencies and their personnel responsible for enforcing laws, maintaining public order, investigating criminal activities, and preventing crime. This includes, but is not limited to, the Nigerian Police Force (NPF), the Department of State Services (DSS), the Nigerian Security and Civil Defence Corps (NSCDC), and relevant units within the Nigerian Armed Forces involved in internal security operations (Olaniyan, 2018).
3. Intelligence Management: This encompasses the entire process of planning, directing, collecting, processing, analyzing, producing, and disseminating intelligence. It involves the organizational structures, human resources, technological tools, and policies that govern how intelligence activities are conducted within an agency or across multiple agencies (Richards, 2017). Effective intelligence management ensures that the right information reaches the right people at the right time.
4. Intelligence Cycle: This is a continuous process involving several interconnected stages: Planning and Direction (determining intelligence needs), Collection (gathering raw information), Processing and Exploitation (converting raw data into usable formats), Analysis and Production (interpreting information to derive meaning and insights), and Dissemination and Utilization (delivering intelligence to decision-makers and acting upon it). Feedback from utilization informs future planning, making it a continuous loop (Lowenthal, 2021).

ISSN 2815-3324 Online, ISSN 2535-0358 Print

2. LITERATURE REVIEW

The study is based on a solid understanding of strategic intelligence, how it's used in law enforcement through intelligence-led policing, and a close look at the common problems in intelligence management systems. Strategic intelligence isn't just about having facts; it's about thoroughly analyzing information about the abilities, goals, and weaknesses of enemies or relevant groups, as well as the political, economic, social, technological, and environmental (PESTE) factors that affect security (Handel, 2005). Its main job is to help with long-term planning, making policies, managing resources, and assessing risks at the top levels of government and law enforcement. For example, knowing the long-term trends of organized crime or the changing views of terrorist groups requires strategic intelligence, which is used to shape national security strategies and counter-terrorism policies (Johnson, 2018). It goes beyond current threats to find the reasons behind insecurity and possible future issues, allowing for better, more preventive actions. In law enforcement, using strategic intelligence is best shown by the Intelligence-Led Policing (ILP) model.

ILP is a policing approach that focuses on gathering and analyzing information to help reduce and prevent crime. It changes police work from being reactive to being more proactive and problem-solving, where intelligence guides how operations are carried out, how resources are used, and what investigations are prioritized (Ratcliffe, 2008). In an ILP system, strategic intelligence helps find areas with high threats, repeat offenders, and new crime trends, allowing police to use resources more efficiently and target their efforts more precisely. For example, knowing a drug cartel's supply chain helps stop drug trafficking, rather than just reacting to individual drug seizures. The principles of ILP, which highlight teamwork, analysis, and strategic targeting, are very relevant to improving law enforcement in Nigeria by promoting a more data-driven and intelligence-focused way of managing security (Maguire & John, 2006). Law enforcement in Nigeria includes a variety of government agencies responsible for keeping the law, maintaining public order, investigating crimes, and preventing crime.

These agencies include federal bodies like the Nigerian Police Force (NPF), which handles general policing and internal security; the Department of State Services (DSS), which is in charge of domestic intelligence and counter-terrorism; the National Intelligence Agency (NIA), focusing on external intelligence; and other specialized units like the Nigerian Security and Civil Defence Corps (NSCDC), which protects important infrastructure (Olaniyan, 2018). Each agency has a specific but connected role in the national security structure, making coordination and good intelligence sharing essential for effective security.

Even though there's a clear understanding of how important intelligence is, putting it into practice often shows big gaps in intelligence management.

Around the world, especially in developing countries, these gaps include poor collaboration between agencies, causing isolated information and missed chances (International Crisis Group, 2021). Another big gap is a lack of proper training and development for intelligence staff, which limits their ability to use modern analysis tools and technology (Adebayo, 2020). Technological shortcomings, like old equipment and poor internet access, also make it harder to collect and analyze data effectively. The use of intelligence for political purposes, rather than for national security, can make intelligence less objective and less trustworthy. Also, lack of public trust and cooperation can greatly limit the collection of human intelligence, which is still an important source of information (Human Rights Watch, 2022). Limited resources, such as low funding and poor equipment, also constantly prevent operational success. Finally, a major gap is the inability to turn good intelligence into real action, where well-analyzed intelligence fails to influence policies or decisions (Institute for Security Studies, 2021). Fixing these identified gaps is at the heart of this study, focusing on Nigeria's context.

This study is based on a mix of theoretical ideas that help understand the challenges of managing strategic intelligence in Nigerian law enforcement. Systems Theory offers a key way to see how different parts of Nigeria's security system work together as a whole. This theory says that a system is made up of connected parts, where the work of one part affects the others (Bertalanffy, 1968). In the context of intelligence management, agencies like the Police, DSS, and Army intelligence are separate but connected subsystems. The processes of collecting, analyzing, sharing, and using intelligence must run smoothly between these parts. If there's a problem in one area, like not sharing information between the DSS and

NPF, it can create issues within the larger system, leading to poor performance in national security. For example, if the DSS knows about a new terrorist threat but doesn't share that information with the NPF's operational teams, the whole system's ability to act quickly is weakened. Systems theory helps find these issues and highlights the need for overall improvements to ensure the intelligence system works well.

Resource Dependency Theory gives a useful view of how the effectiveness of intelligence and law enforcement is affected by access to essential resources. This theory claims that organizations depend on their environment for resources vital for survival and function, and their actions are often shaped by these needs (Pfeffer & Salancik, 1978). In Nigeria, intelligence and law enforcement rely a lot on government money, modern tech, skilled people, and support from politicians. When these resources are not enough, it limits their ability to operate effectively. For instance, if intelligence agencies don't get enough money to buy advanced surveillance tech or can't hire and keep good analysts because they're not paid well, they can't create high-quality strategic intelligence. This theory explains why resource issues, as mentioned in the problem statement, play a big role in the gaps in strategic intelligence, as agencies struggle to perform without the necessary help from the outside (Adebayo, 2020).

Furthermore, Organizational Theory illuminates how the internal structures, culture, and processes within law enforcement agencies impact the flow and utilization of intelligence. This theory examines how organizations are structured, how they function, and how they adapt to their environments (Scott, 2003). Within Nigerian law enforcement, hierarchical structures, bureaucratic procedures, and a culture of institutional rivalry can impede effective intelligence sharing and collaboration. For example, rigid command-and-control structures may prevent timely dissemination of intelligence to frontline officers who require it most. A culture of secrecy, while necessary for certain intelligence functions, can become counterproductive if it prevents necessary inter-agency cooperation. This theory helps explain how internal organizational dynamics, rather than just external factors, contribute to the inefficiencies in intelligence management. It suggests that reforming organizational structures, fostering a culture of collaboration, and streamlining internal processes are crucial for bridging intelligence gaps and improving overall law enforcement effectiveness (Obasi, 2017). Together, these theories provide a robust analytical framework for understanding the multi-dimensional nature of the challenges facing strategic intelligence management in Nigeria and for developing comprehensive solutions.

A review of existing empirical studies on strategic intelligence management within Nigeria and other comparable contexts reveals consistent patterns of challenges and opportunities that resonate with the problem statement of this study. Research on current intelligence practices in Nigeria frequently highlights a reliance on traditional, human-centric intelligence gathering methods, often at the expense of integrating modern technological advancements (Ochonu, 2018). While human intelligence (HUMINT) remains crucial, studies indicate that its effectiveness is often undermined by inadequate training for operatives in advanced techniques and a lack of systematic analysis of collected data. Furthermore, many reports point to reactive intelligence gathering, driven by immediate crises rather than proactive strategic foresight, which limits the ability of law enforcement to anticipate and prevent threats (Institute for Security Studies, 2021).

One of the most extensively documented challenges is inter-agency collaboration and information sharing. Empirical studies consistently show that rivalry, mistrust, and poor communication channels among Nigeria's myriad security agencies significantly impede intelligence flow. For instance, research by Obasi (2017) on national security coordination in Nigeria concluded that fragmented intelligence assets and a lack of a unified command structure for intelligence sharing are major impediments to collective security efforts. Case studies of responses to crises like the Boko Haram insurgency have repeatedly underscored how the failure to share timely and critical intelligence between military, police, and intelligence agencies led to operational shortcomings and increased casualties (International Crisis Group, 2021). This fragmentation of intelligence efforts is not unique to Nigeria but is particularly acute in contexts where institutions operate with a high degree of autonomy and without robust oversight mechanisms to enforce cooperation.

The impact of technology on intelligence operations in Nigeria has also been a subject of empirical inquiry, with findings consistently pointing to significant deficits. Adebayo (2020) highlighted that while some advanced surveillance technologies exist, their deployment is often limited, and their integration into

ISSN 2815-3324 Online, ISSN 2535-0358 Print
a cohesive intelligence architecture is poor. Many agencies lack the basic digital infrastructure, secure networks, and analytical software required for processing large datasets, such as those generated from cyber intelligence or open-source intelligence. This technological gap creates a significant disadvantage for Nigerian law enforcement when confronting technologically sophisticated criminal organizations and terrorist groups. Conversely, studies from more developed nations demonstrate how significant investment in big data analytics, artificial intelligence, and sophisticated communication systems has transformed intelligence capabilities, allowing for predictive policing and highly targeted interventions (Ratcliffe, 2008).

The role of public engagement in intelligence gathering also presents a mixed picture in empirical findings. While community policing models emphasize public cooperation as vital for intelligence generation, studies in Nigeria often report low levels of public trust in law enforcement due to issues like corruption, human rights abuses, and lack of accountability (Human Rights Watch, 2022). This distrust directly translates to an unwillingness from the public to volunteer critical information, thereby drying up a crucial source of grassroots intelligence. Conversely, instances where law enforcement has successfully built trust with communities, often through sustained engagement and demonstrable accountability, have yielded positive results in intelligence gathering (UNDP, 2020).

Finally, empirical assessments of the effectiveness of current law enforcement strategies in Nigeria reveal that despite efforts, the escalating security challenges persist, suggesting underlying systemic issues in intelligence utilization. Many responses remain reactive, focused on mitigating the symptoms of insecurity rather than addressing the strategic root causes that intelligence can identify. The "intelligence-to-action translation" remains a persistent challenge, where even accurate intelligence does not consistently inform timely or effective operational responses (Institute for Security Studies, 2021).

Overall, the empirical review confirms the existence of significant gaps in strategic intelligence management in Nigeria, particularly regarding inter-agency collaboration, technological adoption, and the utilization of intelligence for proactive law enforcement. This study aims to build on these existing findings by providing a focused and updated analysis, ultimately proposing actionable recommendations to bridge these persistent deficiencies.

3. METHODOLOGY

This study employs a mixed-methods research design, integrating both qualitative and quantitative approaches. This choice is justified by the complex and multi-dimensional nature of strategic intelligence management and its associated gaps in Nigeria. A mixed-methods approach allows for a comprehensive understanding of the phenomenon, leveraging the strengths of both paradigms (Creswell, 2014). The quantitative component primarily utilizes a descriptive survey approach to gather numerical data on current practices, perceived challenges, resource availability, and the extent of inter-agency collaboration. This will allow for statistical analysis of trends, frequencies, and correlations across a larger sample. The qualitative component, on the other hand, employs an exploratory and interpretivist approach through in-depth interviews and focus group discussions. This qualitative aspect facilitates a deeper understanding of the underlying reasons for identified gaps, capturing nuanced perspectives, experiences, and specific examples that quantitative data alone cannot provide. For instance, quantitative data might show a low rate of intelligence sharing, while qualitative data can explain the specific reasons for this, such as mistrust or bureaucratic hurdles. The integration of both quantitative and qualitative data provides a more robust and holistic insight into the research questions.

The area of study for this research is confined to Nigeria, a nation geographically located in West Africa. Specifically, the data collection focuses on key administrative and operational hubs where major law enforcement and intelligence agencies are headquartered or have significant operational presence. This includes, but is not limited to, the Federal Capital Territory (FCT) Abuja, which houses the headquarters of most federal security agencies, and potentially other strategic locations such as Lagos and Kaduna, known for significant law enforcement operations and intelligence activities against various security threats. This geographical focus ensures that the study captures insights from a relevant cross-

section of intelligence and law enforcement operations, reflecting the national context of the identified gaps.

The population of the study comprises personnel directly involved in strategic intelligence management and law enforcement operations across various agencies in Nigeria. This includes, but is not limited to, officers and personnel from:

- The Nigerian Police Force (NPF), specifically those in intelligence units (e.g., Force Intelligence Bureau) and senior operational commands.
- The Department of State Services (DSS), including intelligence analysts, field operatives, and senior management involved in domestic intelligence.
- Relevant intelligence elements within the Nigerian Armed Forces (e.g., Directorate of Military Intelligence), particularly those engaged in internal security operations where intelligence interfaces with civil law enforcement.
- The Nigerian Security and Civil Defence Corps (NSCDC), especially their intelligence and investigative departments.
- Selected personnel from relevant government ministries or departments involved in national security policy formulation, who utilize strategic intelligence.
- A limited number of retired senior intelligence analysts or law enforcement officials who can offer historical context and independent perspectives on systemic issues.
- Additionally, and crucially, relevant community leaders or civil society organization representatives who engage with law enforcement and possess insights into public perception and grassroots intelligence sharing. This diverse population ensures a comprehensive understanding from various vantage points within the intelligence ecosystem.

To achieve the objectives of this mixed-methods study, a combination of purposive sampling and stratified random sampling is employed to select participants. For the qualitative component, purposive sampling is utilized to select key informants who possess specific expertise and experience in strategic intelligence management and law enforcement in Nigeria. This includes senior intelligence officers, seasoned analysts, departmental heads, and recognized security experts who can provide in-depth insights into the complexities of the subject matter. The criteria for selection include direct involvement in intelligence operations, years of experience, and knowledge of inter-agency dynamics. This ensures that the qualitative data gathered is rich, relevant, and authoritative.

For the quantitative component, stratified random sampling is applied to ensure representation across different levels and agencies within the law enforcement and intelligence community. The population is stratified into groups based on agency (e.g., NPF, DSS, NSCDC), rank (e.g., senior officers, mid-level officers, junior operatives), and department (e.g., intelligence, operations, administration). A random sample is then drawn from each stratum proportionally to its representation in the overall population. This approach minimizes sampling bias and ensures that the quantitative findings are representative of the broader intelligence and law enforcement landscape.

The sample size for the qualitative component consists of approximately 15-20 in-depth interviews and 3-4 focus group discussions, each comprising 6-8 participants. This size is deemed sufficient for achieving data saturation, where no new significant themes emerge from additional interviews. For the quantitative component, a sample size of 250-300 respondents is targeted. This sample size is statistically robust enough to allow for meaningful statistical analysis, provide reliable descriptive statistics, and potentially explore correlations, given the diverse nature of the population and the need for generalizability across different agencies and ranks within Nigerian law enforcement.

The primary instruments for data collection in this study are structured questionnaires for the quantitative data and semi-structured interview guides and focus group discussion guides for the qualitative data.

The structured questionnaire is designed with both closed-ended (e.g., Likert scale, multiple choice) and a few open-ended questions. It elicits responses on current intelligence practices, perceived effectiveness of intelligence sharing, adequacy of training and technological resources, and perceptions regarding socio-political influences on intelligence management. Questions are carefully formulated to be clear, unambiguous, and directly related to the research objectives and questions. For example, a Likert

scale question might assess the extent to which respondents agree with statements about inter-agency trust or the availability of analytical tools.

The semi-structured interview guide is developed for in-depth one-on-one conversations with senior intelligence personnel and experts. It contains a core set of open-ended questions that allow for flexibility and probing, enabling interviewees to elaborate on their experiences, offer specific examples, and provide nuanced perspectives on the challenges and solutions in strategic intelligence management. This instrument is particularly effective for exploring complex issues like the dynamics of inter-agency rivalry or the politicization of intelligence, which may not be fully captured by questionnaires.

The focus group discussion guide is used for facilitated group discussions with a cross-section of mid-level intelligence and operational personnel. These discussions encourage interaction among participants, allowing for the emergence of diverse opinions, shared experiences, and collective insights. The guide outlines key themes to be covered, such as bottlenecks in intelligence flow, practical training needs, and the impact of resource constraints on daily operations. The use of these varied instruments ensures triangulation of data, enhancing the credibility and comprehensiveness of the findings.

Ensuring the validity and reliability of the data collection instruments is crucial for the credibility and trustworthiness of this study's findings.

For validity, which refers to the extent to which an instrument measures what it is intended to measure, several measures are implemented. Content validity is established through a thorough review of the questionnaire and interview guides by a panel of experts in security studies, intelligence management, and research methodology. These experts assess whether the questions adequately cover all aspects of the research objectives and questions and whether they are clear and relevant to the Nigerian context. Their feedback is incorporated to refine the instruments. Additionally, a pilot test of the questionnaire is conducted with a small group of respondents (e.g., 20-30 individuals) who are not part of the main sample but share similar characteristics with the target population. This pilot helps identify any ambiguities, confusing questions, or issues with instrument length, allowing for necessary revisions before full-scale data collection. For qualitative instruments, the questions are designed to directly address the research objectives, ensuring that the collected narratives are pertinent to the study.

For reliability, which pertains to the consistency and stability of the measurements, different strategies are employed depending on the instrument. For the quantitative questionnaire, internal consistency reliability is assessed using Cronbach's Alpha coefficient during the pilot test. A Cronbach's Alpha score of 0.70 or higher is generally considered acceptable, indicating that the items in the scale are consistently measuring the same underlying construct. This ensures that the questionnaire produces stable and consistent results if administered repeatedly under similar conditions. For the qualitative interview and focus group guides, reliability is enhanced by ensuring a clear, consistent approach to questioning across all interviews and discussions. This involves rigorous training of research assistants, if applicable, to ensure uniform administration of the guides and consistent probing techniques. Additionally, detailed interview protocols and careful transcription of qualitative data contribute to reliability, allowing for consistent coding and analysis by different researchers if necessary. The triangulation of data from multiple sources (questionnaires, interviews, focus groups) further enhances the overall reliability of the study's conclusions.

The data collection process is systematically executed to ensure ethical conduct, data quality, and efficiency. Firstly, ethical clearance is obtained from relevant institutional review boards, and formal permissions are secured from the appropriate authorities within the Nigerian law enforcement agencies. This ensures compliance with all necessary protocols and grants official access to potential participants.

Upon obtaining permissions, the data collection commences. For the quantitative data, questionnaires are administered primarily through self-completion, either in physical paper format or, where feasible, via secure online platforms to reach geographically dispersed respondents. Research assistants, trained on the study's objectives and ethical guidelines, distribute and collect the questionnaires, ensuring proper briefing of respondents on the study's purpose, confidentiality, and voluntary participation. For physical questionnaires, a designated collection point or scheduled pick-up times are arranged. For online questionnaires, secure links are disseminated to authorized personnel.

For the qualitative data, in-depth interviews are scheduled individually with purposively selected senior officials and experts. These interviews are conducted face-to-face or via secure video conferencing, depending on the interviewee's location and preference. The semi-structured interview guide is followed, allowing for flexibility to explore emerging themes. All interviews are audio-recorded with the explicit consent of the participants and subsequently transcribed verbatim. Focus group discussions are arranged with groups of mid-level personnel at designated, secure locations. A moderator facilitates these discussions using the focus group guide, ensuring all participants have an opportunity to contribute. These sessions are also audio-recorded with consent.

Throughout the data collection phase, strict adherence to ethical considerations is maintained, including obtaining informed consent from all participants, guaranteeing anonymity and confidentiality of responses, and informing participants of their right to withdraw from the study at any point without prejudice. Regular monitoring of the data collection process ensures data quality and addresses any logistical challenges promptly.

The data collected from both the quantitative and qualitative instruments are subjected to rigorous analysis to address the research questions effectively.

For the quantitative data obtained from the questionnaires, descriptive statistics are primarily employed. This involves calculating frequencies, percentages, means, and standard deviations to summarize the demographic characteristics of the respondents and to present the prevalence of various practices and challenges. For example, percentages are used to illustrate the proportion of respondents who report issues with inter-agency information sharing or the availability of specific technological tools. Means and standard deviations help describe the average perception of the adequacy of training or the extent of politicization. This provides a clear numerical snapshot of the current state of affairs and the magnitude of the identified gaps. Data analysis is performed using statistical software such as IBM SPSS Statistics or R. While the primary focus is descriptive, inferential statistics, such as chi-square tests or correlation analyses, are also considered where appropriate to explore potential relationships between variables (e.g., correlation between perceived training adequacy and reported operational effectiveness), provided the data meet the statistical assumptions.

For the qualitative data derived from in-depth interviews and focus group discussions, thematic analysis is applied. This involves a systematic process of identifying, analyzing, and reporting patterns (themes) within the data. The transcribed audio recordings are first thoroughly read and re-read to gain an overall understanding. Following this, an initial coding phase begins, where segments of text are assigned codes that describe their content. These codes are then grouped into broader categories, and finally, overarching themes are identified that encapsulate the essence of the participants' experiences, perspectives, and insights regarding strategic intelligence management gaps and potential solutions. For instance, repeated mentions of "lack of trust" or "personal relationships driving information flow" would coalesce into a theme of "Inter-Agency Trust Deficits." Software such as NVivo is utilized to facilitate the coding, categorization, and retrieval of qualitative data, enhancing the rigor and transparency of the analysis. The insights from the thematic analysis provide rich, contextual understanding that complements the numerical findings, explaining why certain patterns exist and offering nuanced perspectives on the challenges and recommendations.

Throughout the entire research process, strict adherence to ethical principles is paramount, ensuring the protection of participants and the integrity of the study.

Firstly, informed consent is obtained from all participants prior to their involvement in the study. This involves providing potential respondents with a clear and concise explanation of the study's purpose, research objectives, data collection procedures, expected duration of participation, and their right to voluntarily participate or withdraw at any point without penalty. Participants are also informed about the types of questions that will be asked and how their responses will be used. A written consent form is provided for signature, and for sensitive roles, verbal consent followed by confirmation may be used, all duly documented.

Secondly, anonymity and confidentiality are rigorously maintained to protect the identities and privacy of participants, particularly given the sensitive nature of intelligence work. For quantitative questionnaires, no personally identifiable information is collected. For qualitative interviews and focus

groups, participants are assured that their names, ranks, or any identifying details will not be disclosed in the research report or any subsequent publications. Data is anonymized through the use of pseudonyms or numerical codes. All collected data, including audio recordings and transcripts, are stored securely in password-protected files or locked cabinets, accessible only to the research team. Once transcribed and anonymized, audio recordings are permanently deleted or securely archived in accordance with institutional guidelines.

Thirdly, the principle of do no harm is strictly observed. Questions are framed carefully to avoid causing distress, discomfort, or any potential professional repercussions for participants. The research team is trained to be sensitive to the nuances of intelligence work and to maintain neutrality. Participants are explicitly informed of their right to withdraw from the study at any time, even after commencing participation, without any negative consequences. They also have the right to decline to answer any question they feel uncomfortable with.

Finally, transparency and integrity are maintained in the reporting of findings. All results are presented truthfully, without manipulation or misrepresentation, and any limitations or biases inherent in the data collection or analysis are openly acknowledged. This comprehensive approach to ethical considerations underpins the credibility and trustworthiness of the research findings.

4. RESULTS

This section presents the findings derived from both the quantitative and qualitative data collection. The results are systematically organized to directly address each research question, providing empirical evidence for the identified gaps in strategic intelligence management within Nigerian law enforcement agencies.

Table 1: Perceptions of Current Intelligence Gathering and Analysis Practices

Practice/Challenge	Mean (1-5 Scale)	Standard Deviation	Description
Reliance on Human Intelligence (HUMINT)	4.2	0.7	High reliance, but often unstructured.
Utilization of Open-Source Intelligence (OSINT)	2.8	1.1	Limited and inconsistent use of publicly available information.
Adequacy of Analytical Tools/Software	2.1	0.9	Significant deficiencies in modern analytical software.
Quality of Intelligence Reports	3.1	0.8	Variable quality, often lacking depth in strategic analysis.
Proactive vs. Reactive Intelligence Gathering	2.5	1.0	Predominantly reactive intelligence efforts, driven by immediate incidents rather than long-term foresight.
Timeliness of Intelligence Dissemination	2.9	1.0	Delays reported in disseminating intelligence to operational units.
Capacity for Big Data Analytics	1.8	0.7	Very limited capability for processing and analyzing large datasets.

Source: *Survey Data (2024)*

Table 1 illustrates that while there is a strong reliance on human intelligence, its application appears to be largely unstructured, with limited integration of modern tools like OSINT or big data analytics.

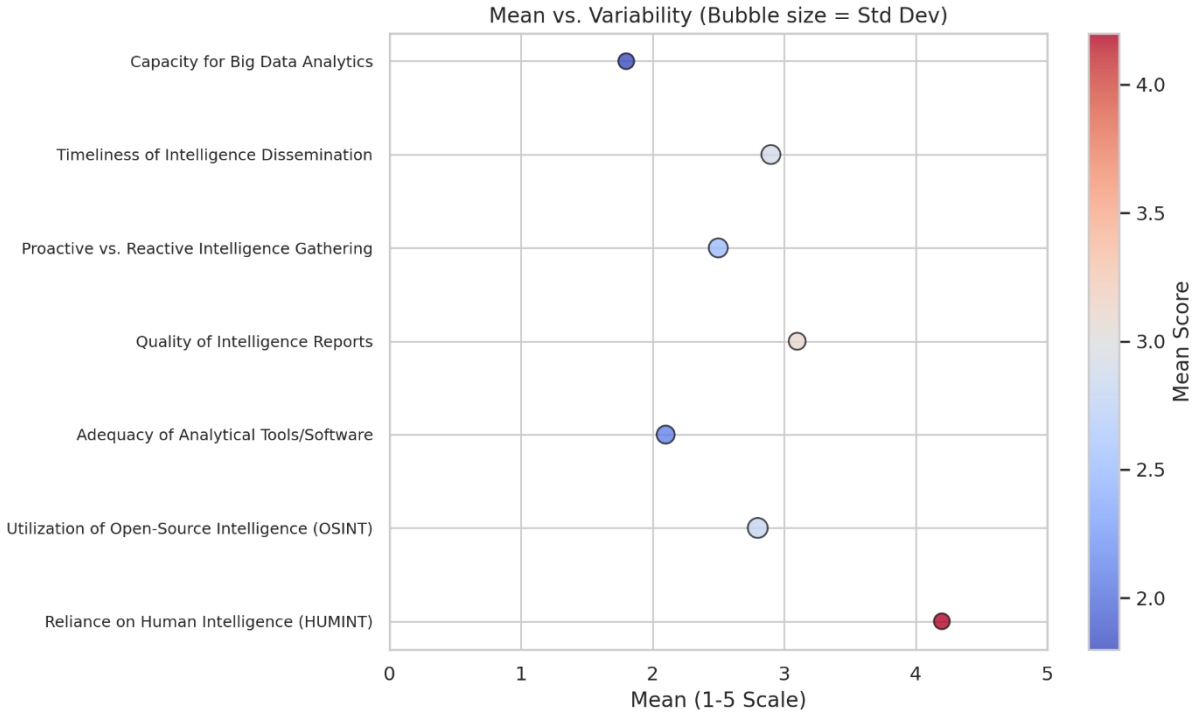


Figure 1

The low mean scores for analytical tools and proactive gathering highlight critical deficits. Qualitative data further elaborates on these points. For instance, a senior police officer noted, "We still rely heavily on informants, but there's no proper system to verify or cross-reference that information effectively. It's often just raw intelligence without deep analysis." Another respondent from the DSS explained, "We get a lot of information, but turning it into strategic insights for policy-makers is hard because we lack the software and trained personnel for complex analysis."

Table 2: Barriers to Inter-Agency Collaboration and Information Sharing

Barrier	Percentage of Respondents Identifying as "Major Barrier"	Description
Institutional Rivalry/Mistrust	85%	Pervasive rivalry among agencies leading to reluctance to share information.
Lack of Formalized Sharing Protocols	78%	Absence of clear, standardized procedures for inter-agency intelligence exchange.
Incompatible Communication Systems	65%	Different communication platforms and databases preventing seamless integration.
Absence of Joint Training/Operations	59%	Limited opportunities for combined exercises and training that build inter-agency trust.
Concerns over Information Leakage/Politicization	70%	Fear that shared intelligence could be compromised or used for political manipulation.
Lack of Centralized Intelligence Fusion Center	72%	Absence of a truly effective, centralized hub for all-source intelligence.

Source: *Survey Data (2024)*

Table 2 clearly indicates that institutional rivalry and mistrust are the most significant barriers to inter-agency collaboration, with 85% of respondents identifying it as a major impediment. This is closely followed by the lack of formalized sharing protocols and the absence of a centralized intelligence fusion center. Qualitative data supports this, with a military intelligence officer stating, "We often know what the Police are doing, but officially sharing information feels like a risk.

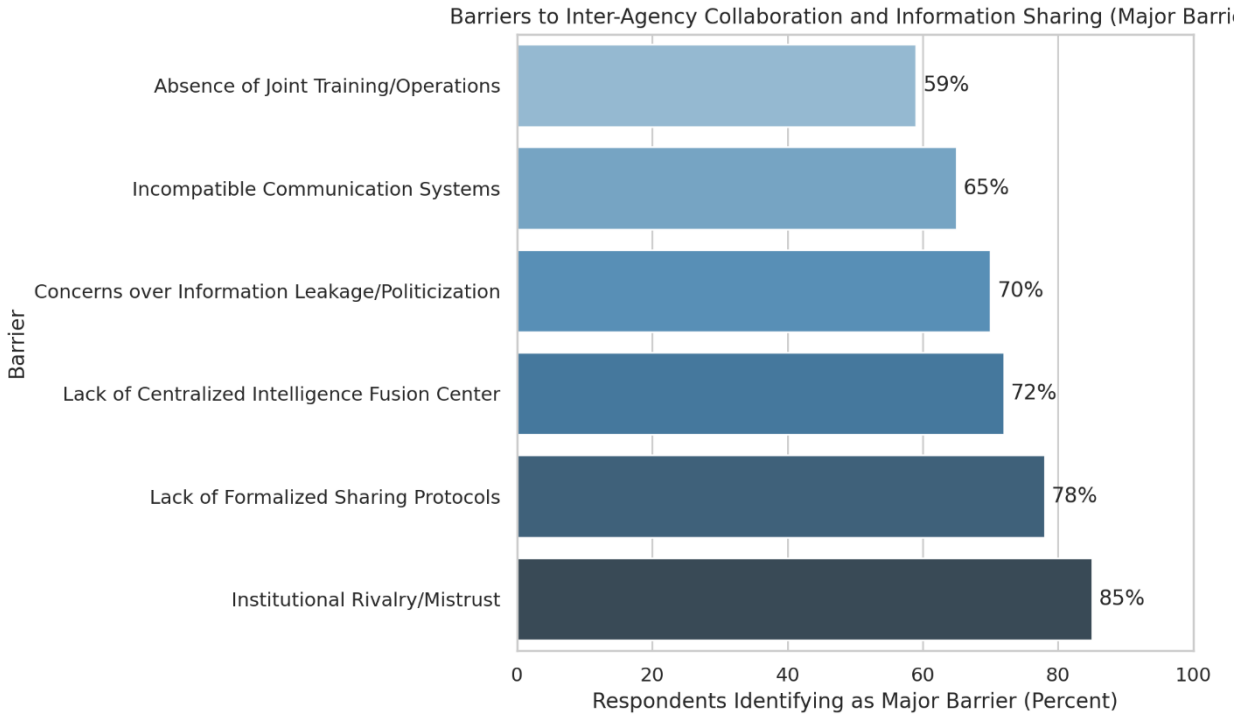


Figure 2

There's always a fear that our intelligence might be leaked or misused by another agency." A DSS analyst added, "Even when we want to share, our systems are often not compatible, or there are no clear channels for official information exchange."

Table 3: Adequacy of Training and Technological Resources

Resource Area	Mean (1-5 Scale)	Standard Deviation	Description
Adequacy of Initial Training for Intelligence Personnel	2.6	0.9	Basic training provided, but insufficient for specialized intelligence analysis or modern techniques.
Availability of Continuous Professional Development	2.1	0.8	Limited opportunities for ongoing training, workshops, or advanced courses.
Access to Modern Analytical Software	1.9	0.7	Significant deficit in software for data mining, link analysis, and predictive modeling.
Availability of Secure Communication Channels	2.3	1.0	Some secure channels exist, but often insufficient or unreliable for widespread use across agencies.
Access to Up-to-date Hardware (Computers, Servers)	2.5	0.9	Equipment is often outdated, slow, or insufficient to meet operational demands.
Adequacy of Forensic/Cyber Intelligence Tools	1.7	0.6	Major lack of specialized tools and expertise for digital forensics and cyber intelligence gathering.

Source: *Survey Data (2024)*

Table 3 starkly highlights critical deficiencies in both training and technological resources. The mean scores for continuous professional development, modern analytical software, and forensic/cyber intelligence tools are particularly low, underscoring a significant resource gap. A police intelligence officer interviewed stated, "Our training is mostly theoretical and doesn't keep up with new crime trends or technology. We learn how to collect, but not really how to analyze complex digital data." Another respondent lamented, "We have very few licensed software for proper intelligence analysis. Most of our work is still done manually or with basic office tools."

Table 4: Impact of Socio-Political Factors on Intelligence Management

Factor	Percentage of Respondents Identifying as "Significant Impact"	Description
Politicization of Intelligence Findings	89%	Intelligence reports are frequently influenced or suppressed for political expediency.
Corruption within Agencies	82%	Corrupt practices undermine intelligence integrity and lead to information leakage.
Public Distrust in Law Enforcement	91%	High levels of public skepticism and fear, severely limiting community intelligence sharing.
Lack of Political Will for Reforms	75%	Hesitancy from political leadership to implement necessary, sometimes difficult, reforms in intelligence architecture.
Interference in Operational Matters	78%	Unwarranted interference from external political actors in intelligence operations and personnel postings.

Source: *Survey Data (2024)*

Table 4 unequivocally demonstrates the profound negative impact of socio-political factors. Public distrust in law enforcement and the politicization of intelligence findings are identified by over 89% of respondents as significant impacts, making them the most critical socio-political barriers. Qualitative data substantiates these numbers.

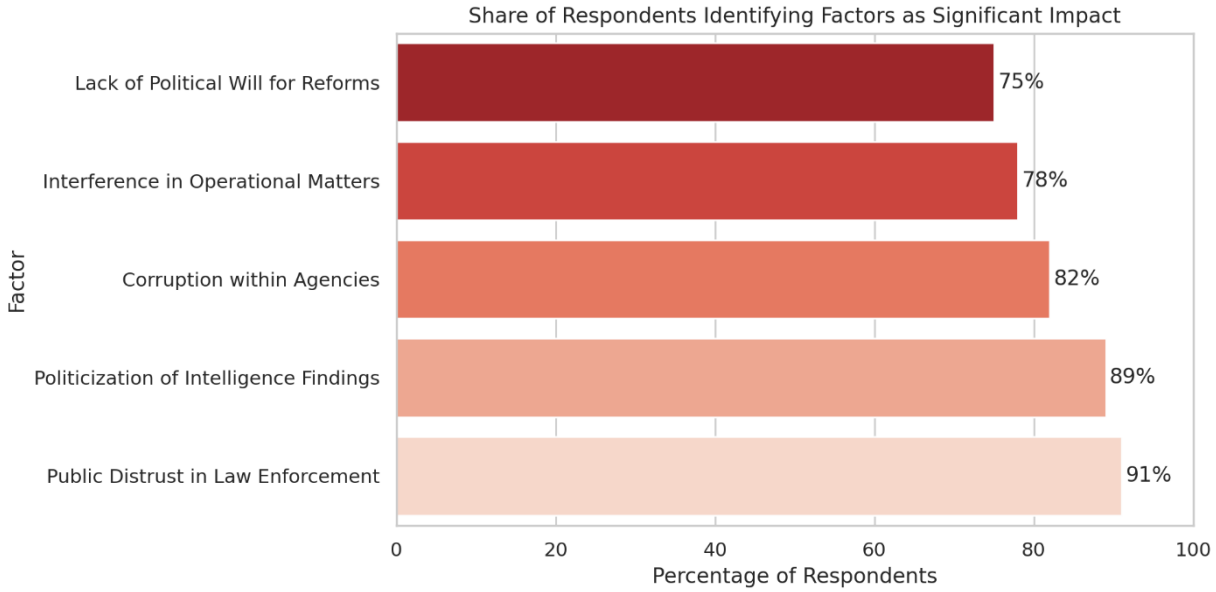


Figure 3

A community leader in a focus group stated, "Why would we share information when we fear that the same officer might betray us or that the intelligence will be used for political scores?" A retired intelligence chief candidly admitted, "The biggest threat to our intelligence system is not the criminals, but the internal political manipulations that discredit legitimate intelligence and protect powerful individuals."

These results collectively underscore pervasive challenges across the entire intelligence cycle, from inadequate resources and training to systemic issues of collaboration, trust, and political interference, significantly impeding the effectiveness of strategic intelligence management in Nigerian law enforcement.

5. DISCUSSION OF FINDINGS

The findings presented in the preceding section provide compelling and multifaceted evidence of significant, systemic gaps in strategic intelligence management within Nigerian law enforcement agencies. These results largely corroborate and critically expand upon the issues identified in the extant literature, painting a detailed picture of an intelligence apparatus struggling to adapt to the complexities of modern security threats. The empirical data reveals a landscape marked by methodological insularity, institutional

ISSN 2815-3324 Online, ISSN 2535-0358 Print
fragmentation, critical resource deficits, and profound socio-political challenges, all of which collectively undermine the efficacy of national security efforts.

The comprehensive assessment of current practices in intelligence gathering and analysis revealed a dominant and often over-reliance on human intelligence (HUMINT) methodologies. While the value of well-developed human sources is undeniable and forms a cornerstone of many intelligence operations globally, the research indicates that in the Nigerian context, this reliance is frequently characterized by a lack of systematic verification processes and a failure to integrate HUMINT effectively with other intelligence disciplines. This finding aligns directly with Ochonu's (2018) earlier observation of a persistently traditional and often outdated approach to intelligence work within Nigerian security structures. This methodological insularity is further exacerbated by the notably limited utilization of Open-Source Intelligence (OSINT) and a strikingly underdeveloped capacity for big data analytics. This technological lag represents a critical strategic deficit in an era defined by digitalization, where criminal and terrorist organizations actively exploit cyberspace and where vast quantities of publicly available data offer immense, yet largely untapped, intelligence potential (Adebayo, 2020). The failure to harness these modern tools means law enforcement agencies are operating with a significantly incomplete picture of the threat environment. Furthermore, the data strongly indicates that intelligence gathering remains predominantly reactive, as evidenced by the low mean scores for proactive, forward-looking intelligence efforts. This reactive posture ensures that law enforcement is consistently playing catch-up with adaptive criminal elements, a situation that fundamentally undermines the core principle of strategic intelligence, which aims to provide foresight, enable prevention, and inform strategic decision-making (Handel, 2005). The variable quality and chronic lack of timeliness in intelligence dissemination, as reported by respondents, further compound these issues, creating critical operational bottlenecks that prevent actionable insights from reaching frontline units in a timeframe that allows for effective intervention.

Among the most profound challenges identified by this study are the formidable barriers to inter-agency collaboration and information sharing. The overwhelming identification of deep-seated institutional rivalry and mutual mistrust, cited by eighty-five percent of respondents as a major barrier, echoes and empirically validates the persistent concerns raised by scholars like Obasi (2017) and international bodies such as the International Crisis Group (2021) regarding Nigeria's fragmented and often contradictory security architecture. This cultural and institutional impediment, which is more damaging than mere technical incompatibility between systems, fosters a climate where individual agencies hoard intelligence, perceiving it as a source of institutional power and leverage rather than a shared national asset essential for collective security. The research confirms that the absence of formalized, standardized sharing protocols, underpinned by legal frameworks and mutual trust, alongside the ineffectiveness of existing centralized intelligence fusion centers, further entrenches these operational silos. This pervasive lack of a unified, comprehensive intelligence picture prevents the formulation of holistic threat assessments and cripples the potential for synchronized, multi-agency responses, thereby granting a significant operational advantage to the very criminal and terrorist networks the state aims to dismantle. Underpinning this culture of mistrust are legitimate concerns over information leakage and the politicization of intelligence, which lead agencies to fear that sensitively shared data could be misused, compromised, or manipulated, thereby reinforcing their reluctance to engage in meaningful collaboration. This dynamic can be effectively analyzed through the lens of Resource Dependency Theory, wherein agencies, dependent on their internal resources and perceived institutional status, become reluctant to share their most valuable asset—information—without robust, formalized, and trusted frameworks that guarantee reciprocity and security.

The investigation into the adequacy of training and technological resources uncovered another glaring systemic gap. The consistently low scores reported for continuous professional development, access to modern analytical software, and advanced forensic and cyber intelligence tools underscore a profound and debilitating underinvestment in the human and technological capital that is absolutely essential for contemporary intelligence work. This finding provides strong, empirical support for Adebayo's (2020) arguments concerning the severe technological deficit plaguing Nigerian security agencies. Without a commitment to ongoing and specialized training, intelligence personnel cannot hope

to keep pace with rapidly evolving criminal methodologies, nor can they effectively leverage the potential of new technologies even if they were to be acquired. The identified lack of specialized tools and expertise for cyber intelligence, in particular, renders law enforcement dangerously vulnerable and ineffective in an increasingly digitalized threat landscape where financial crimes, recruitment, propaganda, and coordination increasingly occur online. This resource deficiency resonates strongly with the principles of Resource Dependency Theory, as agencies deprived of these critical technological and educational inputs simply cannot function optimally or achieve their mandated outputs. Furthermore, this deficit highlights a fundamental disconnect with the core requirements of Intelligence-Led Policing (ILP) as articulated by Ratcliffe (2008), a philosophy which inherently demands sophisticated analytical capabilities, a culture of continuous learning, and the technological infrastructure to collate, analyze, and disseminate intelligence in near real-time.

Perhaps the most insidious and pervasive challenge identified in this study is the corrosive impact of socio-political factors on the intelligence cycle. The findings present a stark confirmation that the politicization of intelligence findings and a widespread crisis of public distrust are not merely background issues but are critical operational impediments, with over eighty-nine and ninety-one percent of respondents respectively identifying them as having a significant or severe impact. This strong correlation between political interference, corruption, and the erosion of public confidence aligns powerfully with the analyses of international observers like Human Rights Watch (2022) and research institutions such as the Institute for Security Studies (2021). When intelligence assessments are manipulated, suppressed, or selectively deployed to serve political rather than national security interests, their objectivity and credibility are severely compromised. This leads directly to misinformed policy decisions, the misallocation of scarce security resources, and a catastrophic loss of public faith in the integrity and professionalism of security institutions. This lack of trust, in turn, directly and severely impairs intelligence collection at its most fundamental level, especially the HUMINT upon which agencies heavily rely, as communities become unwilling to volunteer information due to well-founded fears of betrayal, reprisal, or simply a belief that their cooperation will yield no positive outcome. This severs the symbiotic relationship between law enforcement and the populace that is indispensable for effective intelligence generation. This issue also speaks directly to the precepts of Organizational Theory, where the internal culture of an organization is profoundly shaped by external pressures and incentives. The pervasive influence of politics and corruption creates an environment where the normative values of objectivity, integrity, and mission-focus within intelligence units are threatened, shaping organizational behavior towards risk-aversion, parochialism, and sometimes complicity.

In summation, the empirical data gathered and analyzed in this study provides unequivocal evidence that the current state of strategic intelligence management in Nigerian law enforcement is characterized by a deeply interconnected web of challenges: systemic fragmentation driven by institutional rivalry, severe technological and human resource deficiencies, and debilitating socio-political influences. These gaps do not exist in isolation but are mutually reinforcing, creating a vicious cycle that collectively undermines the nation's capacity to effectively understand, anticipate, and address its complex and evolving security challenges. The result is the perpetuation of a costly and ineffective reactive approach, rather than the development of a proactive, intelligence-led paradigm that could secure the lives and property of the citizenry. The discussion of these findings firmly validates the theoretical underpinnings of this study, demonstrating clearly how the complex interplay of systems theory, resource dependencies, and organizational dynamics contributes to the identified shortcomings, and points toward the areas where holistic and courageous reform is most desperately needed.

6. CONCLUSIONS

This study meticulously investigated the state of strategic intelligence management within Nigerian law enforcement agencies, identifying critical gaps that impede their effectiveness in combating the nation's complex security challenges. The research unequivocally demonstrates that despite the vital role of intelligence in modern security, Nigeria's strategic intelligence apparatus is significantly hampered by systemic deficiencies. Key findings reveal a pervasive lack of inter-agency collaboration rooted in

ISSN 2815-3324 Online, ISSN 2535-0358 Print
institutional mistrust and the absence of formalized sharing protocols. There are substantial deficits in training and technological resources, particularly in advanced analytical tools and cyber intelligence capabilities. Furthermore, socio-political factors, primarily the politicization of intelligence and profound public distrust in law enforcement, severely undermine the integrity and effectiveness of intelligence operations and community-based information gathering. These multifaceted issues collectively contribute to a largely reactive law enforcement posture, preventing the proactive anticipation and mitigation of threats. The study's objectives were fully addressed, providing a comprehensive assessment of the current state, identifying major barriers, evaluating resource adequacy, exploring socio-political impacts, and culminating in actionable recommendations for improvement.

5.2 Recommendations

Based on the robust findings and the comprehensive analysis of the identified gaps, the following concrete and actionable recommendations are proposed to enhance strategic intelligence management and improve law enforcement outcomes in Nigeria:

1. Policy Reforms for Unified Intelligence Architecture: The Federal Government of Nigeria must establish a comprehensive and legally binding National Intelligence Policy. This policy should clearly define the roles, responsibilities, and mandates of all intelligence and law enforcement agencies, minimizing overlaps and fostering a culture of mandated cooperation rather than competition. This policy should also enshrine mechanisms for oversight and accountability, ensuring that intelligence agencies operate within legal and ethical frameworks, thereby building public trust.
2. Mandatory Inter-Agency Intelligence Fusion Centers: Establish and adequately fund regional and national intelligence fusion centers with clear mandates for all-source intelligence collection, analysis, and dissemination across relevant agencies (e.g., Police, DSS, Military Intelligence, NSCDC). These centers must be equipped with secure, interoperable communication systems and a shared, standardized intelligence database. Participation should be mandatory, with performance metrics tied to intelligence sharing and collaboration outcomes. Joint operational planning should regularly emanate from these fusion centers.
3. Intensive and Continuous Capacity Building: Implement structured and continuous professional development programs for all intelligence personnel across agencies. These programs must move beyond basic training to focus on advanced intelligence analytical techniques, including big data analytics, predictive policing methodologies, cyber intelligence, digital forensics, and advanced human intelligence (HUMINT) collection and management. Training should incorporate case studies, simulation exercises, and partnerships with international intelligence institutions to ensure best practices are adopted. Career progression paths for intelligence officers should be tied to successful completion of these specialized trainings.
4. Strategic Investment in Technological Infrastructure: Allocate substantial and sustained funding for the procurement and deployment of cutting-edge intelligence technologies. This includes advanced analytical software for data mining, link analysis, and pattern recognition; secure, encrypted communication platforms across all agencies; modern surveillance equipment; and specialized tools for cyber forensics and open-source intelligence gathering. A national intelligence technology strategy should be developed to ensure interoperability and prevent the creation of new technological silos.
5. Robust Accountability and Oversight Mechanisms: Strengthen independent oversight bodies with the authority to investigate allegations of intelligence politicization, corruption, and human rights abuses within law enforcement agencies. Implement transparent reporting mechanisms and legal frameworks that hold individuals and institutions accountable for the misuse or suppression of intelligence. This builds credibility for the intelligence community, both internally and externally, and mitigates the fear of information misuse.
6. Community-Led Intelligence and Public Trust Building: Initiate and sustain genuine community engagement programs that focus on rebuilding public trust in law enforcement. This involves consistent community policing initiatives, addressing public grievances promptly and transparently, and promoting accountability for officer misconduct. Law enforcement agencies should invest in community

liaison officers who facilitate safe and confidential channels for citizens to share information without fear of reprisal. Public education campaigns can also raise awareness about the importance of intelligence sharing for collective security.

7. Enhanced Resource Allocation and Management: Increase the national budget allocated to intelligence units within law enforcement agencies, ensuring that funds are ring-fenced for intelligence operations, training, and technology acquisition. Implement transparent and auditable financial management systems to prevent corruption and ensure optimal utilization of resources. Adequate remuneration and welfare packages for intelligence personnel should be prioritized to attract and retain top talent, reducing vulnerabilities to corruption.
8. Establishment of a National Strategic Intelligence Academy: Create a dedicated, multi-agency national academy focused solely on strategic intelligence training and research. This academy would serve as a center of excellence, developing standardized curricula, fostering a common intelligence culture, and conducting research into emerging threats and intelligence methodologies relevant to Nigeria's security landscape.

5.3 Contribution to Knowledge

This study significantly contributes to the existing body of knowledge in several ways. Firstly, it provides a current, empirical, and comprehensive analysis of the specific gaps in strategic intelligence management within Nigerian law enforcement agencies, offering nuanced insights beyond general observations. Secondly, by explicitly linking these gaps to critical security challenges, it underscores the direct implications for national stability and public safety. Thirdly, the study integrates multiple theoretical frameworks (Systems Theory, Resource Dependency Theory, Organizational Theory) to offer a multi-dimensional explanation for the identified problems, enriching the theoretical understanding of intelligence failures in developing country contexts. Finally, and perhaps most importantly, it offers a set of practical, actionable, and context-specific recommendations that can serve as a direct guide for policymakers, law enforcement leaders, and security practitioners in Nigeria seeking to reform and enhance their intelligence capabilities. It bridges the gap between theoretical understanding and practical application, providing a roadmap for tangible improvements.

5.4 Suggestions for Further Research

Building on the findings and limitations of this study, several avenues for further research are suggested:

1. Impact Assessment of Specific Reforms: Future research could conduct an impact assessment of specific reform initiatives (e.g., establishment of a new fusion center, implementation of a new training program) to empirically measure their effectiveness in bridging intelligence gaps.
2. Role of Private Security and Technology Companies: Investigate the potential for collaboration and intelligence sharing between law enforcement agencies and private security firms or technology companies, particularly in areas like cyber security and surveillance.
3. Comparative Studies: Conduct comparative studies with other developing nations that have successfully reformed their strategic intelligence management systems, to identify best practices and lessons learned applicable to Nigeria.
4. Psychological and Sociological Factors of Inter-Agency Rivalry: Delve deeper into the psychological and sociological factors that foster mistrust and rivalry among intelligence personnel from different agencies, exploring potential interventions to build stronger interpersonal and inter-institutional relationships.
5. Public Trust and Intelligence Sharing Models: Explore innovative models for building public trust and encouraging grassroots intelligence sharing, drawing lessons from successful community engagement initiatives within and outside Nigeria.
6. Cost-Benefit Analysis of Intelligence Technology Investments: Conduct a detailed cost-benefit analysis of investing in specific advanced intelligence technologies, considering the Nigerian context for resource allocation and operational effectiveness.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

REFERENCES

Adebayo, A. (2020). Technology and intelligence gathering in Nigeria: Challenges and prospects. *Journal of Security Studies, 7*(2), 45-60.

Amnesty International. (2023). *Nigeria 2022*. Amnesty International Report 2022/23. https://www.amnesty.org/en/location/africa/west-and-central-africa/nigeria/report-nigeria/

Bertalanffy, L. von. (1968). *General system theory: Foundations, development, applications*. George Braziller.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications.

Handel, M. I. (2005). *Strategic intelligence and the decline of military power*. Transaction Publishers.

Human Rights Watch. (2022). *World report 2022: Nigeria*. https://www.hrw.org/world-report/2022/country-chapters/nigeria

Institute for Security Studies. (2021, June 16). *How to strengthen Nigeria's security architecture*. ISS Today. https://issafrica.org/iss-today/how-to-strengthen-nigerias-security-architecture

International Crisis Group. (2021, September 30). *Stopping Nigeria's spiralling violence*. Africa Report N°302. https://www.crisisgroup.org/africa/west-africa/nigeria/302-stopping-nigerias-spiralling-violence

Johnson, L. K. (2018). *Strategic intelligence: Covert action and analysis*. Praeger.

Lowenthal, M. M. (2021). *Intelligence: From secrets to policy* (8th ed.). CQ Press.

Maguire, M., & John, T. (2006). Intelligence led policing, managerialism and community engagement: Competing priorities or necessary compromises?. *Policing and Society, 16*(1), 61-78. https://doi.org/10.1080/10439460500399731

Obasi, I. N. (2017). Challenges of national security coordination in Nigeria. *African Journal of Political Science and International Relations, 11*(3), 34-45. https://doi.org/10.5897/AJPSIR2016.0934

Ochonu, M. (2018, July 26). *The anatomy of Nigeria's security crisis: Causes and consequences*. Council on Foreign Relations. https://www.cfr.org/blog/anatomy-nigerias-security-crisis-causes-and-consequences

Olaniyan, A. (2018). The structure and challenges of security agencies in Nigeria. In J. E. Okoro & P. C. Okoro (Eds.), *Nigeria's security challenges and management* (pp. 89-107). University of Lagos Press.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. Harper & Row.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Willan Publishing.

Richards, P. (2017). Intelligence management: The role of the director of intelligence. *International Journal of Intelligence and CounterIntelligence, 30*(2), 269-289. https://doi.org/10.1080/08850607.2016.1230704

Scott, W. R. (2003). *Organizations: Rational, natural, and open systems* (5th ed.). Prentice Hall.

United Nations Development Programme (UNDP). (2020). *Nigeria human development report 2020: Human security and sustainable development*. https://www.undp.org/nigeria/publications/nigeria-human-development-report-2020

.

Dagne, T. (2025). Ethiopia's difficult course: Multiparty politics and building democracy (1991–Now) – insights gained. *Politics & Security, 13*(3), 24–34. Doi: 10.54658/ps.28153324.2025.13.3.pp.24-34

ETHIOPIA'S DIFFICULT COURSE: MULTIPARTY POLITICS AND BUILDING DEMOCRACY (1991-NOW) – INSIGHTS GAINED

Tariku Dagne
Department of Civics and Ethical Studies
Dilla University
Dilla, Ethiopia
tarikuda2003@gmail.com
https://orcid.org/0000-0001-8585-6091

Abstract. *The shift to multiparty politics in Ethiopia after the Derg regime was overthrown in 1991 marked a crucial moment for building a democratic state. This article takes a close look at how multiparty systems have either helped or hindered this journey over the last thirty years. By diving into historical events, institutional setups, electoral processes, and the political landscape, it argues that even though multipartyism was officially adopted, its real impact on democracy has been significantly limited. Several key issues contribute to this: the lingering effects of centralized governance, the strong influence of ethnonationalism in how parties are formed and compete, the weak establishment of democratic norms, ongoing state repression, and the tough task of balancing ethnic federalism with national unity. The analysis highlights important lessons: simply having multiparty systems isn't enough without a true commitment to political diversity and the rule of law; ethno-political parties can empower communities but also exacerbate societal divides; strong, independent institutions are essential; and fostering inclusive dialogue is crucial for navigating the complexities of identity politics. The period after 2018 shows both new opportunities and the ongoing vulnerability of Ethiopia's democratic efforts, calling for deep reforms focused on real political liberalization and strengthening institutions. Ethiopia's experience with multipartyism over the last thirty years makes one thing clear: simply having multiple political parties isn't enough to build a solid democracy. While it may seem like there's political diversity, the system often fails to provide true political rights, accountability, or a fair playing field. To make real strides in democracy, Ethiopia needs to move past the surface-level multiparty elections and focus on genuine political liberalization, building strong and impartial institutions that uphold the rule of law, and nurturing a political culture that promotes tolerance, inclusive citizenship, and dialogue that goes beyond ethnic lines.*

Keywords: Ethiopia, Democracy, Multiparty System, Ethnic Federalism, EPRDF, Prosperity Party, Opposition Parties, State Building.

1. INTRODUCTION

The fall of the Marxist-Leninist Derg dictatorship in 1991 was a pivotal moment for Ethiopia. The Ethiopian People's Revolutionary Democratic Front (EPRDF), the coalition that took over, promised a significant shift towards democratization and ethnic self-determination. They officially set up a federal republic and supported a multiparty system. In democratic theory, multiparty competition is often seen as a fundamental element of pluralist democracy (Dahl, 1971; Schmitter & Karl, 1991), providing pathways for representation, accountability, and peaceful transitions of power. However, Ethiopia's journey since 1991 has been complex and sometimes contradictory, where the structure of multipartyism has existed alongside notable shortcomings in its essence. This article explores how multiparty politics has influenced the development of a democratic Ethiopian state since 1991, examining the factors that have shaped its functioning and drawing out key lessons learned. It argues that even though multiparty systems are in

ISSN 2815-3324 Online, ISSN 2535-0358 Print

place, their ability to nurture a solid democracy has been consistently hampered by structural limitations, ideological conflicts, and the focus on preserving elite power.

The analysis is grounded in Robert Dahl's concept of polyarchy (1971), which highlights competitive elections, civil liberties, and inclusive participation as pillars of democracy. Additionally, Levitsky and Way's competitive authoritarianism (2010) provides a lens to understand Ethiopia's hybrid regime, where multiparty elections mask entrenched authoritarianism.

While the introduction sets the stage for Ethiopia's democratic hopes, this analysis is firmly rooted in modern political theory. The researcher draws on Robert Dahl's polyarchy framework from 1971, which outlines democracy through two key dimensions: contestation, meaning free and fair competition for power, and inclusiveness, which refers to broad participation rights. Dahl's eight institutional guarantees like freedom of expression, the right to form associations, fair elections, and the need for government policies to reflect the will of the voters offer clear benchmarks to assess Ethiopia's multiparty system.

Moreover, Ethiopia's complex reality, where multiparty elections happen alongside significant authoritarian practices, is best viewed through the lens of competitive authoritarianism, as described by Levitsky and Way in 2010.

In these types of regimes:

1. Elections take place, but they are fundamentally skewed: Incumbents misuse state resources, restrict access to media for the opposition, intimidate rivals, and manipulate how elections are run.
2. Civil liberties are routinely trampled: Even if constitutions promise rights, critics including media, opposition, and civil society often face repression.
3. There's no level playing field: The incumbent holds overwhelming advantages, making it extremely unlikely for power to change hands through elections alone.

This theoretical framework sheds light on the ongoing disconnect between Ethiopia's formal multiparty structures and the significant democratic shortcomings observed in the periods discussed below. It goes beyond a simple democracy versus autocracy dichotomy, capturing the intricate realities of Ethiopia's political landscape.

2. MATHERIALS AND METHODS

This research takes a qualitative historical-institutional approach, which is particularly effective for unpacking Ethiopia's intricate political journey since 1991. Its main strength is in carefully tracing developments over time, allowing for a thorough examination of how key institutions like the evolving multiparty system, the National Electoral Board of Ethiopia (NEBE), and the constitutional-legal framework have grown, interacted, and changed through three significant political periods: the foundational yet restrictive EPRDF era (1991-2005), the crackdown and authoritarian consolidation following the 2005 elections (2005-2018), and the tumultuous transition under current government, characterized by initial openness but later conflict and democratic setbacks (2018-2023).

Additionally, this approach enables a deep dive into institutional design and its effects, analyzing how both formal rules like the provisions of the 1995 Constitution, the Charities and Societies Proclamation, and Political Party Laws and informal practices such as patronage networks, elite agreements, and coercive tactics have influenced political behavior, party competition, and ultimately, the stalled process of democratic consolidation. Importantly, it's crucial for unraveling Ethiopia's unique context, capturing the complex interactions between deeply rooted ethnonationalism, the centralizing tendencies of state power, the heavy burden of historical grievances, and the strategic maneuvers of political elites' elements that are key to understanding the ongoing disconnect between formal multiparty frameworks and real democratic progress.

To really understand the discursive and strategic aspects, researcher dive into key political statements, analyzing major speeches, policy announcements, and public comments made by successive Prime Ministers Meles Zenawi, Hailemariam Desalegn, and Abiy Ahmed as well as senior officials from the ruling party. These statements touch on important themes like democracy, multiparty politics, and how opposition forces are treated. To complement these primary sources, researcher also look at a variety of

secondary materials that provide essential context, interpretation, and outside perspectives. Scholarly literature plays a vital role here, drawing from peer-reviewed academic works that cover Ethiopian politics, modern history, federalism, ethnicity, and the processes of democratization. Researcher pay special attention to empirical studies and theoretical analyses that relate to the development of party systems and the challenges of state-building.

Additionally, reports from international organizations offer valuable independent insights and documentation, including detailed election observation mission reports especially from the European Union Election Observation Mission (EU EOM) for the years 2005, 2010, 2015, and 2021, as well as from the Carter Center. Researcher also consider human rights investigations and reports from organizations like Human Rights Watch and Amnesty International, along with in-depth conflict analyses and political risk assessments, primarily from the International Crisis Group (ICG). Lastly, researcher utilize media archives from reputable Ethiopian and international news outlets, which have been carefully cross-referenced for accuracy. These archives serve as crucial contemporary records that document political events, state crackdowns, opposition party activities, and the evolving nature of political discourse during the period we're examining. The sources were chosen for their direct relevance to the core research themes of party system evolution, electoral integrity, and state repression.

Researcher carefully chose sources based on their direct relevance to the study's four main research themes: the evolution of the party system, which includes how political parties form, their registration requirements, internal dynamics, and how they position themselves strategically over time; electoral integrity, which looks at the legal framework that governs elections, how bodies like the NEBE manage and conduct electoral processes, and the trustworthiness of the outcomes; state repression, which examines the legal tools used (anti-terror or CSO laws), actions taken against opposition figures, media, and civil society organizations (CSOs), as well as patterns of coercion; and institutional strength/weakness, focusing on the operational independence, capacity, and effectiveness of key democratic institutions, such as the NEBE, the judiciary, and the federal parliament, in limiting executive power and maintaining democratic standards.

To analyze this varied dataset, researcher used a multi-method qualitative approach. Thematic analysis was a main tool, involving systematic coding of data to uncover recurring themes, significant turning points, underlying causal mechanisms that explain institutional performance, and critical contradictions between how institutions are designed (as laid out in constitutions and laws) and how they actually function in practice, especially in the context of multiparty politics. Process tracing was used to examine key events like the significant 2005 election crisis and its violent aftermath, the strategic breakup of EPRDF and the creation of Prosperity Party (PP) in 2019, and the start of the Tigray War in November 2020.

This approach helped to carefully piece together their causes, how they unfolded, and their deep impacts on the structure and sustainability of the multiparty system. Additionally, critical discourse analysis was employed to analyze the language found in official statements, legal documents, and policy announcements from various regimes. This analysis revealed the prevailing narratives, legitimizing discourses, and justifications related to political pluralism, national security needs, and the contentious idea of national unity, highlighting how power was framed and contested through discourse.

3. MULTIPARTYISM UNDER EPRDF (1991-2018): CONTROLLED PLURALISM

During EPRDF era, the groundwork for multiparty democracy was laid, but it was all within a tightly controlled framework known as "revolutionary democracy" (Lefort, 2010; Aalen, 2002).

The 1995 Constitution promised multipartyism and essential freedoms. Yet, the laws that governed political parties like registration rules and vague restrictions on "ethnic" or "religious" parties along with the notorious Charities and Societies Proclamation, created a stifling atmosphere (Abbink, 2006). EPRDF

ISSN 2815-3324 Online, ISSN 2535-0358 Print
held a dominant position thanks to its extensive organizational network, control over state resources, and its grip on the NEBE, which many viewed as lacking true independence (Tronvoll, 2009).

The 1995 Constitution (Articles 29, 30, 38) established multipartyism and fundamental freedoms, but the reality was quite different due to restrictive laws. The Political Parties Proclamations from 1993 and 2008 set up tough registration requirements like needing 1,500 members for national parties (as stated in Art. 8(1) of the 2008 version) and included vague rules against parties based on religion, ethnicity, gender, or language (Art. 46(2) in the 1993 version, which was later modified but still left room for confusion). This created a double standard: while EPRDF's own parties Tigray People's Liberation Front (TPLF), Oromo People's Democratic Organization (OPDO), Amhara National Democratic Movement (ANDM), Southern Ethiopia People's Democratic Movement (SEPDM) were clearly ethnic-based, opposition parties trying to do the same faced obstacles or were branded as divisive. The notorious 2009 Charities and Societies Proclamation (Proclamation No. 621/2009) severely restricted civil society by preventing NGOs that received more than 10% of their funding from abroad from engaging in human rights and governance advocacy (Art. 14(2)), effectively silencing important watchdogs. EPRDF maintained its grip on power through its unmatched bureaucratic penetration (Vaughan, 2011) via the party-state structure, which controlled local administrations, the security forces, and, crucially, NEBE. Appointments to NEBE were tightly managed by the ruling party (Tronvoll, 2009), ensuring that election administration and outcomes consistently favored EPRDF.

The elections of 2005 opened a brief window in the political scene, giving us a rare chance to see some real competition, as Dahl would put it. Opposition parties, rallying around the Coalition for Unity and Democracy (CUD) and United Ethiopian Democratic Forces (UEDF), really stepped up, managing to win an impressive number of seats, particularly in urban areas. But then came the harsh state response to the protests that erupted after the elections, along with the imprisonment of opposition leaders. This was a serious blow to inclusiveness, effectively silencing any dissenting voices in the political arena (Lyons, 2006). After 2005, EPRDF ramped up its control, employing legal harassment, co-optation, and intimidation to push the opposition to the sidelines, reducing their role in parliament to little more than a symbolic presence (Aalen & Tronvoll, 2009).

The 2005 Ethiopian elections seemed to open a door to democracy, even if just for a moment. Riding the wave of significant discontent in urban areas, opposition groups mainly CUD and UEDF put up a formidable fight. According to NEBE, the ruling EPRDF and its allies snagged 327 seats (59.8%), while CUD managed to secure 109 seats (19.9%) and UEDF got 52 seats (9.5%). This was a remarkable gain for the opposition, hinting at a possible shift in power. Unfortunately, that momentum was brutally crushed. Widespread and credible claims of fraud during the vote counting sparked massive protests in Addis Ababa and other cities. The government's response was harsh: security forces killed at least 193 protesters, according to official reports, but Human Rights Watch suggested the actual number could be much higher. Thousands were injured, and over 30,000 people were arrested, including the entire leadership of CUD (Lyons, 2006; Abbink, 2006). Prominent figures like CUD Vice Chair Birtukan Mideksa faced years behind bars on charges like "outrages against the constitution".

This severe crackdown, known as 'Qinijit' after the date it escalated on May 15th, effectively snuffed out any real electoral competition for the time being. After 2005, EPRDF systematically worked to dismantle the opposition through a series of coordinated strategies. Legal harassment became a key strategy, taking advantage of the broad provisions in the 2004 Criminal Code like charges of "outrages against the constitution" and "inciting violence" and later the infamous 2009 Anti-Terrorism Proclamation (Proclamation No. 652/2009 - Articles 3 & 4) to silence critics, including Andualem Arage from Unity for Democracy and Justice (UDJ) party. Co-optation was also widely used, intentionally breaking apart opposition groups and luring members to switch sides to EPRDF or its affiliated parties. At the same time, a climate of intimidation and violence marked by harassment, beatings, and even killings, especially targeting opposition supporters in rural areas fostered a pervasive sense of fear.

By the time the 2010 elections rolled around, this extensive suppression led to a staggering victory for EPRDF, which "secured" 499 out of 547 seats (91.2%), leaving the opposition with only a token presence and solidifying authoritarian rule (Aalen & Tronvoll, 2009). The hopeful moment of 2005 was effectively shut down.

The ethnic federal structure laid out in Article 39 of the Constitution granting Nations, Nationalities, and Peoples the right to self-determination, including the option to secede has had a profound impact on the party system in Ethiopia. While it allowed for regional self-governance, it also entrenched ethnicity as the main political identity. EPRDF ruled through its ethnic-based member parties, each one holding sway in its own region like the TPLF in Tigray, OPDO in Oromia, ANDM in Amhara, and SEPDM in SNNPR using extensive patronage networks and coercive tactics (Vaughan, 2011).

This setup made it really tough for strong, nationwide parties with clear programs to emerge. Opposition groups had to organize mainly along ethno-regional lines to make any headway, as seen with the Oromo Federalist Congress (OFC) and the Somali People's Democratic Party (SPDP), which only added to the fragmentation. Efforts to create pan-Ethiopian parties, such as UDJ after 2005, struggled to find support outside urban areas, facing state repression and the challenge of overcoming the deep ethnic divides that the system itself had created (Turton, 2006). As a result, politics turned into a zero-sum game, pitting ethnic blocs against one another.

The formation and competition of parties were largely shaped by ethno-regional lines, a direct result of the ethnic federal system (Turton, 2006). While it offered recognition and self-governance for major groups, this system entrenched ethnicity as the main political identity, stifling the emergence of cross-cutting, issue-based parties and escalating tensions between different groups. The EPRDF itself was a coalition of ethnically based parties, ruling through a combination of patronage and coercion within each regional state (Vaughan, 2011).

4. THE POST-2018 TRANSITION: UNFULFILLED PROMISE AND RENEWED FRAGMENTATION

When Prime Minister Abiy Ahmed took office in 2018, it seemed like a new era of political freedom was on the horizon.

Abiy Ahmed's rise to power in April 2018 marked the beginning of a remarkable political shift in Ethiopia. His government quickly set in motion a wave of important reforms aimed at breaking down the oppressive structures of the past. They suspended or repealed several key repressive laws: the State of Emergency that had been in place since February 2018 was lifted; thousands of political prisoners, including notable leaders from groups like Ginbot 7, OFC, and Oromo Liberation Front (OLF), were freed; various exiled opposition groups, particularly Ginbot 7, OLF, and Ogaden National Liberation Front (ONLF), were taken off official terrorist lists and invited back to the country to return peacefully; and the restrictive Charities and Societies Proclamation (CSO law), which had greatly hindered civil society and NGO activities, especially those focused on human rights and advocacy was revised in 2019 to ease burdensome funding restrictions. Additionally, to enhance the integrity of elections, a new, more independent NEBE was appointed, with Birtukan Mideksa, a former judge and political prisoner herself, at the helm.

The sweeping liberalization measures sparked an immediate and unprecedented surge in political party registrations, with NEBE reporting over 120 legally recognized parties by 2021. This newfound pluralism saw the rise of significant explicitly pan-Ethiopianist parties, like Ethiopian Citizens for Social Justice (Ezema), which boldly challenged the ethnic federalist model that had shaped the state for decades by promoting a unified civic national identity. However, this rapid opening and the ascent of centralizing, pan-Ethiopian forces also triggered a strong ethno-nationalist backlash. Groups within historically

ISSN 2815-3324 Online, ISSN 2535-0358 Print
marginalized ethnic communities, especially among Oromo and Tigrayan political leaders, viewed these developments as a serious threat to their constitutionally guaranteed rights to self-determination and ethnic representation (Feyissa, 2021). This backlash led to deep internal rifts: the OLF fractured, with one faction engaging in the reconciliation process while others remained armed. At the same time, the once-dominant TPLF became increasingly estranged from Abiy's federal government, perceiving its reforms and centralizing moves as a direct attack on Tigrayan autonomy and the federal agreement, setting the stage for future, devastating conflict.

Ethiopia held its national and regional elections on June 21, 2021, after facing significant delays due to the COVID-19 pandemic and various logistical challenges. These elections were seen as the most competitive since the crucial 2005 polls. The Prosperity Party (PP), which came into being in December 2019 by merging the three largest regional parties from the former ruling coalition, EPRDF excluding TPLF along with several allied parties, achieved a remarkable landslide victory. This outcome solidified the PP's grip on the federal government and important regional states, signaling a clear political shift away from EPRDF era.

According to the official results from NEBE in 2021, the Prosperity Party achieved an impressive victory, securing 410 out of 436 contested federal parliamentary seats an astounding 94%. They also dominated 5 out of 11 regional state councils that were up for grabs. Voter turnout was remarkable, hitting 90% in the areas where polling occurred, which shows a strong public interest where it was possible. The elections did reveal some positive changes, particularly the noticeable independence of the NEBE under the leadership of former political prisoner Birtukan Mideksa. The NEBE took a bold step by publicly criticizing government actions and logistical issues during the elections, marking a significant shift from their previous compliance. Additionally, some opposition parties found themselves able to campaign more freely in certain regions compared to past elections, hinting at a bit more political space opening up.

While there were some positive points, they were mostly overshadowed by the significant issues pointed out in the EU EOM 2021 Report, which exposed serious shortcomings in both contestation and inclusiveness. The entire process was fundamentally undermined by extreme insecurity and the widespread disenfranchisement of millions of voters in Tigray, Oromia, and other areas, which directly contradicts Dahl's principle of inclusiveness.

In Tigray, where 38 parliamentary seats were at stake, no voting took place due to the ongoing and devastating conflict. Additionally, many constituencies in Oromia, especially in regions like Wollega and Guji along with areas in Benishangul-Gumuz, and parts of the Southern Nations, Nationalities, and Peoples' Region (SNNPR) and Afar, faced severe disruptions or were completely unable to hold elections, disenfranchising millions of eligible voters. To make matters worse, there was widespread harassment and violence aimed at opposition candidates and their supporters, particularly those linked to the Oromo and Sidama parties. This included systematic arrests, intimidation, physical assaults, and even killings, especially noted around the Sidama referendum. Several opposition candidates were arrested right in the middle of their campaigns (EU EOM, 2021).

The playing field was incredibly uneven. The ruling PP had a massive edge, thanks to state-sponsored advantages like almost complete control over media coverage, special access to essential resources such as government vehicles and venues, and the extensive use of state bureaucracy to support their campaign. On the flip side, private media outlets were under heavy pressure and faced numerous restrictions, which stifled critical reporting. To make matters worse, significant ‘Boycotts’ by major opposition parties further diminished the election's competitiveness and credibility. OLF and OFC completely boycotted the elections in Oromia, the most populous region in the country, citing widespread repression and a perilous security situation. TPLF, caught up in conflict with the federal government, also chose not to participate. These boycotts severely limited meaningful political competition in key areas, paving the way for the PP's overwhelming victory in the contested seats.

The political landscape took a sharp turn when the Tigray War erupted in November 2020, cutting short any hopes for a peaceful opening. This conflict saw federal forces, backed by Eritrean and Amhara militias, clashing with TPLF, leading to horrific atrocities, war crimes, and a dire humanitarian crisis (ICG, 2021, 2022, 2023). The violence quickly spread to neighboring regions like Afar and Amhara. Since late 2021 and early 2022, the political space has shrunk considerably (ICG, 2022, 2023).

After declaring a state of emergency in November 2021, which was lifted in February 2022, Ethiopian authorities began a widespread campaign of arbitrary detentions. This primarily targeted ethnic Tigrayans, with thousands being detained, as well as notable Oromo opposition leaders. The crackdown was largely justified under broad anti-terrorism laws. Among those arrested were high-profile figures like Jawar Mohammed, the leader of OFC and a media mogul, and Eskinder Nega, who heads Balderas for True Democracy. Both were taken into custody in July 2021 and later convicted on charges that many international observers and human rights organizations condemned as politically motivated "terrorism" and "treason." Jawar was initially sentenced to life in prison, though this was later reduced, while Eskinder received a six-year sentence. These actions clearly indicated a significant restriction on political freedoms. (ICG, 2022, 2023).

At the same time, the government ramped up its crackdown on independent media. Many outlets were shut down, including notable ones like Addis Standard (albeit temporarily) and Awlo Media Center. Journalists found themselves facing arrests, with Meaza Mohammed from Ethio-360 being a prime example. Internet blackouts became a common tactic to hinder the flow of information, especially in conflict areas like Tigray and Oromia, as well as during protests in other regions. Importantly, the government increasingly portrayed any form of opposition, dissent, or critical journalism particularly regarding its actions in Tigray and Oromia as backing "terrorists" (targeting groups like the TPLF and OLA-Shene) or as threats to national security. This widespread narrative of "securitization of politics" (as noted by ICG in 2022 and 2023) was used to legitimize harsh repression against civil society organizations, independent media, and opposition parties that didn't align with the ruling PP.

Efforts to initiate a promised national dialogue a crucial part of Ethiopia's declared political transition fell apart amid rising conflict and deep-seated distrust. Although the government set up the Ethiopian National Dialogue Commission (ENDC), its credibility took a significant hit. Major opposition groups, such as TPLF and key factions within the OFC and OLF, either chose to boycott the process or voiced serious doubts about the Commission's true independence and inclusivity. As a result, by late 2021 and throughout 2022, the political landscape in Ethiopia had worsened considerably. The ongoing war, widespread mass arrests, a crackdown on the media, and the increasing repression of dissent created a political environment that had shrunk to levels comparable to, or even worse than, the repression seen during the final years of the previous EPRDF regime (ICG, 2022, 2023). Under these circumstances, genuine multiparty political competition became utterly impossible.

5. ANALYSIS: WHY MULTIPARTYISM FAILED TO ANCHOR DEMOCRACY

The Ethiopian experience offers valuable insights into the challenges multiparty systems face in fragile, diverse nations that are navigating complex transitions:

Just having multiple parties doesn't automatically mean a country is democratic. If there's no real dedication to political pluralism, the rule of law, independent institutions (especially the judiciary and electoral bodies), and the safeguarding of civil liberties, multiparty systems can turn into mere fronts for authoritarianism, what some call "competitive authoritarianism" (Levitsky & Way, 2010). The elections in 2005 and 2021 really highlight this issue. Even though there were some competitive aspects, the state's grip on the NEBE before 2018, along with tactics like disenfranchisement in Tigray in 2021, harassment of opposition candidates that same year, ongoing media bias, and the legal manipulation through laws like the CSO law from 2009 and the Anti-Terror Proclamation after 2005 and 2020, made it clear that

ISSN 2815-3324 Online, ISSN 2535-0358 Print
multipartyism was just a front for the EPRDF/PP's control. This aligns perfectly with Levitsky and Way's (2010) concept of competitive authoritarianism.

Ethnic-based parties can improve representation for marginalized groups in a federal system, but they also have their downsides:

- They can splinter the political landscape, making it tough to build national consensus.
- They may create a zero-sum game mentality and breed inter-ethnic distrust.
- They can hinder the growth of policy-focused, programmatic politics.
- They are often easily exploited by elites for mobilization and power grabs.

In Ethiopia, the emphasis on ethnic identity nearly pushed aside other forms of political organization, which only intensified the forces pulling the country apart. The ethnic federal system established by the EPRDF gave rise to parties like the TPLF, OPDO/PP, and ANDM/PP, while it actively stifled non-ethnic national parties before 2018. After 2018, the emergence of pan-Ethiopianist parties, such as Ezema, sparked a violent backlash rooted in ethno-nationalism and led to fragmentation, including splits within the OLF. This turmoil has made it difficult to build a national consensus and has contributed to the ongoing conflicts in Tigray and Oromia. The way elites have manipulated ethnicity for political mobilization seen in the actions of TPLF, various PP factions, and OLF factions highlights the inherent dangers of this approach.

Democratic institutions like the parliament, judiciary, NEBE, and media have struggled to stand strong and independent from the executive branch throughout various regimes. This lack of autonomy and capability has made it tough to effectively check power and ensure fair competition. The NEBE's struggle for independence under the EPRDF, which was a biased administration, along with its challenges related to capacity and government pressure in 2021 despite some improvements really brings this issue to light. Parliament often just went along with whatever the executive decided. The judiciary's inability to hold the executive accountable, especially seen in the politically charged trials after 2005 and again in 2021 involving figures clearly shows its lack of independence.

The ongoing use of state coercion through arrests, intimidation, and violence against opposition figures, journalists, and activists has consistently eroded trust in the political process and discouraged public participation. The shift towards a more securitized political landscape after 2005 marks a significant step backward. The crackdown in 2005, which involved mass killings and arrests, followed by legal harassment, and the pre-election repression leading up to 2010 and 2015, along with the harsh measures taken like mass arrests, media closures, internet shutdowns, and the tragic killings of protesters in Oromia and Amhara have all played a significant role in eroding trust and discouraging people from participating.

EPRDF and its alliances held onto power by creating extensive patronage networks that controlled state contracts, jobs, licenses, and resources (De Waal, 2015). Those who challenged them were systematically pushed aside through legal, economic, and coercive tactics, which ultimately corrupted the political landscape (De Waal, 2015).

Successive governments have struggled to create a genuine, inclusive national dialogue that could tackle deep-rooted historical grievances, reconcile differing visions of the state like ethnic federation versus unitary, and establish a shared set of democratic rules. It's crucial to recognize that the failure to create a credible and inclusive national dialogue before tensions escalated into the Tigray war and the Oromia conflict serves as a significant lesson. Over the years, various regimes have focused more on maintaining control rather than engaging in meaningful discussions about fundamental issues like the nature of the federation, historical grievances, and citizenship.

6. THE PATH FORWARD FOR ETHIOPIA

The time after 2018 showed us a glimpse of what could be, but it quickly got buried under conflict and a return to authoritarianism. Ethiopia's hopes for a democratic future are still hanging by a thread. To make

real progress, it's not enough to just have multiple political parties on paper; we need a complete shift towards a system that truly values the rule of law, human rights, and institutional integrity. It's crucial that we commit to resolving our differences through peaceful, democratic means instead of resorting to violence. The very survival of Ethiopia as a nation might hinge on embracing these hard-earned lessons.
Ethiopia's path to a stable future and its dreams of democracy really depends on a significant change that goes well beyond just the surface-level presence of multiple political parties. Simply having a variety of parties isn't enough; what's truly needed is a real political liberalization that's firmly rooted in the rule of law and a universal commitment to human rights. This is the bedrock upon which everything else must be built. To get there, we need to face some tough lessons from the past and make some serious, systemic changes.

First and foremost, we absolutely need deep institutional reforms. It's crucial that key state institutions, especially the NEBE and the judiciary, are given real independence and protection. This means they should operate freely, without interference from political parties, have enough resources, and be backed by strong legal protections. Without truly independent institutions that can run fair elections and provide unbiased justice, we won't see any real democratic progress. Building trust in these essential pillars is vital for any political process to be seen as legitimate.

It's absolutely essential to put an end to systematic state repression. We need to ensure that fundamental freedoms like the rights to express ourselves, gather, associate, and have a free press are protected for everyone, no exceptions. This includes those who might disagree with the government or voice criticism. The widespread use of arbitrary detention, intimidation, media censorship, and internet shutdowns as means of political control has to stop. We need a safe space where citizens can engage in civic life without fear; that's the foundation of a healthy democracy.

It's really important to nurture a political culture that embraces tolerance and inclusive citizenship. Achieving this goes beyond just talking the talk; we need to put some real systems in place. We should revamp civic education to highlight a shared Ethiopian identity while also honoring our diversity. We need independent public service media that can operate free from government control, allowing them to promote national dialogue and showcase balanced discussions. Plus, initiatives like cross-ethnic youth programs and cultural exchanges can play a big role in breaking down stereotypes and building trust among the younger generation. After years of conflict and division, our social fabric has taken a hit. To mend it, we need to move beyond ethnic or political exclusion and cultivate a strong sense of nationhood, supported by these tangible actions.

At the heart of this change is a credible, inclusive, and truly participatory national dialogue process. This dialogue can't just be for show; it needs to tackle the deep-rooted, contentious issues that have led to instability. These issues include the fundamental structure of the state (federalism versus centralization), unresolved historical grievances, and the very essence of what it means to share an Ethiopian identity and nationhood. For this dialogue to succeed, all key political players, including those who are currently marginalized or in opposition, must have a genuine seat at the table.

The alternative path is both stark and risky. Sticking to a facade of multipartyism, which only hides ongoing authoritarian practices amid growing ethnic divisions, doesn't offer a real future. This strategy has clearly failed, resulting in nothing but repeated violence, instability, and the curtailing of basic rights. Ethiopia is at a pivotal moment: embracing the tough but essential journey of true institutional reform, putting an end to repression, and encouraging inclusive dialogue is the only credible way to achieve lasting peace, stability, and the democratic future that its people truly deserve.

7. CONCLUSION AND IMPLICATIONS

Ethiopia's three-decade journey with multiparty politics clearly shows that just having multiple parties isn't enough to truly solidify democracy. When we look at Dahl's criteria for polyarchy, it becomes evident

ISSN 2815-3324 Online, ISSN 2535-0358 Print

that there are ongoing issues with both contestation and inclusiveness. The competitive authoritarian framework proposed by Levitsky and Way perfectly captures a situation where elections take place, but they are consistently manipulated by those in power using state resources.

Ethiopia's experience with ethnic federalism isn't an isolated case; it serves as a powerful example in the realm of comparative politics. Unlike more successful multinational federations such as India or Canada, where a sense of constitutional patriotism and robust central institutions help to counteract divisive forces, Ethiopia's approach has been marked by fragile institutional protections and the manipulation of ethnicity by elites. This situation reflects the difficulties faced by countries like Bosnia and Herzegovina or Iraq. This comparison highlights that the framework of federalism itself is not as important as the political culture and the strength of the institutions that support it.

The journey of multiparty politics in shaping a democratic Ethiopia since 1991 has been quite a mixed bag. Although it was officially embraced as a cornerstone of democracy, its actual functioning has often been stifled, manipulated, and at times outright suppressed. This has led to a failure in fulfilling its fundamental promise of accountable governance and peaceful political transitions.

The lasting impact of centralized governance passed down from earlier regimes, the overpowering influence of ethnonationalism embedded in the federal system, the ongoing fragility of essential democratic institutions like NEBE, the judiciary, and parliament, the systematic repression of dissent (from the 2005 crackdown to the heightened security measures post-2021), and the way elites manipulate patronage networks have all played a significant role in hindering multiparty competition from achieving its democratic goals of accountability and smooth power transitions.

The shift that happened after 2018 showed us a glimpse of what could be possible, highlighted by a notable increase in party registrations and reforms from NEBE. Yet, the lingering issues surrounding identity and power, the way the tragic Tigray conflict has been used to justify a return to authoritarian rule, and the lack of a truly inclusive national dialogue have all contributed to a swift decline in democracy. The jailing of key opposition leaders on politically motivated charges is a clear sign of this troubling trend.

REFERENCES

Aalen, L. (2002). *Ethnic Federalism in a Dominant Party State: The Ethiopian Experience 1991-2000*. Chr. Michelsen Institute.

Aalen, L., & Tronvoll, K. (2009). The End of Democracy? Curtailing Political and Civil Rights in Ethiopia. *Review of African Political Economy*, *36*(120), 193-207.

Abbink, J. (2006). Discomfiture of Democracy? The 2005 Election Crisis in Ethiopia and its Aftermath. *African Affairs*, *105*(419), 173-199.

Dahl, R. A. (1971). *Polyarchy: Participation and Opposition*. Yale University Press.

De Waal, A. (2015). *The Real Politics of the Horn of Africa: Money, War and the Business of Power*. Polity Press.

European Union Election Observation Mission (EU EOM). (2021). *Ethiopia: Final Report - Federal Parliamentary Elections 2021*.

Feyissa, D. (2021). *Ethiopia's Transition: The Prospect of Pluralism*. Carnegie Endowment for International Peace.

International Crisis Group (ICG). (2022). *Ethiopia's Oromia Conflict: A Dangerous Stall*. (Report No. 306).

International Crisis Group (ICG). (2023). *Ethiopia: Fragile Calm in Tigray, Mounting Risks in Amhara*. (Briefing No. 186).

Lefort, R. (2010). Powers–mengist–and peasants in rural Ethiopia: the May 2005 elections. *Journal of Modern African Studies*, *48*(3), 435-460.

Levitsky, S., & Way, L. A. (2010). *Competitive Authoritarianism: Hybrid Regimes after the Cold War*. Cambridge University Press.

Lyons, T. (2006). *Ethiopia in 2005: The Beginning of a Transition?* (CSIS Africa Notes, No. 25).

Schmitter, P. C., & Karl, T. L. (1991). What Democracy Is... and Is Not. *Journal of Democracy*, *2*(3), 75-88.

Tronvoll, K. (2009). *War & the Politics of Identity in Ethiopia: Making Enemies & Allies in the Horn of Africa*. James Currey.

Turton, D. (Ed.). (2006). *Ethnic Federalism: The Ethiopian Experience in Comparative Perspective*. James Currey.

Vaughan, S. (2011). Revolutionary Democratic State-Building: Party, State and People in the EPRDF's Ethiopia. *Journal of Eastern African Studies*, *5*(4), 619-640.

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

THE VISEGRAD GROUP AND THE WAR IN UKRAINE: FROM VETO BLOC TO VOID

Yassine Guennoun
Sidi Mohammed Ben Abdellah University
Fez, Morocco
yassine.guennoun@usmba.ac.ma
https://orcid.org/0009-0003-8777-9781

Abstract *This article asks why Russia's 2022 invasion fractured the Visegrád Group and answers by showing that the cohesion once visible during the 2015 migration crisis rested on a model of negative integration that could resist supranational pressure yet could not be translated into the demands of war. When faced with a proximate conflict that required convergent threat perception, collective risk-sharing and credible military capacity, the four states moved along divergent paths: Poland recast sovereignty as survival and bound itself more deeply to NATO and United States' guarantees, Hungary treated sovereignty as autonomy and used veto power while maintaining energy ties with Moscow, Slovakia balanced cooperation and restraint within a polarised domestic arena, and Czechia consolidated an Atlanticist line alongside Poland. These trajectories produced a structural split that removed the V4 from the centre of Europe's security debates and revealed a deeper mechanism: coalitions forged in opposition can endure in institutional disputes but falter once coercive shocks demand common strategy. What remains of the Visegrád format is protocol and symbol only, while effective agency has shifted to NATO, to coalitions of the willing within the EU, and to minilateral formats that reflect the real distribution of threat, capacity and political will across the continent.*

Keywords Visegrád Group; Ukraine war; Sovereignty; NATO; European Union; Strategic autonomy; Central and Eastern Europe.

1. INTRODUCTION

The Visegrád Group was created in 1991 as a platform for coordination among Czechia, Hungary, Poland, and Slovakia. In the EU era it evolved into a recognisable regional actor, most visible when the four governments converged against common pressures from Brussels (Dangerfield, 2008, 2012). The 2015 migration crisis crystallised this posture. V4 leaders framed quota schemes as an intrusion on sovereign decision and issued joint statements that linked security to border control and national discretion (Visegrad Group, 2015). This pattern produced a durable image: a bloc capable of acting together when the issue was sovereignty vis-à-vis the EU. The V4's pre-2022 unity is best understood through the lens of negative integration (Scharpf, 1999), a mode of coordination that resists transfers of competence to the centre and concentrates on blocking or diluting EU mandates rather than on constructing joint institutions or capabilities.

Russia's full-scale invasion of Ukraine in 2022 exposed a different structure. The war placed the four states inside a security environment defined by proximity to Russia's offensive power and dependence on external guarantors. In terms of regional security-complex theory, this was a textbook case of small states embedded in a contested neighbourhood where survival depends on alliance configuration (Buzan & Wæver, 2003; Lake, 2009). Yet under this pressure, the V4 did not convert its earlier migration-era unity into a coherent security line. Instead, pre-existing differences hardened into incompatible strategies. Comparative analysis confirms the arc: the migration crisis activated cohesion, but the pandemic and the Ukraine war exposed fragmentation (Kaniok & Hloušek, 2025). Contemporary policy commentary reaches the same conclusion: V4 cooperation on high politics has effectively withered (Beck, 2024).

This article addresses a precise question: Why did Russia's invasion of Ukraine fracture the Visegrád Four? The answer lies in how each member redefined sovereignty and security under wartime pressure. Poland treated sovereignty as survival against Russia and built a forward defence posture anchored in

NATO and the United States. Hungary treated sovereignty as insulation from alliance pressure and doubled down on a defiant balancing line towards Brussels and Moscow. Slovakia alternated around domestic polarisation, signalling support for Ukraine in some domains while restraining it in others. Czechia aligned clearly with EU and NATO policy and moved institutionally and discursively closer to Poland. These divergent logics left the bloc without a common strategic language, producing a split that renders the V4 ineffective on Europe's central security question.

The paper contributes three things. First, it reframes V4 cooperation as a case of negative integration that translated poorly to war. Unity formed around resisting EU mandates did not translate into shared strategy once coercive external threat set the agenda. This clarifies why a once-cohesive group failed to act as a regional security pole in 2022–2025 (Beck, 2024; Kaniok & Hloušek, 2025; Visegrad Group, 2015). Second, it links regional security-complex dynamics to hierarchy: Poland's ascent as a frontline state deepened reliance on United States power and NATO command structures, while Hungary asserted autonomy against those same structures, creating a structural cleavage inside the bloc (Buzan & Wæver, 2003; Lake, 2009). Third, it traces the institutional consequence at EU level. As unanimity faltered on sanctions, financing, and accession questions, EU practice shifted towards flexible "coalitions of the willing," a move with direct implications for debates on strategic autonomy and alliance cohesion (Rankin, 2025; Roos, 2020).

Methodologically, the analysis integrates primary statements and communiqués, national security strategies and official speeches, and secondary assessments from peer-reviewed scholarship and leading policy institutes. The periodisation runs from the 2015 migration crisis through mid-2025, relying on primary statements, national strategies, communiqués, and secondary assessments published and available at the time of writing. Section II reconstructs pre-war V4 unity on sovereignty and migration, drawing on official statements such as the September 2015 joint statement (Visegrad Group, 2015) and scholarship that tracked how the bloc acted as a collective veto against EU relocation schemes (Ivanova, 2016; Nagy, 2016). Earlier analyses of the V4's institutional role within the EU provide useful background on the group's integration trajectory (Dangerfield, 2008, 2012), but the empirical focus here is on the decade of crises that ultimately fractured the bloc. Section III examines Poland's shift to a NATO-anchored security pivot. Section IV analyses Hungary's sovereignty-through-defiance line and its effects on EU decision-making. Section V contrasts Slovakia's two-track adaptation with Czechia's consolidation of Atlantic alignment. Section VI draws out the implications for EU security governance and the autonomy debate. The conclusion returns to the argument: The V4's coherence was contingent on opposition to Brussels; the war forced real security choices and dissolved that contingency.

2. THE V4 BEFORE 2022: SECURITY THROUGH UNITY

The Visegrád Four entered the EU as a coordination platform with flexible aims, but its most cohesive phase came during the 2015 migration crisis. In that moment the four governments converted a diffuse cooperation forum into a disciplined bloc that tied security to sovereign control of borders and policy discretion. The September 2015 joint statement rejected any mandatory and permanent redistribution scheme and cast solidarity as voluntary, within national competence (Visegrad Group, 2015). This was more than just posturing as Budapest securitised asylum through law and policing, constructing physical barriers, criminalising unlawful entry, and restricting access to procedure in ways that courts and monitors later scrutinised (Nagy, 2016). Warsaw, Prague and Bratislava refrained from replicating Hungary's legal architecture; instead, they adopted the same political grammar, framing sovereignty, order, and territorial control as the core of national security and treating Brussels' relocation design as the foil.

The legal confrontation fixed this alignment into a recognisable pattern. When Slovakia and Hungary challenged the Council's emergency relocation decision, the Court of Justice dismissed the actions in September 2017, upholding the scheme's legality (Court of Justice of the European Union [CJEU], 2017). Compliance did not follow. In April 2020, the Court found Poland, Hungary, and Czechia in breach of their obligations under the relocation decisions (CJEU, 2020). The rulings clarified law. The politics clarified the bloc. Across 2015-2020, the V4 treated EU intrusiveness as the principal security problem and presented

ISSN 2815-3324 Online, ISSN 2535-0358 Print

their resistance as a defence of constitutional self-government. This fused discursively with themes of cultural protection and risk containment, producing a negative-integration coalition that acted together precisely when it refused to share competence with the centre.

Three features of this phase set the baseline for the war period. First, the V4 defined its common enemy as institutional pressure from the EU's legal and administrative machinery rather than an external military adversary. Security was internalised as the preservation of decision authorship, with migration as the arena where that authorship was most visibly contested (Nagy, 2016; Visegrad Group, 2015). Second, the choice of instruments. The tools of unity were domestic: legislative change, policing, constitutional arguments, and coordinated announcements. Even where the Court validated the Council's authority, the four governments showed that prolonged contestation could blunt implementation, creating space for national manoeuvre despite adverse jurisprudence (CJEU, 2017, 2020; Gkliati, 2022). Third, rhetorical convergence. Leaders across the four capitals narrated their stance in the same style: defence of sovereignty, protection of citizens, and rejection of imposed burdens. This produced what external observers read as a coherent bloc shaped by migration and rule-of-law conflict rather than by joint military planning (Kaniok & Hloušek, 2025; Ivanova, 2016).

The V4's coherence was real but conditional, built on an alignment of negative aims. It could speak with one voice when blocking quota designs or diluting enforcement without needing to harmonise broader threat assessments beyond the shared conviction that Brussels was overreaching. That single claim sustained summits, joint texts, and tactical coordination, and it was enough to anchor the bloc's reputation: by the end of the 2010s the V4 had come to represent, in EU debates, a Central European veto cluster on migration and sovereignty. Its unity was therefore a function of institutional conflict structures rather than a shared external security doctrine.

This matters for two reasons. First, the V4's pre-war record does not constitute an emergent security alliance, since its instruments and targets were inward-facing and its operational expertise was legal and administrative rather than military. Second, it shows why the bloc would later fail the stress test of regional war. When Russia attacked Ukraine, the problem set shifted from competence defence to deterrence, logistics, energy exposure and alliance posture, and the tools and narratives that bound the V4 in 2015–2020 could not carry over because they had never been designed for that purpose. Later sections trace how Poland, Hungary, Slovakia and Czechia each reinterpreted sovereignty under war pressure, but the pre-2022 terrain explains their starting positions: unity rested on resisting Brussels, and no joint doctrine existed for handling Moscow.

This section therefore establishes a baseline: the V4 was cohesive when it could translate a domestic legal-political agenda into a collective stand inside EU institutions, acting as a security community only in the thin sense of guarding national control against supranational allocation. The Court's 2017 and 2020 decisions mark the boundary between law and politics, the 2015 joint statement captures the bloc's self-understanding, and scholarship records both the effectiveness and the limits of this mode of cooperation. What appeared to be a durable regional alliance was in fact a contingent coalition organised around a single set of institutional conflicts, a contingency the war would later expose.

3. POLAND: FROM REGIONAL ALLY TO NATO'S SECURITY PIVOT

Poland entered the war period with a strategic doctrine already oriented towards the Atlantic alliance. The 2020 National Security Strategy of the Republic of Poland codified Russia as the primary threat, the United States as the pivotal security partner, and NATO as the framework through which Poland would build regional leadership on the eastern flank (Government of Poland, 2020). It also stressed coalitional formats that amplify Central and Eastern European voice, including the Bucharest Nine and the Three Seas Initiative, as instruments that complement the alliance rather than replace it (Janulewicz, 2020). Thus, this pre-war alignment mattered because, once Russia expanded the war, Warsaw did not seek a V4 position but instead accelerated its existing trajectory that placed NATO at the centre of Polish sovereignty and deterrence.

The Russian invasion recast sovereignty in Warsaw as survival against a proximate adversary, and the policy response was immediate and structural. Poland expanded its force posture, accelerated modernisation, and raised defence spending to about four per cent of GDP, a level unmatched among major European allies in 2023 (Jones, 2023). This was not meant to be a symbolic benchmark: the acquisitions pipeline and force design aimed to generate mass and lethality for a high-intensity contingency on NATO's north-eastern front, prioritising heavy armour, integrated air and missile defence, combat aviation, and munitions depth to shape the Polish Army into a large, manoeuvre-capable force able to hold ground and absorb shocks while allied support arrived (Jones, 2023).

Operational practice reinforced the procurement drive. Poland became a critical logistics corridor, training and staging platform, and frontline donor for Ukraine. Parliamentary and official accounts from 2023 document Warsaw's role in rallying allied assistance and embedding reconstruction and accession goals for Kyiv within Euro-Atlantic agendas. They also show how support was positioned within a larger strategic design: sustained deterrence on the eastern flank, accelerated Ukrainian integration with Western institutions, and a long-term tightening of transatlantic defence ties (NATO Parliamentary Assembly, 2023). In this context, sovereignty is defended through depth of alliance rather than distance from it. Consequently, the regional geometry shifted. Instead of treating the V4 as the default vehicle for Central European coordination, Poland invested political capital in formats that map directly onto the alliance's eastern defence line. By early 2025, Poland was openly reorienting its regional strategy, seeking "more effective regional formats" after the Visegrád Group fractured over Russia (Bugajski, 2025). The government emphasised the Bucharest Nine, the Three Seas Initiative, closer ties with the Baltic and Nordic states, and other minilateral arrangements aligned with NATO planning cycles. The logic was functional: groupings that reproduced NATO's threat picture and readiness requirements were elevated, while a bloc unable to agree on the adversary was deprioritised (Bugajski, 2025).

This reconfiguration reshaped V4 cohesion in two ways. First, it removed the centre of gravity that had given the bloc leverage inside EU debates: Poland's mass, economy, and diplomatic reach had anchored every push, but once Warsaw tied its security authorship to NATO formats and coalition leadership with frontline states, the incentive to invest in V4 consensus declined. Second, it turned the latent Poland–Hungary divergence into an open structural split. Hungary recoded sovereignty as insulation from alliance pressure, while Poland recoded it as deep integration with the alliance. These logics imply different risk tolerances, instruments, and audiences, leaving no basis for a common security policy under wartime conditions.

Thus, Poland's approach reshapes the role of European instruments, maintaining their importance for financing, sanctions, and reconstruction while locating the military core of sovereignty where Warsaw judges credible power to reside in NATO force structure, bilateral commitments from the United States, and regionally nested coalitions able to act at speed. This approach aligns with the 2020 strategy's hierarchy of guarantees and with parliamentary narratives that link Ukraine's defence and accession prospects to Poland's own security horizon (Janulewicz, 2020; NATO Parliamentary Assembly, 2023). It also matches the procurement and spending profile that by 2023 marks Poland as the alliance's land-power outlier in Europe (Jones, 2023).

The consequence for this paper's broader claim is direct. Poland's shift from regional ally to NATO pivot was more than rhetorical. It represented a redistribution of institutional trust and material power that reduced V4 solidarity to a secondary asset in the domain that now defines European security. The bloc had amplified Poland's leverage against Brussels on migration, but it offered no leverage against Russia on deterrence. Warsaw's Atlanticist orientation, already evident in its consistent alignment with NATO and the United States, was amplified by the war in Ukraine, which reinforced the primacy of alliance formats over regional consensus. Poland's leadership therefore migrated to the coalitions that could deliver.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

4. HUNGARY: SOVEREIGNTY THROUGH DEFIANCE

Hungary carried its sovereignty doctrine from the migration decade into wartime Europe and hardened it. The government condemned the invasion at the level of principle, then organised practice around insulation from alliance pressure and preservation of economic ties with Russia. In EU forums this produced a pattern of obstruction on Ukraine files. Budapest refused to endorse European Council conclusions on support to Kyiv, stalled sanctions rollovers, and blocked collective instruments such as reimbursements for military aid, conditioning movement on concessions to Hungarian priorities (Gizińska & Sadecki, 2025). The position was packaged domestically through "peace" messaging and national consultations that portrayed sanctions and financing as threats to Hungarian welfare, thereby fusing the external war with an internal claim to protect sovereignty against Brussels (Gizińska & Sadecki, 2025; Reuters, 2025).

Hungary's stance rests on two pillars: the first is a consistent use of veto power within unanimity procedures; Budapest leveraged institutional rules to force issue linkage across dossiers, including Ukraine's EU track, sanctions design, and budgetary instruments, creating recurrent blocking points in 2023–2025 where the other twenty-six had to work around or buy time. The second is a refusal to treat Russia as an existential adversary. Hungarian leaders argued that the war's costs to Europe outweighed its benefits, that escalation risk was high, and that energy dependence required pragmatism. Prime Minister Orbán's claim that financing Ukraine's war effort would "ruin Europe" condensed this posture into a single line of political economy (Reuters, 2025). In practice, Hungary maintained its energy relationship with Moscow and presented this continuity as rational stewardship of national interests (Gizińska & Sadecki, 2025). A further dimension is the securitisation of Ukraine's ethnic Hungarian minority, which Budapest portrays as vulnerable to assimilationist pressures. This narrative has been used to justify obstruction of Ukraine's EU accession path and to sustain a narrative in which defending co-ethnics becomes part of Hungary's sovereignty doctrine (Balogh & Kovály, 2025).

The Hungarian stance broke the V4 hinge with Poland because Warsaw's definition of sovereignty runs through NATO mass and forward deterrence whereas Budapest's definition runs through policy autonomy vis-à-vis Brussels and strategic ambivalence towards Moscow. These logics cannot generate a joint security position under war conditions. The fracture was visible inside the EU, where Hungary forced stalemate and other capitals pivoted to flexible formats to keep Ukraine support flowing. Analysts documented a shift towards "coalitions of the willing" for financing and capability pipelines as a direct response to the Hungarian veto strategy (Rankin, 2025). The institutional result is paradoxical as Hungary asserts sovereignty against supranational pressure and thereby accelerates a Europe of variable geometry on security, a Europe in which decisions move without it.

Hungary's posture is coherent on its own terms as it prioritises insulation from EU discipline, low exposure to military entanglement, and price stability through Russian energy. It is also isolating. The policy mix places Budapest in direct opposition to the dominant Euro-Atlantic line on deterring Russia and sustaining Ukraine, and it collapses the V4's ability to speak as a bloc on the continent's central security problem. In the framework of this paper, Hungary is the fixed point around which V4 unity dissolves once war replaces migration as the agenda.

5. SLOVAKIA AND CZECHIA: BETWEEN ADAPTATION AND ALIGNMENT

Slovakia's trajectory since 2022 is a study in dual signalling. After early support to Kyiv under the previous government, the return of Robert Fico introduced a rhetorical break: within days of taking office he announced that Slovakia would not back further EU military aid to Ukraine, presenting humanitarian assistance as the acceptable ceiling (Reuters, 2023). This position mobilised a domestically powerful constituency sceptical of the war and wary of escalation, while also fitting a communication strategy that cast sanctions and arms as costly distractions from national priorities. That constituency is anchored in a voter base where pro-Russian sympathies are stronger than the national average and where scepticism of Ukraine's NATO bid resonates as a defence of small-state prudence. Surveys in 2023 showed that more than a third of Smer voters preferred a Russian victory, while only a marginal share supported Ukraine,

which helps explain why Fico's rhetorical line carries domestic weight even as his government maintains forms of practical cooperation with Kyiv (Dębiec, 2024). The stance appeared to align Slovakia with Hungary, yet the reality has been more complex.

In its first year under Fico, Slovakia pursued a two-track approach. Bratislava declared that it would not provide military assistance and rejected Ukraine's path to NATO, yet it continued forms of support that mattered in aggregate: electricity exports, ammunition produced under commercial contracts, maintenance pathways for Ukrainian equipment, and a steady fulfilment of NATO obligations including the two per cent benchmark (Dębiec, 2024). These measures were coupled with diplomatic assurances on Ukraine's EU track, producing a calibrated stance that preserved ties with the Euro-Atlantic mainstream while sustaining a domestic narrative of restraint. The result kept Slovakia out of outright obstructionism and prevented automatic alignment with Budapest's veto strategy inside the EU, while also keeping doors open in Kyiv. The price was ambiguity: Slovakia avoided clear placement in the coalition's front rank, limiting its influence over the war agenda while protecting space for internal political management.

Czechia moved in the opposite direction, and it did so decisively. The shift began before the invasion with the defeat of Andrej Babiš and continued with the election of Petr Pavel, after which Prime Minister Petr Fiala and President Pavel consolidated a pro-EU, pro-NATO line and treated support for Ukraine as an extension of Czech security. This alignment had two consequences: it loosened the remaining connective tissue with Budapest, as Czech ministers spoke openly about the V4's loss of political coherence and deprioritised the format for high politics, and it tightened operational links with Poland and with Baltic and Nordic partners, reflecting a shared threat picture and a preference for alliance-centric solutions to the war (Beck, 2024).

The divergent trajectories of Slovakia and Czechia reshaped Central Europe's coordination geometry. By early 2025, Warsaw invested in formats that mapped directly onto NATO's eastern posture: the Bucharest Nine and the Three Seas Initiative rose in salience, minilateral ties with frontline states deepened, and the V4 receded as a vehicle for security policy (Bugajski, 2025). Within that shift, Czechia emerged as a consistent partner for Poland, while Slovakia became a contingent one. Bratislava could join when the issue was EU financing, reconstruction logistics, or energy stabilisation, but it held back or softened its stance when measures involved ammunition pipelines or deeper alliance entanglement that complicated Fico's domestic strategy (Dębiec, 2024; Reuters, 2023).

The result is a durable 2–2 split on the war's central questions. Poland and Czechia form the Atlanticist core, aligning their security directly with NATO and anchoring support for Ukraine. Hungary and Slovakia sit on the opposite side, ranging from open obstruction to selective cooperation shaped by domestic politics and energy dependence. This configuration ends any expectation that the V4 can act as a regional security pole. What remains is a bloc fractured into two different logics of sovereignty: integration through alliance for Poland and Czechia, and insulation or ambiguity for Hungary and Slovakia. The consequence is structural. EU policy on Ukraine now advances through flexible coalitions, while NATO carries the operational centre of gravity for Central Europe's defence (Beck, 2024; Bugajski, 2025).

6. IMPLICATIONS FOR REGIONAL SECURITY AND THE EU

By 2024, the Visegrád Four had ceased to function as a security actor, unable to sustain even minimal consensus on war and deterrence. The Prague summit exposed open division and left the group in tatters (Beck, 2024). What persists is residual symbolism and low-stakes coordination, far removed from the hard security questions that dominate Europe's agenda. The significance of this collapse reaches beyond Central Europe, for it reveals where agency in Europe's security order has migrated and how EU institutions adapt when unanimity among member states collapses under pressure.

Institutionally, the most immediate consequence was procedural. Hungary's vetoes and abstentions on Ukraine-related dossiers transformed unanimity from a safeguard into a choke point. In response, European practice shifted towards coalitions of the willing for financing and capability pipelines, allowing like-minded states to carry the policy while holdouts stood aside (Rankin, 2025). This pattern exemplifies crisis governance by design: momentum is preserved at the expense of unity, accelerating the Union's long-standing drift towards variable geometry in foreign and security policy, a trend that becomes most visible

ISSN 2815-3324 Online, ISSN 2535-0358 Print

in emergencies when collective action must outrun internal blockage (Costa, Juncos, Müller, & Sjursen, 2024; Keukeleire & Delreux, 2022). The workaround in facing Hungary's and Slovakia's obstructions, however, sets a precedent. Normalising variable-geometry coordination in EU foreign and security policy risks bleeding into adjacent fields, from industrial policy to budget governance, where formal unanimity is not required but political cohesion remains essential.

Strategically, the war confirmed a hierarchical order in which NATO remains the operational backbone of European security. Eastern frontline states concentrated credible power and decision-making within the alliance rather than in EU frameworks, reshaping debates on strategic autonomy. These debates now revolve less around institutional ambition and more around the conditions under which autonomy can function within a NATO-centred order, echoing earlier analysis that warned against equating autonomy with separation from NATO or the United States (Howorth, 2019). The trajectory of the V4 reinforces this logic. Even before 2022, the four capitals had expressed a shared preference for NATO centrality and treated EU defence instruments as complements rather than substitutes (Roos, 2020). The war entrenched that preference: as Poland and Czechia anchored an Atlanticist line while Hungary resisted, the space for an EU-first defence project narrowed. What survives of autonomy is confined to capacity building and industrial coordination, without replacing the alliance's deterrent core in the East.

Poland anchors its security in NATO and the United States because it reads Russia as existential across power, proximity, capability, and intent, while Hungary emphasises cost and energy dependence and therefore resists entanglement. This divergence follows the logic highlighted in alliance theory: allies fracture when they weigh threat dimensions differently (Walt, 1987). Hungary's behaviour fits the pattern described in Pedersen's shelter diplomacy model, where small states navigate abandonment and entrapment risks by calibrating the depth of their commitments (Pedersen, 2023). Poland is not a small state, yet its proximity to Russia generates a similar fear of abandonment, which drives it to over-invest in alliance integration and rapid capability expansion. Hungary, by contrast, treats entrapment as the greater danger, justifying vetoes, hedging, and energy pragmatism. These conflicting equilibria cannot coexist inside a unanimity-based bloc and lead either to paralysis or to fragmentation into minilateral formats.

Subsequently, the EU's adaptation has two layers. At the political level, leaders increasingly authorise sub-coalitions to move first on aid, training, and procurement while keeping the door open for late joiners once domestic conditions allow. At the legal-institutional level, off-budget facilities, enhanced cooperation, and Council conclusions framed to permit constructive abstention carry the load. This pattern reflects the broader logic of EU crisis management, which relies on flexible coordination when speed is decisive (Costa, Juncos, Müller, & Sjursen, 2024), and it demonstrates how EU foreign policy operates as a multi-level process in which coalitions and institutions constantly renegotiate scope and agency (Keukeleire & Delreux, 2022). The price is greater risk of fragmentation, but the benefit is continuity of support for Ukraine and deterrence signalling to Russia even when unanimity is blocked.

Moscow's view of the Visegrád fracture has been limited and largely instrumental, with Russian officials and media showing little indication that the Kremlin regards the V4 as a meaningful strategic unit in its own right. Russia has long preferred to cultivate bilateral channels with Central European governments rather than engage with the Visegrád format as such, and this tendency only deepened after 2022, when Hungary's vetoes and Slovakia's rhetorical ambivalence created tactical openings that Moscow could exploit inside EU decision-making (Ušiak, 2024). Yet these gestures, however useful in slowing or complicating consensus in Brussels, are counterbalanced by Poland's deliberate Atlanticist attitude and Czechia's consolidation within NATO, which together anchor the region firmly inside the Euro-Atlantic security order. The fracture, in this sense, provides Moscow with a convenient set of talking points and occasional institutional leverage, but it does not alter the underlying distribution of power, leaving Russia with discursive advantages rather than structural gains (Beck, 2024).

For NATO, the V4 fracture scarcely registers. The alliance's command structure, integrated planning, and United States leadership continue to anchor Central Europe's security, with Poland's military build-up and Czechia's alignment bolstering deterrence. Hungary's dissent remains manageable thanks to NATO's focused consensus mechanisms. The war has therefore reshaped Europe's security architecture: NATO defines the hard-power boundary conditions, while the EU handles financing, sanctions, and

reconstruction through flexible coalitions that can operate without unanimity. This outcome deepens Europe's strategic dependence on NATO and the United States. Russia's invasion made Europe's reliance on American political and military support unmistakable (Ratti, 2023) and confirmed that the idea of strategic autonomy remains constrained by this reliance, with Europe still unable to act independently in a high-intensity conflict (Helwig, 2023).

The fracture within the V4 clarifies two strategic consequences. First, European strategic autonomy can only advance when anchored in NATO and translated into capability and industrial delivery, rather than imagined as the EU acting alone. As Howorth makes clear, autonomy becomes possible through strengthening the EU–NATO relationship, which consolidates rather than weakens the transatlantic bond (Howorth, 2019). Second, EU foreign policy will continue to move through minilateral leadership groups that set pace during crises, a mode better understood as the resilient face of collective action under stress, consistent with the EU's ability to adapt foreign policy cooperation despite contestation (Costa, Juncos, Müller, & Sjursen, 2024). The collapse of the V4 as a coherent actor makes both patterns more visible: it removes a once-loud regional brand from the decision table and redirects attention to formats that reflect the actual distribution of threat, will, and capacity.

Overall, the war compelled Europe to privilege function over form. The V4's negative-integration model offered no tools for deterrence, logistics, or war finance, and quickly became irrelevant. The EU adapted by allowing coalitions of the willing to carry the load, while NATO absorbed the strategic core in the East. Strategic autonomy now takes shape as usable power in industrial capacity, procurement, and coordination, functioning as a complement to the alliance order rather than a substitute for it. The settlement produced by the fracture is therefore unambiguous: the Visegrád Four no longer functions as a strategic bloc, NATO defines the hard boundary of European security, and the EU acts where it can deliver, through flexible formats and functional instruments rather than through regional unity.

7. CONCLUSION

The record of the Visegrád Four over the past decade reveals a recurrent pattern in which external shocks redefined the threat environment, governments recast sovereignty through the prism of domestic political landscapes and material exposures, and these recalibrations translated into divergent institutional choices. When danger was read as proximate and existential, the logic of survival drew governments towards depth in alliances, mass in forces, and readiness at speed; when the calculus was weighted more heavily by energy dependence or fiscal cost, the imperative shifted instead to insulation, veto capacity, and cross-dossier linkage. A grouping designed to coordinate law, procedure, and rhetoric against supranational intrusion thus reached the edge of its architecture once the object of policy became deterring a hostile military adversary, and at that threshold it fractured along incompatible definitions of risk and responsibility.

The V4 fractured under the strain of war because its unity had always rested on resisting Brussels rather than on confronting Moscow, and once security required a shared threat perception and collective risk-taking, that foundation could not hold. This trajectory illuminates the boundaries of negative-integration coalitions. They can deliver coherence in legal contestation and wield agenda-setting power when the field of struggle is the distribution of competence within the Union, yet they cannot be scaled into deterrence, logistics, or war finance, domains that demand both a shared perception of threat and a collective willingness to bear costs and risks. The cohesion that had appeared durable in the migration decade dissolved rapidly once war set the terms, for members weighted proximity, intent, and cost in different ways and relied on instruments that belonged to different institutional families.

The findings carry weight, yet they must be read with caution, for the analysis centres on a single conflict, the Russian invasion of Ukraine, which exposed the structural limits of one regional coalition. The eclipse of the V4 under wartime conditions does not prove that all negative-integration groupings will fracture under external pressure, but it does reveal a mechanism whose transferability remains uncertain. Comparative research across minilateral groups such as the Nordic Council, the Baltic Assembly, or the Benelux Union will be needed to test whether coalitions built on cooperative integration can withstand coercive shocks more effectively than those, like the V4, that were forged in opposition to supranational

authority. The study is also bounded by timing: it closes in mid-2025, when alliance planning cycles are still unfolding and politics in Bratislava and Budapest remain unsettled. The findings therefore rest on the best open evidence available, and while refinement will follow as new material emerges, the causal pathway identified here remains stable.

The fracture of the V4 was absorbed by the wider system, as unanimity rules turned into choke points and momentum shifted towards coalitions of the willing, off-budget mechanisms, and Council formulations crafted to permit constructive abstention. This mode of flexible coordination preserved movement at the expense of visible unity. At the same time, the war reaffirmed NATO's primacy as the operational backbone of European security, while the EU retained relevance in financing, sanctions, reconstruction, and industrial scaling only insofar as coalitions could sustain decisions. In this setting, strategic autonomy survives less as a stand-alone project than as a function embedded in the alliance order and expressed through tangible capabilities and industrial delivery.

Although the V4 has ceased to matter as a security actor, it does not vanish altogether. What remains are residual functions that occupy the softer terrain of European cooperation: cultural and educational initiatives, research exchanges, occasional coordination on infrastructure, and the ritualised summitry that preserves the appearance of continuity. These activities sustain a symbolic presence, but they do not alter the structural verdict on security. Rather, they show that the bloc persists as form and protocol even as substance has migrated elsewhere.

The eclipse of the Visegrád Group cannot be reduced to personalities or passing quarrels but reflects the deeper fact that its architecture was built for resisting Brussels rather than for managing war, and once Moscow set the terms that foundation dissolved, leaving behind little more than a shell while strategic decisions moved through NATO, through coalitions within the EU, and through minilateral formats that map more closely onto the actual distribution of threat, will, and capacity across the continent.

REFERENCES

Balogh, P., & Kovály, K. (2025). Small but salient: The securitization of Ukraine's ethnic Hungarian minority. *Nationalities Papers, 53*(4), 798–821. https://doi.org/10.1017/nps.2024.51

Beck, R. (2024, April 3). *The Visegrád Four: From troubled to broken*. Foreign Policy Research Institute. https://www.fpri.org/article/2024/04/visegrad-four-from-troubled-to-broken/

Bugajski, J. (2025, January 14). *Poland seeks more effective regional formats as the Visegrád Group fractures*. Jamestown Foundation. https://jamestown.org/program/poland-seeks-more-effective-regional-formats-as-the-visegrad-group-fractures/

Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press.

Costa, O., Juncos, A. E., Müller, P., & Sjursen, H. (2024). Contested but resilient: Accounting for the endurance of the European Union's foreign policy. *JCMS: Journal of Common Market Studies*. Advance online publication. https://doi.org/10.1111/jcms.13686

Court of Justice of the European Union. (2017, September 6). *Slovakia and Hungary v Council of the European Union* (Joined Cases C-643/15 and C-647/15). https://curia.europa.eu/juris/liste.jsf?num=C-643%2F15

Court of Justice of the European Union. (2020, April 2). *European Commission v Republic of Poland, Hungary and Czech Republic* (Joined Cases C-715/17, C-718/17 and C-719/17). https://curia.europa.eu/juris/liste.jsf?num=C-715/17

Dangerfield, M. (2008). The Visegrád Group in the enlarged European Union: From preaccession to postaccession cooperation. *East European Politics and Societies, 22*(3), 630–667. https://doi.org/10.1177/0888325408315840

Dangerfield, M. (2012). Visegrád cooperation, enlargement, and the European Neighbourhood Policy. *East European Politics and Societies, 26*(2), 394–418. https://doi.org/10.1177/0888325411435942

Dębiec, K. (2024, October 8). *"Dr Fico and Mr Hyde": Slovakia's game with Ukraine and Russia*. OSW – Centre for Eastern Studies. https://www.osw.waw.pl/en/publikacje/analyses/2024-10-08/dr-fico-and-mr-hyde-slovakias-game-ukraine-and-russia

Gizińska, I., & Sadecki, A. (2025, March 28). *Hungary hardens its stance on Ukraine*. OSW – Centre for Eastern Studies. https://www.osw.waw.pl/en/publikacje/analyses/2025-03-28/hungary-hardens-its-stance-ukraine

Gkliati, M. (2022). The next phase of the European Border and Coast Guard: Responsibility for returns and push-backs in Hungary and Greece. *European Papers*, 7(1), 171–193. https://doi.org/10.15166/2499-8249/553

Government of Poland. (2020). *National Security Strategy of the Republic of Poland*. Bureau of National Security. https://www.bbn.gov.pl/ftp/dokumenty/National Security Strategy of the Republic of Poland 2020.pdf

Helwig, N. (2023) EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War. *JCMS: Journal of Common Market Studies*, 61: 57–67. https://doi.org/10.1111/jcms.13527

Howorth, J. (2019, August 8). *Strategic autonomy: Why it's not about Europe going it alone*. Martens Centre. https://www.martenscentre.eu/publication/strategic-autonomy-why-its-not-about-europe-going-it-alone/

Ivanova, D. (2016). Migrant Crisis and the Visegrád Group's Policy. *International Conference Knowledge-Based Organization*, *22*(1), 35–39. https://doi.org/10.1515/kbo-2016-0007

Janulewicz, Ł. (2020, June 23). *Poland's new National Security Strategy: The potential for regional leadership, cooperation and cohesion on NATO's eastern flank*. RUSI Commentary. https://www.rusi.org/explore-our-research/publications/commentary/polands-new-national-security-strategy-potential-regional-leadership-cooperation-and-cohesion-natos

Jones, P. (2023, September 28). *Poland becomes a defense colossus*. CEPA. https://cepa.org/article/poland-becomes-a-defense-colossus/

Kaniok, P., & Hloušek, V. (2025). Visegrad Four as an institution in times of EU crises. *European Politics and Society*, 1–19. https://doi.org/10.1080/23745118.2025.2488815

Keukeleire, S., & Delreux, T. (2022). *The foreign policy of the European Union* (3rd ed.). Bloomsbury Publishing.

Lake, D. A. (2009). *Hierarchy in International Relations*. Cornell University Press.

Nagy, B. (2016). Hungarian Asylum Law and Policy in 2015–2016: Securitization Instead of Loyal Cooperation. *German Law Journal*, *17*(6), 1033–1082. doi:10.1017/S2071832200021581

NATO Parliamentary Assembly. (2023, March 23). *Poland plays leading role in garnering support for Ukraine's defence, reconstruction and accession to Euro-Atlantic institutions*. https://www.nato-pa.int/news/poland-plays-leading-role-garnering-support-ukraines-defence-reconstruction-and-accession-euro

Pedersen, R. B. (2023). *Small states shelter diplomacy: Balancing costs of entrapment and abandonment in the alliance dilemma*. *Cooperation and Conflict, 58*(4), 441–459. https://doi.org/10.1177/00108367231164497

ISSN 2815-3324 Online, ISSN 2535-0358 Print

Rankin, J. (2025, March 2). *Orbán problem pushes EU towards "coalitions of the willing" on Ukraine*. *The Guardian*. https://www.theguardian.com/world/2025/mar/02/orban-problem-pushes-eu-towards-coalitions-of-the-willing-on-ukraine-russia

Ratti, L. 2023. "NATO and the CSDP After the Ukraine War: The End of European Strategic Autonomy?". *Canadian Journal of European and Russian Studies* 16 (2):73-89. https://doi.org/10.22215/cjers.v16i2.4150

Reuters. (2023, October 26). *Slovakia's Fico will not support more military aid to Ukraine at EU summit*. https://www.reuters.com/world/europe/slovakias-fico-will-not-support-more-military-aid-ukraine-eu-summit-slovak-media-2023-10-26/

Reuters. (2025, March 7). *Orban says financing Ukraine's war effort would "ruin Europe."* Reuters. https://www.reuters.com/world/europe/hungary-pm-orban-financing-ukraine-would-ruin-europe-2025-03-07/

Roos, G. (2020, December 4). *The V4 and EU strategic autonomy: Consensual voice, discordant tones?* GLOBSEC. https://www.globsec.org/what-we-do/publications/v4-and-eu-strategic-autonomy-consensual-voice-discordant-tones

Scharpf, F. W. (1999). *Governing in Europe: Effective and democratic?* Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198295457.001.0001

Ušiak, J. (2024). Navigating new waters: Russian military aggression on Ukraine and effects on the Visegrad Group. *Revista UNISCI/UNISCI Journal, 66,* 1–22. http://dx.doi.org/10.31439/UNISCI-208

Visegrad Group. (2015, September 4). *Joint Statement of the Heads of Government of the Visegrad Group countries*. https://www.visegradgroup.eu/home/documents/2015/joint-statement-of-the-150904

Walt, S. M. (1987). *The Origins of Alliances*. Cornell University Press.

.

Guennoun, Y. (2025). From crisis to doctrine: A decade of migration securitization and strategic defiance in Hungary. *Politics & Security, 13*(3), 46–57. Doi: 10.54658/ps.28153324.2025.13.3.pp.46-57

FROM CRISIS TO DOCTRINE: A DECADE OF MIGRATION SECURITIZATION AND STRATEGIC DEFIANCE IN HUNGARY

Yassine Guennoun
Sidi Mohammed Ben Abdellah University
Fez, Morocco
yassine.guennoun@usmba.ac.ma
https://orcid.org/0009-0003-8777-9781

Abstract. *This article examines how Hungary, between 2015 and 2025, reworked migration policy into a doctrine of sovereignty-driven securitization. What started as short-term crisis responses became a governing toolkit that joined restrictive law, threat-heavy messaging, and calculated non-compliance with EU rules. Read through securitization theory and differentiated integration, the shift turns migration from a welfare or demographic matter into the main stage for asserting state sovereignty. The study employs a critical case study design, drawing on governmental speeches, EU court rulings, media campaigns, and regional declarations, alongside secondary scholarship. The findings demonstrate that Hungary not only entrenched legal resistance and fortified its borders with symbolic and technological infrastructures, but also mobilised regional alliances to contest supranational authority. In doing so, it recast European integration as conditional and strategically reversible. The article argues that Hungary exemplifies a broader post-liberal mode of governance in which the language and institutions of liberal order are retained yet redirected toward sovereignty-first objectives. The case offers a potential template for how member states can recalibrate supranational authority from within, embedding fragmentation as a structural condition of the European project.*

Keywords: Migration, securitization, Hungary, sovereignty, European Union, strategic non-compliance, compliance minimalism, post-liberal governance.

1. INTRODUCTION

In his 2025 State of the Nation address, Hungarian Prime Minister Viktor Orbán once again placed migration at the centre of Hungary's political identity. He rejected the European Union's New Pact on Migration and Asylum as an existential imposition and credited his government with defending the nation against demographic and cultural dissolution (Orbán, 2025). This declaration was not an isolated flourish. It capped a decade in which migration pressures, the geopolitical turbulence of the war in Ukraine, and continued movements from Africa and the Middle East combined to shape Hungary's security posture. Since 2015, the government has assembled what it now treats as a migration security doctrine. This framework reshapes domestic governance while recalibrating Hungary's relationship with European norms on borders, law, and solidarity.

This article contends that Hungary's migration stance between 2015 and 2025 is best understood as the consolidation of a sovereignty-centred securitization doctrine. Hungary's doctrine operates on three connected fronts: legislative restriction, symbolic narrative, and persistent defiance of EU legal demands. Rather than isolated measures, these fronts interlock into a single logic that draws authority from a civilisational threat narrative. Migration is cast as a stand-in for broader geopolitical struggles rather than as a social challenge, allowing the state to speak both as Europe's sentinel and as its critic.

This trajectory reflects a wider shift toward what can be described as post-liberal security governance. Integration mechanisms remain in place, but they are redirected to privilege sovereignty over collective norms. Legal instruments, institutional procedures, and even the language of compliance are

ISSN 2815-3324 Online, ISSN 2535-0358 Print

retained, yet retooled to consolidate national authority. Unlike the government's preferred label of "illiberalism" (Orbán, 2014), post-liberal governance is less a slogan than a method of rule. Thus, post-liberal governance preserves the institutional shell of liberal democracy, keeping courts, procedures, and compliance scripts formally intact. Yet these are reoriented to sovereignty-first objectives through legal redesign, administrative practice, and symbolic politics.

The argument builds on securitization theory (Buzan, Wæver, & de Wilde, 1998; Huysmans, 2006) and on differentiated integration (Schimmelfennig, 2018) to map the transition from emergency reaction to durable state doctrine. Border construction, asylum law reform, and targeted public campaigns did not remain temporary tools. They were assembled into a coherent strategy that endures beyond crisis moments. Within this framework, the state elevates migration from a demographic or humanitarian question to an existential vector of risk that legitimises institutional reconfiguration, political centralization, and heightened executive authority.

Existing scholarship maps core aspects of this transformation. Research traces how migration securitization shaped electoral dynamics in favour of the ruling party (Bíró-Nagy, 2021; Batory, 2021) and how intensified border practices reframed territorial governance and national identity (Waterbury, 2020; Scott, 2023). Officials spoke of Ukrainians in humanitarian terms while casting the 2015 arrivals as a danger, producing a selective humanitarianism filtered by ethnicity and geopolitics (Vidra & Messing, 2025). Taken together, the literature points to a field organised by clear lines of inclusion, exclusion, and legitimation.

At the European level, Hungary has resisted integrationist migration governance. It refused the EU's 2015 relocation quotas, litigated in the Court of Justice of the European Union (CJEU, 2020), and enacted legislation criminalizing civil assistance to asylum seekers (CJEU, 2021). Hungary remains outside the core proposals of the New Pact (European Commission, 2020) and promotes alternatives through the Visegrád Group (Visegrád Group, 2021). The European Parliament's 2022 report links migration policy to a broader pattern of democratic erosion (European Parliament, 2022). The case exposes enforcement gaps in EU governance and shows how member states can leverage institutional fragmentation to assert autonomy.

This article makes two contributions. It first identifies the legal, symbolic, and institutional elements of Hungary's migration securitization as parts of a unified doctrine. It then evaluates how this doctrine interacts with and reshapes European migration governance, institutional coherence, and security integration. In doing so, the analysis demonstrates how selective adherence and strategic non-compliance recalibrate the boundaries of European integration. Post-liberal governance emerges as a process of refunctionalisation: institutional forms remain intact, yet their operational purpose shifts toward sovereignty consolidation.

The structure follows directly from this agenda. Section 2 outlines the methodological approach, Section 3 presents empirical findings by period and theme, Section 4 interprets them through securitization and differentiated integration theory, and Section 5 draws implications for EU migration policy and institutional cohesion.

2. MATERIALS AND METHODS

This critical case study treats Hungary as a strategic exemplar of sustained migration securitization and its implications for European security governance. Case selection rests on three grounds. First, a coherent securitization narrative spans a full decade, enabling longitudinal analysis. Second, the approach generated legal, political, and symbolic confrontations with EU institutions, exposing tensions between sovereignty claims and supranational governance. Third, Hungary projected its model through the Visegrád Group, creating a vector for diffusion and coordinated resistance.

The framework joins securitization theory (Buzan, Wæver, & de Wilde, 1998) with differentiated integration (Schimmelfennig, 2018; Genschel & Jachtenfuchs, 2014). This dual lens links threat construction to the elasticity of multilevel governance and clarifies how states assert sovereignty from within EU structures.

2.1 Data and triangulation

The corpus covers 2015-2025 and spans six source classes, each tied to a specific analytic function. Texts were coded thematically around policy instruments, compliance events, and framing signifiers, then cross-checked across source classes for convergence.

1. Governmental speeches and consultations

State of the Nation addresses (2017, 2022, 2025), National Consultations ("Stop Brussels!", "Soros Plan"), and official communications on the New Pact. Function: identify securitizing moves, stated objectives, and claimed mandates.

2. EU legal and policy texts

CJEU judgments (C-808/18, C-821/19), the Commission's 2020 New Pact Communication, and the European Parliament's 2022 Article 7 report. Function: establish legal baselines, breach points, and institutional responses.

3. Media ecosystem and NGO monitoring

Hungarian Helsinki Committee reports on enforcement patterns, combined with (Vidra & Messing, 2025) on post-Ukraine discourse. Function: observe framing, practice, and adaptation.

4. Peer-reviewed scholarship

Core studies in securitization and integration documenting institutional change (e.g., Bíró-Nagy, 2021; Waterbury, 2020; Scott, 2023). Function: theoretical anchoring and longitudinal interpretation.

5. Regional and intergovernmental declarations

Visegrád Group communiqués and joint statements (2015–2021). Function: trace coordination on relocation, border control, and "flexible solidarity."

6. Regional comparative research

V4-focused analyses of migration and crisis governance, including work on the Ukraine divergence (e.g., Czyż, 2024; Glied & Zamęcki, 2021). Function: corroborate diffusion patterns and the weakening of bloc coherence after 2022.

2.2 Units Of Analysis And Coding

Units of analysis are distinct policy acts, legal decisions, official speech events, media campaign artifacts, and regional declarations. Close textual analysis was paired with thematic coding of instruments (fences, surveillance, asylum procedures, NGO regulation), compliance events (infringement actions, CJEU outcomes, administrative responses), and signifiers (sovereignty, security threat, civilisational danger, illegal migration, Brussels imposition). Coding proceeded iteratively with constant comparison. For each unit the analysis recorded source, date, actor, instrument, and signifier set to enable temporal mapping.

2.3 Analytic Strategy

The framework joins securitization theory (Buzan, Wæver, & de Wilde, 1998; Huysmans, 2006) with differentiated integration (Schimmelfennig, 2018; Genschel & Jachtenfuchs, 2014) to trace how threat construction travels into institutional design within a multilevel governance field. The strategy combines process tracing across 2015–2025 to link discourse, law, technology, and diplomacy; triangulation across source classes to test convergence and identify discrepancies; a contrastive reference to the German reception trajectory to situate crisis governance choices; and a regional lens on V4 coordination to capture diffusion and fracture.

2.4 Design And Epistemic Stance

The study is structured as a theory-oriented plausibility probe (George & Bennett, 2005) that uses a crucial, most-likely case to test mechanism plausibility. The purpose is conceptual refinement rather than sample-wide generalization. The epistemic stance is illustrative-analytical within an interpretivist logic, sharpening theory through close tracing of institutional, discursive, and symbolic structures. This orientation aligns with the post-liberal turn in European security governance, where states retain liberal-

democratic forms and refunctionalise them toward sovereignty-first outcomes (Lottholz, 2022). Internal validity rests on triangulation across legal documents, government communication, and secondary monitoring sources. The design's reliability follows from structured coding protocols, while the single-case scope limits external generalization and instead advances mechanism plausibility.

3. RESULTS

3.1 From Crisis Response to Sovereign Doctrine (2015–2016)

Hungary's securitization drive moved into high gear during the 2015 refugee crisis and, from there, laid the groundwork for a lasting governance approach. The immediate policy responses included the construction of a 175-kilometer border fence along Hungary's southern frontier, the declaration of a "migration state of emergency," (Jaroszewicz & Gniazdowski, 2015) and significant amendments to the Asylum Act enabling rapid rejection of claims and establishing transit zones as de facto detention centres.

These measures diverged sharply from the humanitarian approach adopted by Germany, whose policy under Chancellor Merkel prioritised moral responsibility and legal protection obligations (Schammann et al., 2021). While Germany mobilised institutional capacity toward reception and integration, Hungary's leadership portrayed the same events as a civilisational confrontation, embedding the language of existential threat into state policy from the outset. This contrast reveals Hungary's path not as a reactive aberration, but as a calculated strategic departure from dominant EU crisis governance norms.

State-sponsored campaigns such as "Let's Stop Brussels!" and the "Soros Plan" consultations portrayed the EU not only as a threat to Hungary's demographic and cultural integrity but as an active agent undermining national sovereignty (Hungarian Government, 2017). The October 2016 national referendum on the EU's mandatory refugee quotas, with 98% of valid votes rejecting the quotas despite insufficient turnout for legal validity, was presented domestically as a public mandate for defiance (Batory, 2021). This strategic attitude extended migration securitization beyond immediate border protection, embedding it deeply within Hungary's political, legal, and symbolic governance frameworks.

Legally exceptional, symbolically civilisational, strategically defiant. This triadic pattern began defining the emergent doctrine.

3.2 Institutionalizing Legal Defiance (2017–2020)

Between 2017 and 2020 Hungary moved from emergency measures toward an entrenched confrontation with EU institutions. In 2018 the government introduced the so-called *Stop Soros* legislative package, which criminalised assistance to asylum seekers and placed direct pressure on NGOs and legal aid providers (Hungarian Government, 2018). The Court of Justice of the European Union later found these measures incompatible with EU law (CJEU, 2021). Brussels launched infringement procedures in response, and the Court of Justice of the European Union delivered rulings in 2020 and 2021 declaring Hungary's practices incompatible with Union law (CJEU, 2020; 2021).

These judgments, however, did not lead to policy reversal. Hungary maintained its restrictive agenda and recast adverse EU rulings as illegitimate intrusions into sovereignty, presenting non-compliance as proof of resolve rather than liability (Gkliati, 2022; Prime Minister's Office, 2022). The Hungarian defiance was woven directly into domestic political theatre, as speeches and campaigns depicted Brussels as an overreaching outsider and used the slow pace of EU legal procedures to reinforce the claim of acting with a national mandate.

By 2020, the right to asylum at Hungary's borders had been hollowed out. Formal membership in the EU continued, along with the disputes before European courts, yet access to protection on the ground had nearly vanished. At the same time, the government's rhetoric grew more ideological. References to "population replacement," "cultural invasion," and the decline of Christian Europe became central motifs in Hungary's securitization discourse (Sukosd, 2022; Scott, 2023). This vocabulary echoed narratives circulating across European and American far-right discourse, anchoring the securitization agenda more

firmly in the state's governing framework (Lamour, 2023; Weninger, 2025). Taken together, these legal defiance strategies and ideological framings transformed migration from a policy challenge into a cornerstone of Hungary's sovereignty doctrine, fusing domestic politics with a broader post-liberal model of governance.

Domestic opposition did not vanish. Civil-society groups and legal aid organisations repeatedly litigated and documented practices at the border, winning CJEU rulings even if enforcement lagged. In parliament, opposition MPs increased the number of bills tabled in the 2018–2022 term, but their success rate remained below one percent, and procedural reforms curtailed scrutiny. Oversight instruments such as interpellations and committees of inquiry survived in form yet were blunted in practice, often neutralised by government majorities or even co-opted through "self-interpellation." Resistance thus persisted, but it was structurally contained by the government's dominance and by the embedding of the sovereignty-first doctrine in law and administration (Tanács-Mandák, 2025).

3.3 Post-Ukraine Paradox and Selective Humanitarianism (2022–2023)

The war in Ukraine set a decisive test. Within months more than one million refugees crossed into Hungary, confronting a state that had long framed mass arrival as a civilisational threat. Officials and major outlets presented these arrivals in positive, proximate terms that matched a self-image of European, Christian, and culturally aligned populations (Vidra & Messing, 2025).

Brussels pressed for military and financial support to Kyiv while Hungary withheld arms and prioritised domestic energy security and bilateral channels with Moscow. Partners read this stance as obstruction inside the Union's crisis response (Czyż, 2024; European Parliament, 2022). The policy mix produced a clear pattern. Humanitarian assistance flowed where ethno-cultural proximity and geopolitical alignment could be claimed. Those outside that frame met systemic barriers. Pushbacks and the effective denial of protection persisted for asylum seekers from the Middle East and Africa (Hungarian Helsinki Committee, 2023). This conditionality carried institutional consequences. Hungary extended help while reaffirming a sovereignty filter that privileges national identity over universal asylum principles (Vidra & Messing, 2025). The approach exposed a wider weakness in EU migration governance, where formal commitments can be selectively implemented in ways that undercut supranational coherence (Gkliati, 2022).

Regionally, the war fractured earlier Visegrád alignment. Poland, Slovakia, and Czechia supplied military and humanitarian aid to Ukraine. Hungary held its line on neutrality and energy ties. Bloc cohesion thinned, yet the migration stance remained coordinated. Opposition to mandatory relocation endured, and flexible solidarity stayed in use as an organising frame (Czyż, 2024; Glied & Zamęcki, 2021).

Taken together, the Ukraine episode crystallised the method. Humanitarian aid moved through an identity filter, alliance politics shifted with energy and war, and the migration line held. The doctrine proved adaptable and resistant to concession. Symbols were adjusted, core structures kept in place, and each crisis was used to validate sovereignty claims while exposing weaknesses in EU enforcement and coordination.

3.4 Migration Pact and 2025 Doctrinal Apex

In 2024-2025 the approach reached its clearest form. The New Pact on Migration and Asylum became the focal dispute. In the 2025 State of the Nation address, Orbán rejected the pact as demographic engineering and a direct threat to sovereignty (Orbán, 2025). The stance drew on a decade of legal reinterpretation, administrative slow-rolling, and regional messaging. Although Visegrád unity thinned after the war in Ukraine, Hungary kept the frame alive by centring "sovereignty" and "flexible solidarity" in regional language, with earlier joint statements as reference points (Visegrád Group, 2021; Czyż, 2024).

Border infrastructure expanded and upgraded in 2024 and early 2025. Surveillance systems multiplied, biometric screening became routine, and fencing was extended. These choices turned defence rhetoric into hardware and made migration control a visible claim to sovereign authority (Human Rights Watch, 2025; Khoury & Hendow, 2025; European Digital Rights et al., 2025).

ISSN 2815-3324 Online, ISSN 2535-0358 Print

By mid-2025, message control, legal resistance, and technological build-out operated as one system. Migration policy functioned as a tool of sovereign authority at home and as a workable playbook for resisting supranational constraints from inside the Union.

4. DISCUSSION

Between 2015 and 2025, migration policy in Hungary became a textbook case of securitization, and then moved beyond the classical model. An emergency response turned into a rule-making doctrine that reorganised institutions and external relations. Migration stopped being treated as a narrow social issue and became a lens for rewriting law, politics, and Hungary's place in Europe. The discussion traces four consequences: a threat narrative turned into durable rule; legal pushback that recast EU norms; border practices that built lasting symbols; and a regional spread of the model.

4.1 From Speech Act to Structural Doctrine

Within the Copenhagen School, securitization is the move that casts an issue as an existential threat that justifies exceptional measures (Buzan, Wæver, & de Wilde, 1998). Hungary's steps in 2015 fit that description. By 2025, the logic was embedded in statutes, media strategies, alliance choices, and surveillance systems organised around civilisational defence.

This path echoes Huysmans' account of "insecurity politics," where fear production stabilises authority (Huysmans, 2006). Migration became a flexible signifier that reinforced sovereignty, concentrated power, and sustained legitimacy. The story reduced politics to a choice between national autonomy and external imposition.

Critical work is a reminder that practice and infrastructure matter alongside speech (McDonald, 2008; Aradau & Blanke, 2010). In Hungary, biometrics, administrative filtering, and dense media cycles kept a sense of permanent risk in play. The operative goal was to re-engineer integration selectively in favour of sovereignty. Institutions stayed in place and, in many areas, intensified, but their normative direction tilted toward domestic control. In short, threat talk and structural redesign moved together to produce a security order built to outlast electoral time.

4.2 Strategic Non-Compliance and the Rewriting of EU Norms

Hungary shows how a member state can routinise non-compliance without leaving the Union. It resisted relocation quotas, stalled the New Pact on Migration and Asylum, and continued practices the CJEU found unlawful, exploiting weak EU enforcement in a field where implementation depends on national authorities and political will (Gkliati, 2022). Hungary's strategy performs formal alignment to preserve access to EU benefits while disabling unwanted rules in core state functions (Schimmelfennig, 2018). A simple contrast makes the stakes clear. Germany framed migration as a shared management problem requiring coordination, while Hungary cast it as a sovereignty test and converted Brussels' pushback into domestic legitimacy (Schammann et al., 2021).

In this field it is useful to distinguish two modes of defiance. Strategic non-compliance refers to deliberate and open rejection of EU law, exchanged for domestic political gain even when it brings legal or fiscal costs. Compliance minimalism refers to formal adherence to procedures and the letter of rules while neutralising their substance in practice. The former contests rules directly, the latter hollows them out.

The result in Hungary is compliance minimalism within a post-liberal governance mode: institutional forms persist while their normative content is redirected toward sovereignty consolidation (Lottholz, 2022). This method can be replicated, but only under specific conditions. It requires weak EU enforcement in a high-discretion field such as migration, long remedial timelines that allow domestic practices to entrench, sustained domestic demand for sovereignty-first framing, and access to regional coordination that normalises selective adherence. Where such conditions are absent, diffusion remains partial and outcomes converge toward symbolic alignment rather than structural change.

4.3 The Symbolic Border as Security Infrastructure

Hungary's border regime operates as deterrent and as stage. Fencing, surveillance systems, and biometric controls assemble into a security dispositif in Foucault's sense, a material and discursive apparatus that manufactures a durable perception of threat and organises conduct around it (Foucault, 2007). The continued upgrading long after peak arrivals signals priority for political symbolism over throughput management. The border's function is to show sovereignty at work.

Symbolic charge is produced through repetition and visibility. Camera towers, patrol footage, press events, and official briefings convert routine enforcement into a ritual of protection. Government-aligned outlets routinely link migration with crime, disease, and cultural decline, filling the information space with cues that justify constant vigilance (Sukosd, 2022). Image and hardware feed each other: the more the fence appears in public view, the more it reads as the source of order.

Technology then fixes the arrangement. Camera grids expand, biometric checks become routine, and layered barriers raise the procedural price of entry. Discretion at the edge narrows, decisions shift into technical systems, and what began as exception turns into daily administration. Unwinding the setup becomes costly once cameras, databases, and patrol rhythms are in place, whatever the level of arrivals (Human Rights Watch, 2025; Khoury & Hendow, 2025; European Digital Rights et al., 2025).

Security here works by regulating movement and sorting risk, not only by speech (Aradau & Blanke, 2010). Bodies are filtered, mobilities managed, and a civilisational defence is made tangible in steel and sensors. The result is a border order that both deters and performs, turning securitization from a claim into an institutional habit.

4.4 The Regional Export of the Hungarian Model

Visegrád gave the doctrine a regional route. Poland, Slovakia, and Czechia drew on its core elements: existential sovereignty framing and a firm refusal of binding relocation. The outcome was bloc resistance that strained supranational consensus. "Flexible solidarity" moved from slogan to operating principle. In core state domains such as security, borders, and migration, integration is especially vulnerable to rollback, and Hungary's approach tapped that vulnerability (Genschel & Jachtenfuchs, 2014).

Transnational networks of think tanks, media hubs, and state-backed institutes helped the spread by normalising sovereignty-first politics and supplying channels for policy transfer (Coman et al., 2025). Hungary's stance exports a governance logic that institutionalises resistance from within EU procedures.

Notwithstanding, diffusion was uneven, and the war in Ukraine split earlier Visegrád alignment. Poland and Czechia adopted firm pro-Ukrainian positions, while Hungary mainly refused arms transfers and prioritised national interest (Czyż, 2024). The split confirms a post-liberal pattern. Symbolic coherence can persist while strategic alliances shift. Sovereignty-first governments preserve liberal veneers and recalibrate partnerships to fit domestic imperatives, sustaining the appearance of regional unity inside a reoriented order (Lottholz, 2022; Kim, 2023). Yet the Ukraine-era fracture has reduced the bandwidth for coordinated high-stakes action. Residual convergence on migration frames is likely to persist, but diminished political capital and divergent security priorities make a reprise of the 2015–2020 bloc-wide veto strategy far less certain.

4.5 Implications for Securitization and Integration Theory

The case pushes both sets of theory. In doing so, it also clarifies the distinction between the two compliance modes that shape the trajectory of internal disintegration. Strategic non-compliance contests EU rules openly, trading legal or fiscal costs for political gain at home. Compliance minimalism performs adherence to procedures and the letter of rules while neutralising their substance in practice. Together these modes explain how Hungary recalibrated integration from within. For securitization theory, the case shows how an initial speech act settles into an infrastructure of rule: claims travel into statutes, budgets, procurement, and routines, and security becomes an everyday operating system rather than a temporary exception (Buzan, Wæver, & de Wilde, 1998; Huysmans, 2006). For integration, it lays out an internal

ISSN 2815-3324 Online, ISSN 2535-0358 Print

disintegration pathway: strategic non-compliance erodes a policy field while formal membership stays intact. Moreover, it specifies audience dynamics under conditions of repetition. Legitimacy is reproduced through cyclical rituals of boundary drawing and selective humanitarianism, which refresh consent without reopening first-order debates (McDonald, 2008; Aradau & Blanke, 2010; Balzacq & Guzzini, 2015).

The case extends integration theory further by formalising a disintegration mechanism that operates through practice rather than exit. Strategic non-compliance erodes a policy field by refusing enforcement, while compliance minimalism hollows out implementation. Administrative delay, legal reinterpretation, and coalition work inside the Council convert binding rules into optional guidance. This is differentiated disintegration by design rather than drift (Schimmelfennig, 2018). The enforcement gap in migration makes this strategy scalable, since implementation rests on national authorities with high discretion and uneven incentives (Gkliati, 2022).

Two additional concepts refine this picture. Governance hardening names the conversion of short-term emergency into durable institutional architecture. Compliance minimalism names the selective performance of EU duties that preserves access to benefits while filtering obligations. Taken together, they capture how sovereignty-first states recalibrate supranational authority from within, signalling adherence in form while shifting substance in practice.

These refinements carry testable propositions. Where security infrastructures expand and narrative cycles intensify, exceptional measures are likely to persist beyond the initiating shock. Where enforcement relies on national implementation and judicial timelines are slow, compliance minimalism will spread through policy emulation and bloc coordination. Where governments can trade symbolic alignment for procedural obstruction, internal disintegration will advance without formal opt-outs.

Placed in a wider frame, Hungary functions as a forerunner of post-liberal security governance. Sovereignty-first states retain the institutional shell of integration but redirect its content toward national closure while remaining inside common structures. The result is a Europe that appears integrated and works as a patchwork. This is the theoretical horizon that the case makes visible and actionable.

5. CONCLUSION

This article has traced how a set of crisis measures adopted in 2015 settled into Hungary's governing doctrine on migration. Over a decade, restrictive legislation, message discipline, and border practice combined into a single operating logic of sovereignty-first rule, as threat talk moved from podium lines to statutes, budget lines, procurement decisions, and routine administration. EU membership continued, yet participation increasingly took shape on Hungary's terms.

Three empirical outcomes stand out. First, securitization became embedded in everyday state machinery, shaping laws, funding choices, and bureaucratic routines rather than appearing only in moments of exception. Second, legal resistance hardened into method: adverse rulings were absorbed without meaningful reversal, while compliance was curated to preserve access to EU benefits and filter obligations. Third, borders were turned into visible instruments of authority, as fencing, surveillance networks, and biometric checks built a material and symbolic architecture that is costly to unwind.

The regional dimension amplified these dynamics. Through the Visegrád channel, Budapest helped move "flexible solidarity" from slogan to operating principle. Further, the war in Ukraine then exposed the limits of bloc cohesion, with Poland and Czechia adopting clear pro-Ukrainian positions while Hungary maintained a narrow sovereignty line on aid and energy. That fracture, however, did not erase earlier convergence on migration, which is analytically revealing: post-liberal governance adapts to shifting geopolitics while preserving its institutional shell, allowing a measure of symbolic coherence to survive even as alliances shift.

Conceptually, the paper identifies two travelling mechanisms organising this story over a decade. Governance hardening captures the conversion of emergency tools into stable institutional architecture and compliance minimalism captures the selective performance of EU obligations that maintains the form of adherence while shifting substance in practice. Taken together, these mechanisms explain how threat politics endures and how integration can be trimmed from within without formal opt-outs.

Theoretically, the Hungarian decade pushes securitization analysis beyond the initiating speech act toward the infrastructures, media ecologies, and administrative routines that keep threat governance running. For integration theory, it details an internal disintegration track that operates through delay, reinterpretation, and coalition work inside EU procedures, yielding a pattern of differentiated disintegration pursued as strategy rather than drift. The resulting picture is of a Europe that appears integrated yet operates as a patchwork.

Methodologically, a critical, theory-oriented case study can do more than illustrate. By triangulating legal texts, government communication, media output, and regional statements, the analysis shows where and how a doctrine settles and offers a template for tracing similar moves in other high-discretion, thin-enforcement domains.

Policy implications follow. If EU rules are to bind, enforcement must be felt at the point of implementation, not deferred to courts alone. Monitoring should cover practices and infrastructures as well as formal transposition, because technologies and routines quietly reshape the application of rules. Border management systems require sustained oversight so that biometric and surveillance infrastructures do not set de facto terms of governance. Regional coordination should anticipate shifting alignments and invest in issue-specific coalitions capable of sustaining policy through geopolitical shocks.

Limits remain and call for caution in generalization. Hungary is a forerunner rather than a universal template, and national histories and institutional legacies shape how doctrines take root. Future work should test the reach of governance hardening and compliance minimalism across other EU member states and across adjacent policy fields such as policing, digital regulation, or public health, while close study of how officials and media actors sustain doctrines in daily practice would deepen understanding of persistence and change.

Looking beyond 2025, three tensions are likely to steer the doctrine's trajectory. Technology-led hardening at the border will continue as biometric and surveillance systems expand, embedding sovereignty claims in infrastructure. Judicial–administrative frictions will persist as additional adverse rulings meet entrenched practice, renewing clashes between legal principle and political authority. Shifting regional alignments may lower the collective payoff from coordinated defiance even as a measure of symbolic convergence endures. None of these dynamics points to simple reversal; together they imply path-dependent persistence punctuated by periodic recalibration.

The core finding stands; between 2015 and 2025, Hungary turned migration into the primary arena where sovereignty is asserted at home and negotiated with Europe. The doctrine endures because it is inscribed in law, infrastructure, and routine, and, seen through the paired mechanisms of governance hardening and compliance minimalism, it offers a script that others can adapt where conditions permit. If widely emulated, this script would entrench fragmentation as a structural condition of the Union, with migration as the decisive site where sovereignty and integration collide.

REFERENCES

Aradau, C., & Blanke, T. (2010). Governing circulation: A critique of the biopolitics of security. In M. de Larrinaga & M. G. Doucet (Eds.), *Security and global governmentality: Globalization, governance and the state* (pp. 41–56). Routledge.

Balzacq, T., & Guzzini, S. (2015). Introduction: 'What kind of theory – if any – is securitization?'. International Relations, 29(1), 97-102. https://doi.org/10.1177/0047117814526606a

Batory, A. (2021). Hungary's EU Refugee Relocation Quota Referendum: 'Let's Send a Message to Brussels'. In: Smith, J. (eds) The Palgrave Handbook of European Referendums . Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-55803-1_31

Bíró-Nagy, A. (2021). Orbán's political jackpot: migration and the Hungarian electorate. *Journal of Ethnic and Migration Studies*, *48*(2), 405–424. https://doi.org/10.1080/1369183X.2020.1853905

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.

Coman, R., Paulis, E., Puleo, L., & Trino, N. (2025). Building and legitimizing an illiberal transnational field: Illiberal think tanks' struggle for cultural hegemony in Poland and Hungary. *European Political Science*. Advance online publication. https://doi.org/10.1057/s41304-025-00544-6

Court of Justice of the European Union. (2020, December 17). *Commission v Hungary (Asylum)*, Case C-808/18 (Judgment). https://curia.europa.eu/juris/liste.jsf?num=C-808/18

Court of Justice of the European Union. (2021, November 16). *Commission v Hungary (Criminalisation of assistance to asylum seekers)*, Case C-821/19 (Judgment; Press release No 205/21). https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210205en.pdf

Czyż, A. (2024). The Visegrad Group countries towards the war in Ukraine in 2022. *Studia Politologiczne*, 73, 254–271. https://doi.org/10.33896/SPolit.2024.73.15

European Commission. (2020). *Communication on a New Pact on Migration and Asylum* (COM(2020) 609 final). Brussels. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:609:FIN

European Digital Rights, Access Now, & Hungarian Civil Liberties Union. (2025, May 6). Hungary's new biometric surveillance laws violate the AI Act. EDRi. https://edri.org/our-work/hungarys-new-biometric-surveillance-laws-violate-the-ai-act/

European Parliament. (2022). *Report on the situation in Hungary pursuant to Article 7(1) TEU (A9-0217/2022)*. Brussels: European Parliament. https://www.europarl.europa.eu/doceo/document/A-9-2022-0217_EN.html

Foucault, M. (2007). Security, Territory, Population: Lectures at the Collège De France, 1977-1978. Basingstoke: Palgrave Macmillan

Genschel, P., & Jachtenfuchs, M. (Eds.). (2014). *Beyond the regulatory polity? The European integration of core state powers*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199662821.001.0001

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

Gerring, J. (2007). *Case study research: Principles and practices*. Cambridge University Press.

Gkliati, M. (2022). The next phase of the European Border and Coast Guard: Responsibility for returns and push-backs in Hungary and Greece. *European Papers*, 7(1), 171–193. https://doi.org/10.15166/2499-8249/553

Glied, V. & Zamęcki, Ł. (2021). Together, but Still Separated? Migration Policy in the V4 countries. *Politics in Central Europe*, *17*(s1), 2021. 647-673. https://doi.org/10.2478/pce-2021-0027

Human Rights Watch. (2025). Hungary. In *World report 2025*. https://www.hrw.org/world-report/2025/country-chapters/hungary

Hungarian Government. (2017, April 3). *The national consultation packages are already being delivered, including a letter from the Prime Minister*. Cabinet Office of the Prime Minister. https://akadalymentes.2015-2019.kormany.hu/en/cabinet-office-of-the-prime-minister/news/the-national-consultation-packages-are-already-being-delivered-including-a-letter-from-the-prime-minister

Hungarian Government. (2018). *Proposal on the "Stop Soros" legislative package*. https://helsinki.hu/wp-content/uploads/STOP-SOROS-LEGISLATIVE-PACKAGE-PROPOSAL.pdf

Hungarian Helsinki Committee. (2023). *Country report: Hungary—2023 update*. European Council on Refugees and Exiles (AIDA). https://asylumineurope.org/wp-content/uploads/2024/07/AIDA-HU_2023-Update.pdf

Huysmans, J. (2006). *The politics of insecurity: Fear, migration and asylum in the EU*. Routledge.

Jaroszewicz, M., & Gniazdowski, M. (2015, September 9). *The Hungarian stage of the migration crisis*. Centre for Eastern Studies (OSW). https://www.osw.waw.pl/en/publikacje/analyses/2015-09-09/hungarian-stage-migration-crisis

Khoury, C., & Hendow, M. (2025, February). *Advances in border management: Digitalisation trends and emerging technologies* (Working paper). International Centre for Migration Policy Development. https://research.icmpd.org/wp-content/uploads/2025/02/Advances-in-Border-Management-Digitilisation-trends-and-emerging-technologies.pdf

Kim, S. (2023). "Illiberal democracy" after post-democracy: Revisiting the case of Hungary. *The Political Quarterly, 94*(3), 437–444. https://doi.org/10.1111/1467-923X.13255

Lamour, C. (2023). Orbán Placed in Europe: Ukraine, Russia and the Radical-Right Populist Heartland. *Geopolitics*, *29*(4), 1297–1323. https://doi.org/10.1080/14650045.2023.2241825

Lottholz, P. (2022). Theorizing post-liberal forms of statebuilding and order-making globally. In *Post-liberal statebuilding in Central Asia* (pp. 27–50). Bristol University Press. https://doi.org/10.51952/9781529220025.ch002

McDonald, M. (2008). Securitization and the Construction of Security. European Journal of International Relations, 14(4), 563-587. https://doi.org/10.1177/1354066108097553

Orbán, V. (2014, July 26). *Prime Minister Viktor Orbán's speech at the 25th Băile Tuşnad (Tusnádfürdő) Summer University and Student Camp*. kormany.hu. https://2015-2019.kormany.hu/en/the-prime-minister/the-prime-minister-s-speeches/prime-minister-viktor-orban-s-speech-at-the-25th-balvanyos-summer-free-university-and-student-camp

Orbán, V. (2025, February 22). *State of the Nation Address*. https://miniszterelnok.hu/en/prime-minister-viktor-orbans-state-of-the-nation-address-2025-02-22/

Prime Minister's Office. (2022, December 19). *Common sense prevailed; we protected Hungary's sovereignty and Hungarian people's money*. miniszterelnok.hu. https://2015-2022.miniszterelnok.hu/common-sense-prevailed-we-protected-hungarys-sovereignty-and-hungarian-peoples-money/

Schammann, H., Gluns, D., Heimann, C., Müller, S., Wittchen, T., Younso, C., & Ziegler, F. (2021). Defining and transforming local migration policies: a conceptual approach backed by evidence from Germany. *Journal of Ethnic and Migration Studies*, *47*(13), 2897–2915. https://doi.org/10.1080/1369183X.2021.1902792

Schimmelfennig, F. (2018). European integration (theory) in times of crisis: A comparison of the Euro and Schengen crises. *Journal of European Public Policy, 25*(7), 969–989. https://doi.org/10.1080/13501763.2017.1421252

Scott, J. W. (2023). Hungary's illiberal border politics and the exploitation of social, spatial and temporal distinctions. *European Urban and Regional Studies*, *31*(1), 14-28. https://doi.org/10.1177/09697764231186741

Sukosd, M. (2022). Victorious Victimization: Orbán the Orator: Deep Securitization and State Populism in Hungary's Propaganda State. In C. Kock, & L. S. Villadsen (Eds.), *Populist Rhetorics* (pp. 165-185). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-87351-6_7

Tanács-Mandák, F. (2025). The Hungarian governments in the decade of crises (2015–2024). *Frontiers in Political Science, 7,* 1541887. https://doi.org/10.3389/fpos.2025.1541887

Vidra Z., Messing V. (2025). The Representation of the Arrival of Ukrainian Refugees in the Hungarian Media in 2022. Central and Eastern European Migration Review 14(24): 1-20. https://doi.org/10.54667/ceemr.2025.08

Visegrád Group. (2021, July 9). *Joint Statement of the Prime Ministers of the Visegrad Group* https://www.visegradgroup.eu/home/documents/2021/joint-statement-of-the-210713

Waterbury, M. A. (2020). Populist Nationalism and the Challenges of Divided Nationhood: The Politics of Migration, Mobility, and Demography in Post-2010 Hungary. East European Politics and Societies, 34(4), 962-983. https://doi.org/10.1177/0888325419897772

Weninger, O. (2025, January 14). Manufacturing the migrant threat: Race, politics, and human rights. *Human Rights Research*. https://www.humanrightsresearch.org/post/manufacturing-the-migrant-threat-race-politics-and-human-rights

Britchenko, I. (2025). The role of private military companies in contemporary conflicts: Legal and security dilemmas.
Politics & Security, 13(3), 58–69. Doi: 10.54658/ps.28153324.2025.13.3.pp.58-69

THE ROLE OF PRIVATE MILITARY COMPANIES IN CONTEMPORARY CONFLICTS: LEGAL AND SECURITY DILEMMAS

Igor Britchenko
University of the National Education Commission
Krakow, Poland
ibritchenko@gmail.com
https://orcid.org/0000-0002-9196-8740

Abstract. *This article undertakes an examination of the escalating role assumed by Private Military Companies (PMCs) within the matrix of contemporary conflicts, positing that their proliferation—most notably the ascendancy of state-proxy models exemplified by the Wagner Group—constitutes an exploitation of a critical vacuum within the corpus of international law. Effectuated through a comparative analysis of PMC operations across Iraq, Ukraine, Syria, and Africa, this paper demonstrates the mechanisms by which such entities precipitate an erosion of state sovereignty, present a formidable challenge to the tenets of international humanitarian law (IHL), and engender systemic lacunae in accountability. Our findings indicate that extant regulatory frameworks, inclusive of the Montreux Document and the International Code of Conduct (ICoCA), are possessed of an inherent insufficiency for addressing the geopolitical instrumentality characteristic of modern PMCs. The article culminates in the proposal of a binding UN Convention on Private Military and Security Activities, wherein a four-pillar governance model is outlined with the objective of re-establishing state responsibility, guaranteeing accountability, and regulating the ongoing privatization of warfare.*

Keywords: Private Military Companies, State Sovereignty, International Humanitarian Law, Accountability, Wagner Group, Privatization of War, Global Governance.

1. INTRODUCTION

1.1 The Privatization of Warfare: A Defining Feature of 21st-Century Conflict

The landscape of modern armed conflict is presently undergoing a transformation of profound significance, the character of which is defined by an increasing delegation of coercive force to corporate actors (Bijos & de Souza, 2020). This phenomenon, to which the term privatization of warfare is often applied, has borne witness to the evolution of Private Military Companies (PMCs) from their erstwhile status as peripheral support contractors into that of central players in the formulation of defense policy and the execution of military operations globally (Has, 2025).

The private military services market, with a valuation exceeding $241 billion in 2025 and a projection to surpass $371 billion by 2035, maintains operations in more than 50 countries, thereby blurring the traditionally distinct lines between state and non-state violence (Business Research Insights, 2024; Bijos & de Souza, 2020). Such a shift presents a direct challenge to the Westphalian principle concerning the state's monopoly on the legitimate use of force, a normative standard that has for centuries structured the conduct of international relations (Marshall Center, 2024; Leander, 2005).

A complex ecosystem constitutes the contemporary PMC industry, offering a spectrum of services that extends from logistical support and security training to direct combat operations and the deployment of sophisticated cyber warfare capabilities (Bijos & de Souza, 2020; Kumar, 2023). The surge in their utilization, particularly in the period following the conclusion of the Cold War and accelerating with dramatic effect during the conflicts in Iraq and Afghanistan, was propelled by a confluence of factors: the downsizing of national armies, the strategic pursuit of cost-effective military solutions, and a desire for interventions possessed of political deniability (Swed & Burland, 2020; Has, 2025). From this has emerged

ISSN 2815-3324 Online, ISSN 2535-0358 Print

a reality wherein states, including major global powers, have cultivated a critical dependency on these private actors, rendering them incapable of waging war in their absence (Singer, 2007).

1.2 The Governance Gap and the Rise of the State-Proxy Model

Within a significant governance gap has the proliferation of PMCs occurred. International law, having been designed in an era dominated by state-centric conflict, has demonstrated a failure to adapt, thereby leaving a regulatory vacuum that is not merely a passive oversight but rather a strategically maintained space of legal ambiguity (Has, 2025; Civilians in Conflict, 2023). Anti-mercenary conventions are with facility circumvented by the corporate structuring of PMCs, while soft-law initiatives, such as the Montreux Document, persist in their non-binding status and are largely ineffectual in compelling accountability (Mquirmi, 2022; Has, 2025).

This very legal ambiguity has been the enabling condition for the evolution of a new and more perilous form of privatized violence: the state-proxy model. In contrast to their market-driven predecessors, whose operations were primarily motivated by profit, entities such as Russia's Wagner Group (now rebranded as the Africa Corps) function as direct, albeit deniable, instruments of state foreign policy (van der Lugt, 2025; International Review, 2025). These "proxy military companies" are not engaged in competition within a commercial market; their purpose is the conduction of combat operations, hybrid warfare, and resource exploitation on behalf of their state sponsors, frequently with an impunity that is near-total (van der Lugt, 2025).

A qualitative shift in the nature of the industry is what this represents. The central challenge is thus no longer the simple regulation of a commercial market but rather the addressing of state conduct that outsources violence as a means to evade responsibility under international law. A lowering of the threshold for conflict is effectuated by this model, permitting states to engage in proxy wars while they avoid direct accountability, a dynamic that is reminiscent of the Cold War but is imbued with the additional complexity of corporate structures (van der Lugt, 2025; Harper, 2025).

1.3 Thesis Statement and Research Roadmap

It is the argument of this article that the proliferation of PMCs, and state-proxies in particular, is not an accidental byproduct of globalization but rather a strategic exploitation of a deliberate vacuum in international law, a condition which fundamentally alters conflict dynamics, erodes the Westphalian state system, and necessitates the establishment of a robust, binding international regulatory regime. This article proceeds in four principal parts, adhering to the IMRaD structure. The Methods section delineates the qualitative, comparative case study approach employed for the analysis of PMC operations. The Findings section provides a detailed account of the international regulatory void and presents a comparative analysis of PMC activities in Iraq, Ukraine, Syria, and Africa, synthesizing these findings to demonstrate the erosion of international norms. The Discussion undertakes a critical examination of how PMCs reshape modern warfare, power dynamics, and legal paradigms, arguing for a reclassification of certain groups as "Proxy Military Companies."

Finally, the Conclusion and Recommendations section summarizes the argument and puts forth a comprehensive, four-pillar model for a binding UN Convention on Private Military and Security Activities, advocating for an urgent reassertion of state responsibility and international oversight over the market for force.

2. METHODS

2.1 Research Design

For the purpose of conducting a comprehensive and critical analysis of the role of PMCs in contemporary conflicts, this study makes use of a qualitative, multi-method research design. At the core of the methodology lies a structured, comparative case study analysis, an approach which permits an in-depth

examination of the phenomenon across disparate geopolitical contexts and operational models (Has, 2025). Supplementing this approach is a systematic literature review of recent (2020-2025) scholarly contributions in the fields of international law, security studies, and international relations. The combination of these methods facilitates both a broad comprehension of the overarching legal and theoretical dilemmas and a granular analysis of specific instances of PMC deployment.

2.2 Data Collection and Analysis

The analysis of secondary data sources forms the basis of this research. Data were systematically collected from an extensive range of materials, which included peer-reviewed academic articles, legal documents, governmental reports (e.g., U.S. Congressional Research Service), and publications originating from international organizations and think tanks, among them the United Nations (UN), the International Committee of the Red Cross (ICRC), the Stockholm International Peace Research Institute (SIPRI), and the Geneva Academy of International Humanitarian Law and Human Rights (Bijos & de Souza, 2020; Has, 2025). To code and synthesize the collected data, a thematic analysis was employed, through which recurrent themes related to legal ambiguity, accountability mechanisms (or their absence), state sovereignty, impacts on human rights, and the evolving geopolitical roles of PMCs were identified. This process enabled the systematic identification of patterns and divergences across the different cases and regulatory environments.

2.3 Case Selection Rationale

The four case studies—Iraq, Ukraine, Syria, and Africa (with a specific focus on Mali, the Central African Republic, and Sudan)—were selected with purposive intent to represent distinct archetypes of PMC deployment and to illuminate the multifaceted nature of the legal and security challenges they engender. A nuanced analysis that moves beyond a monolithic conception of the PMC industry is enabled by this comparative framework. The rationale for each selected case is articulated as follows:

- Iraq: This case represents the archetype of large-scale, Western-led contracting within a post-invasion, nation-building context. The extensive utilization of PMCs such as Blackwater by the U.S. government serves as a seminal case study on the challenges of oversight, the blurring of civilian-military distinctions, and the profound failures of accountability that are liable to occur within a permissive legal environment (Chapman University Digital Commons, 2024; Welch, 2008).
- Ukraine: Herein is illustrated the escalatory potential inherent in the state-proxy model. The role of the Wagner Group evolved from that of a covert instrument for destabilization in the Donbas region (2014-2022) to that of a semi-conventional assault force in the full-scale invasion, an evolution that culminated in a direct challenge to its sponsor state. Uniquely, this case demonstrates the complete life cycle and the intrinsic instability of a state-proxy PMC (ACLED, 2023; Velychenko, 2023).
- Syria: A complex theater is provided by this case, wherein PMCs operate as force multipliers within a protracted, multi-sided civil war. Russian PMCs have acted in concert with regular military forces, supported a client regime, and secured economic assets, thereby showcasing the hybrid commercial and geopolitical functions that these entities are capable of performing in highly contested environments (Kalamar, 2021; Has, 2025).
- Africa (Mali, CAR, Sudan): This region serves as the primary archetype for PMCs functioning as instruments of neocolonial influence and resource extraction. The "regime survival package" model employed by the Wagner Group—which involves trading security services for mining concessions and political alignment—highlights the manner in which PMCs are utilized by external powers to project influence in fragile states, often resulting in the displacement of traditional Western partners and the perpetuation of instability (Congressional Research Service, 2025; ACLED, 2024).

ISSN 2815-3324 Online, ISSN 2535-0358 Print

3. FINDINGS: THE LANDSCAPE OF PRIVATIZED VIOLENCE

3.1 The International Regulatory Void: A Feature, Not a Bug

The operational milieu of the contemporary PMC industry is one defined by a profound international regulatory vacuum. This absence of a binding legal framework is not to be understood as a passive failure of international law to maintain pace with new realities; it appears, rather, to be a strategically maintained condition that serves the interests of powerful states which utilize PMCs as instruments of foreign policy (Has, 2025). A systematic inadequacy to address the corporate nature and state-sponsorship of modern PMCs is characteristic of existing international legal instruments.

The primary international treaties that address private military actors, such as the *International Convention against the Recruitment, Use, Financing and Training of Mercenaries* (1989), were conceived to criminalize the "soldier of fortune" archetype (Gómez del Prado, 2021). Ill-suited are these conventions to the regulation of PMCs, which operate as legally registered corporations, often possessing complex international structures that permit them to easily circumvent the narrow and subjective definition of a "mercenary" as found in instruments like Article 47 of Additional Protocol I to the Geneva Conventions (Mquirmi, 2022; Has, 2025). The limited number of state ratifications for these conventions serves to further underscore their ineffectiveness (Has, 2025).

In response to high-profile incidents, among them the Nisour Square massacre, the international community has developed soft-law initiatives. A significant step was the *Montreux Document* (2008), which clarified the existing obligations of states under IHL and human rights law in the context of contracting PMCs (Federal Department of Foreign Affairs, Switzerland, 2021). It delineates good practices for home states (wherein PMCs are based), territorial states (wherein they operate), and contracting states (which employ them) (Montreux Document Forum, n.d.). Subsequent to this, the *International Code of Conduct for Private Security Service Providers* (ICoCA) was established in 2010, a multi-stakeholder initiative intended to create industry standards and an oversight mechanism (ICoCA, n.d.-a).

The fundamental limitation of both the Montreux Document and ICoCA, however, is their non-binding nature (Global Policy Forum, 2021). Their efficacy relies upon voluntary adherence, and they are devoid of robust enforcement or punitive mechanisms. While their contribution to the professionalization of certain segments of the industry is acknowledged, they are fundamentally incapable of compelling accountability from states that instrumentalize PMCs for geopolitical ends (van der Lugt, 2025). For a state such as Russia, which has not endorsed these initiatives and operates PMCs within a deliberately extra-legal space, these frameworks are of no relevance (Has, 2025). Even for signatory states like the United States, the prevention of impunity has not been achieved by these frameworks, as evidenced by the eventual pardoning of the convicted Blackwater contractors (Academi, n.d.). A 2021 amendment to the ICoC further legitimized the industry through the broadening of its scope to include "military support," an act which effectively endorsed the outsourcing of functions that approach direct participation in hostilities (Has, 2025). This dynamic suggests that the regulatory vacuum is a constructed space, one that is actively shaped and preserved by powerful states for the purpose of maintaining plausible deniability and strategic flexibility in their application of force.

3.2 Comparative Analysis of PMC Operations and Impacts

Significant variation is observed in the operational realities of PMCs across different conflict zones, a variation that reflects the diverse strategic objectives of their clientele. A comparative analysis of key theaters reveals distinct models of PMC deployment, each possessing unique implications for international security and law.

3.2.1 Iraq: The Western Corporate Model and the Legacy of Impunity

The zenith of the Western corporate PMC model was marked by the U.S.-led invasion of Iraq in 2003. Tens of thousands of private contractors were deployed for the purpose of augmenting U.S. forces, providing a range of services from logistical support to armed protection for diplomats and infrastructure

(U.S. Department of Defense, 2022; Singer, 2007). Companies such as Blackwater (later Xe, then Academi, now a part of Constellis), DynCorp, and Triple Canopy became indispensable components of the war effort, operating under lucrative contracts with the U.S. Department of State and Department of Defense (Constellis, n.d.; Blackwater, n.d.).

A "gray zone" of accountability was created by this extensive outsourcing. Contractors operated under a grant of immunity from Iraqi law (Coalition Provisional Authority Order 17) and fell into jurisdictional gaps within the framework of U.S. law (EBSCO, 2021). This environment of impunity reached its culmination in the Nisour Square massacre in Baghdad on September 16, 2007. Blackwater contractors, while guarding a U.S. diplomatic convoy, opened fire in a crowded intersection, an act which resulted in the deaths of 17 Iraqi civilians and injuries to 20 more (ICoCA, n.d.-b; Constellis, n.d.). The conclusion of both Iraqi and U.S. investigators was that the shooting was unprovoked, an event that sparked international outrage and precipitated a crisis in U.S.-Iraqi relations (EBSCO, 2021).

A protracted saga that exposed the deep-seated flaws in accountability mechanisms was the legal aftermath. Following the dismissal of initial charges on procedural grounds, four Blackwater guards were eventually convicted in a U.S. federal court in 2014—one for murder and three for manslaughter (EBSCO, 2021; ICoCA, n.d.-b). However, in a move that cemented a legacy of impunity, presidential pardons were granted to all four in December 2020 (Constellis, n.d.). The Iraq case stands as the archetypal example of how, even within a system possessing nominal legal oversight (the U.S. model of "explicit regulation"), political will can override judicial processes, leaving victims without justice and establishing a dangerous global precedent (Has, 2025).

3.2.2 Ukraine: The State-Proxy Escalation Model

The conflict in Ukraine serves to showcase the evolution and escalatory potential of the state-proxy PMC model, a model centered on the Wagner Group. Wagner's involvement commenced in 2014, at which time its operatives, functioning as deniable Russian forces, assisted in the destabilization of the Donbas region and facilitated the annexation of Crimea (Britannica, 2025; Wagner Group, n.d.). For years, any connection was denied by the Kremlin, which used Wagner to wage a proxy war while avoiding official casualties and international responsibility (Wagner Group, n.d.).

With Russia's full-scale invasion in February 2022, a dramatic transformation of Wagner's role occurred. It shifted from a shadow force to a publicly acknowledged and critical component of Russia's military campaign (ACLED, 2023). Under the leadership of Yevgeny Prigozhin, Wagner swelled its ranks to over 50,000 fighters, a feat accomplished largely through the mass recruitment of convicts from Russian prisons (Britannica, 2025). It became the primary assault force in the brutal, attritional battle for Bakhmut, securing a pyrrhic victory for Russia in May 2023 at an immense human cost (Britannica, 2025; Wagner Group activities in Ukraine, n.d.).

This period demonstrated the instability inherent in such a model. The growing public profile of Prigozhin and his criticism of the Russian military establishment culminated in an armed mutiny in June 2023, during which Wagner forces seized a major military headquarters and initiated a march on Moscow (ACLED, 2023). Though the rebellion proved short-lived, it exposed the profound risks associated with a state's creation of a powerful, parallel army existing outside its formal command structure. Following the deaths of Prigozhin and other senior leaders in a plane crash in August 2023, the Russian state moved to absorb the remnants of Wagner into its formal military and intelligence structures, rebranding its African operations as the "Africa Corps" under direct GRU oversight (Velychenko, 2023; ACLED, 2024). A complete arc is thus provided by the Ukraine case: from covert proxy to semi-conventional army to existential threat, ultimately revealing the state's hand and the fiction of plausible deniability.

3.2.3 Syria and Africa: The Geopolitical Leverage Model

In Syria and across several African nations, Russia has expertly deployed the Wagner Group as a low-cost, high-impact instrument of geopolitical influence. This model effectuates a combination of military intervention with economic extraction and political manipulation, thereby displacing Western influence in fragile states.

In Syria, Wagner mercenaries were deployed in 2015 in concert with the formal Russian military intervention to provide support to the Assad regime (Britannica, 2025). Their role was twofold: to serve as a deniable ground force in offensive operations against rebel groups and to secure valuable economic assets. In exchange for their services, companies with links to Prigozhin received lucrative contracts for oil and gas fields, a mechanism which directly funded Wagner's operations while also enriching the Kremlin's inner circle (Brookings Institution, 2023). The Battle of Khasham in February 2018, where a Wagner-led force attacked a position held by U.S. and Kurdish troops and was subsequently decimated by U.S. airpower, starkly illustrated their function as an expendable proxy force (Britannica, 2025).

Across the African continent, Wagner perfected its "regime survival package" (Has, 2023). In countries such as the Central African Republic (CAR), Mali, and Sudan, Wagner offered military training, counter-insurgency support, and personal security for embattled leaders and military juntas (Congressional Research Service, 2025). In return, Wagner-affiliated companies gained exclusive access to valuable natural resources, such as gold and diamond mines, which were then smuggled out of the country to assist Russia in circumventing international sanctions (Brookings Institution, 2023; Congressional Research Service, 2025). Deeply intertwined with gross human rights violations is this model. Mass killings, summary executions, torture, and rape by Wagner mercenaries have been documented by UN investigators and human rights organizations, an example being the March 2022 massacre of over 500 civilians in Moura, Mali (Britannica, 2025; SIPRI, 2023). By propping up authoritarian regimes in exchange for resources and UN votes, Russia utilizes its proxy force to construct a sphere of influence, undermine democratic governance, and secure a strategic foothold on the continent (International Review, 2025).

3.3 Synthesis of Comparative Findings

A clear trend is revealed by the distinct operational models of PMCs across these conflict zones: a shift from market-driven contracting toward geopolitically-driven state proxyism, accompanied by a corresponding decline in accountability. The key dimensions of PMC deployment in the selected case studies are synthesized in the following table.

Table 1: Comparative Analysis of PMC Roles and Impacts in Key Conflict Zones

Dimension	Iraq (2003-2011)	Ukraine (2014-2025)	Syria (2015-Present)	Africa (Mali, CAR, Sudan)
Key PMC(s)	Blackwater (Xe/Academi), DynCorp, Triple Canopy	Wagner Group, Redut	Wagner Group, Slavonic Corps	Wagner Group / Africa Corps, Chinese PMCs
Primary Client(s)	U.S. Dept. of State, Dept. of Defense	Russian State (MoD, GRU)	Syrian Government, Russian State	National Governments (Juntas), Russian State
Mission Profile	Diplomatic security, convoy protection, logistics, training	Covert action, frontline assault, political destabilization	Combat support, asset protection (oil/gas), force multiplication	Regime security, counter-insurgency, resource extraction, political influence
Relationship to State	Contractual (Market-Driven)	State-Proxy (Geopolitically-Driven)	Hybrid (State-Proxy & Commercial)	State-Proxy (Geopolitical & Extractive)
Notable Incident(s)	Nisour Square Massacre (2007)	Battle of Bakhmut (2023), Prigozhin Mutiny (2023)	Battle of Khasham (2018)	Moura Massacre, Mali (2022)
Accountability Outcome	U.S. convictions followed by presidential pardons; impunity	State absorption; no accountability for war crimes	No accountability; plausible deniability maintained	Near-total impunity; UN investigations blocked

This comparative framework serves to demonstrate that as the relationship between the PMC and the state undergoes a shift from a contractual, market-based one (Iraq) to a direct proxy relationship (Ukraine, Africa), the possibility of meaningful accountability diminishes to a point of non-existence. In the former instance, accountability failed as a result of political intervention; in the latter, it is precluded by design.

3.4 Erosion of International Norms

The proliferation and evolving nature of PMCs are actively contributing to the erosion of foundational norms within the international system. The most significant challenge is posed to the state's monopoly on the legitimate use of violence (Marshall Center, 2024). Through the outsourcing of core military functions, states are not merely engaging in the hiring of services; they are, in fact, creating parallel power structures possessed of their own loyalties and command chains, a situation which leads to a "feudalization" of warfare (Marshall Center, 2024). This phenomenon fundamentally alters civil-military relations, complicates the mechanisms of democratic oversight, and diffuses responsibility for the decision to employ force (Bijos & de Souza, 2020; Has, 2025).

Also evident is this erosion within the framework of United Nations peacekeeping. A deep paradox confronts the UN: while its charter and official position express condemnation of mercenarism, its peacekeeping operations have become increasingly reliant on private security contractors for a range of functions, from the guarding of facilities to logistics and demining (ResearchGate, 2021). Former Secretary-General Kofi Annan once decried the use of PMCs, yet the practical necessities of the organization in under-resourced and dangerous environments have led to their widespread utilization (Eisenhower, 1961; ResearchGate, 2021). Significant challenges for mission integrity, impartiality, and accountability are created by this reliance. When abuses are committed by UN-contracted personnel, the legitimacy of the entire operation is undermined, and complex questions concerning institutional responsibility are raised, questions which the UN system is ill-equipped to address (ResearchGate, 2021; Chicago Unbound, 2016).

4. DISCUSSION: RESHAPING WAR, POWER, AND LAW

4.1 The Geopolitical Instrumentality of "Proxy Military Companies"

A critical re-evaluation of the terminology used to describe these actors is necessitated by the findings. The term "Private Military Company" carries the implication of a commercial, market-based entity, a description that fails to adequately capture the nature of groups such as the Wagner Group or Turkey's SADAT (van der Lugt, 2025). A compelling argument is made in recent scholarship for their reclassification as "Proxy Military Companies" (PMCs) or "contractual proxies" (van der Lugt, 2025). This is not a distinction of mere semantics; it represents a crucial analytical shift that re-frames the problem from one of corporate regulation to one of state responsibility.

The recognition of these entities as extensions of state power reveals their true geopolitical function. They serve as a tool by which states can circumvent the political and legal constraints on the use of force (Harper, 2025). Through the deployment of a proxy, a state is enabled to intervene in a conflict, pursue strategic objectives, and project power with minimal domestic political costs—entailing no official troop deployments, no flag-draped coffins, and a shield of plausible deniability to deflect international condemnation (Bijos & de Souza, 2020; Civilians in Conflict, 2023). This effectively lowers the entry barrier to conflict, thereby encouraging a return to Cold War-style proxy warfare, in which great powers clash through surrogates in fragile states, a dynamic that prolongs conflicts and increases civilian suffering (van der Lugt, 2025).

ISSN 2815-3324 Online, ISSN 2535-0358 Print

4.2 The Accountability Paradox: The Strategic Value of Impunity

Through the lens of the "accountability paradox," the persistent failure to establish effective international regulation for PMCs can be understood. The very lack of accountability that renders PMCs so dangerous is also the quality that makes them so attractive to their state sponsors. The legal grey zone is not a flaw in the system to be rectified, but a feature to be exploited (Has, 2025). States utilize PMCs precisely because their operations can be conducted outside the strictures of IHL and national military codes of conduct that are binding upon their own armed forces (Harper, 2025).

This condition permits states to outsource not only military tasks but also legal and moral culpability. When a proxy military company perpetrates a massacre of civilians, the sponsor state is able to deny knowledge or control, thereby shifting blame to a "private" entity and avoiding state responsibility (Civilians in Conflict, 2023; van der Lugt, 2025). A powerful disincentive for major state actors to support a binding international treaty that would close these loopholes is created by this strategic value of impunity. The current system of non-binding codes and voluntary principles allows states to project an appearance of commitment to regulation while simultaneously benefiting from the lack of it, a clear illustration of how legal deficiencies at the international level are instrumentalized for the achievement of foreign policy goals (Has, 2025).

4.3 Implications for International Relations Theory

The core tenets of state-centric International Relations (IR) theory are directly challenged by the rise of powerful, state-aligned non-state actors (CBS, 2021). Realist and Neorealist theories, which posit states as the primary unitary actors within an anarchic system, encounter difficulty in accounting for entities that are simultaneously corporate and state-controlled, functioning as both market participants and instruments of national power. A more complex and fragmented international system is suggested by the PMC phenomenon, a system that echoes concepts of "neo-medievalism," wherein sovereignty is not absolute but is instead layered and shared among a variety of actors, including states, corporations, and hybrid entities (GIS Reports Online, 2023; ResearchGate, 2021).

Furthermore, a pernicious feedback loop that accelerates state decay is created by the role of PMCs in fragile states. A weak state, incapable of providing security, proceeds to hire a PMC (often at the behest of an external patron) (DIIS, 2021). This outsourcing of a core state function serves to prevent the development of legitimate, capable national security institutions, such as a professional army and police force. The continued presence of the PMC is predicated upon the persistence of the threat, a condition which provides it with no incentive to build lasting local capacity (DIVA, 2024). The state's dependency on the external provider is thereby deepened, rendering it more vulnerable to the political and economic influence of the PMC's sponsor state. This cycle—wherein fragility leads to outsourcing, which in turn deepens fragility and dependency—constitutes a key mechanism through which PMCs actively reshape global power dynamics, eroding the sovereignty of host nations and strengthening the influence of their patrons.

5.CONCLUSION AND RECOMMENDATIONS: A MODEL FOR GLOBAL GOVERNANCE

5.1 Summary of Findings and Argument

This analysis has served to demonstrate that the proliferation of Private Military Companies represents a systemic challenge to the international legal and security order. The extant regulatory framework, which is composed of antiquated anti-mercenary conventions and non-binding soft-law initiatives, is possessed of a fundamental inadequacy. It has failed to prevent the evolution of PMCs from market-driven contractors into state-proxy military actors who function as deniable instruments of foreign policy. This evolution, starkly illustrated by the comparative analysis of PMC operations in Iraq, Ukraine, Syria, and

Africa, has resulted in the normalization of unaccountable warfare, the erosion of the state monopoly on violence, and the creation of a culture of impunity for gross violations of human rights and international humanitarian law. The current regulatory vacuum is not a matter of accident but rather a strategically maintained condition that accrues to the benefit of powerful states, thereby posing an urgent and growing threat to global peace and security.

5.2 Policy Proposal: A Binding UN Convention on Private Military and Security Activities

The addressing of this challenge necessitates a move beyond voluntary codes and good practices. Building upon the long-standing call from the UN Working Group on the Use of Mercenaries, the international community must undertake the development and adoption of a new, binding international treaty (Gómez del Prado, 2021; United Nations, 2024). A *UN Convention on Private Military and Security Activities* is essential for the purpose of closing legal loopholes, re-establishing clear lines of responsibility, and providing effective remedies for victims. A convention of this nature should be structured around the four following pillars:

- Pillar 1: Differentiated Legal Definitions and Prohibition of Inherently State Functions: The convention must establish clear, legally binding definitions that effectuate a differentiation between legitimate Private Security Companies (PSCs), which provide purely defensive and static security, and Private Military Companies (PMCs), which offer logistical and training support. It must also create a new category for illegal "State-Proxy Military Actors" (SPMAs), to be defined as any private entity funded, directed, or controlled by a state for the purpose of conducting activities that amount to a use of force. An explicit prohibition on the outsourcing of inherently governmental functions must be included in the convention, encompassing offensive combat operations, intelligence gathering for offensive purposes, and the detention of persons (Mquirmi, 2022; Policy Center, 2022).
- Pillar 2: Codifying Absolute State Responsibility: The legal fiction of "plausible deniability" must be eliminated by the convention. It should codify the principle of ultimate and non-delegable state responsibility under international law (IILJ, n.d.). A state must be held directly responsible for any violation of IHL or human rights law committed by a company that is either headquartered or registered in its territory (home state), is contracted by its government (contracting state), or is found to be acting in furtherance of its strategic objectives. The legal focus would thereby be shifted from the actions of the private entity to the responsibility of the sponsoring state.
- Pillar 3: A UN-Mandated Global Registry, Licensing, and Oversight Body: The convention should establish a new body, operating under the authority of the UN Security Council, which would be tasked with the creation and maintenance of a mandatory global registry for all legitimate PSCs and PMCs. For inclusion on this list, companies must meet stringent criteria, including transparent ownership, financial audits, and adherence to a strict code of conduct. This body would issue licenses for operations in specific contexts, contingent upon the rigorous vetting of all personnel for past human rights violations and mandatory, certified training in IHL. The authority to monitor operations and revoke licenses for non-compliance would be vested in this body, effectively separating legitimate actors from rogue and state-proxy entities.
- Pillar 4: An International Adjudicatory Mechanism and Victim Compensation Fund: To overcome the failures of national jurisdiction, the convention should establish a dedicated international judicial mechanism possessing jurisdiction over both corporate entities and individuals for crimes related to private military and security activities. This could assume the form of a special chamber within the International Criminal Court or a new, specialized tribunal (Ryngaert, 2023). Crucially, this must be paired with a mandatory Victim Compensation Fund, to be financed through a levy on all registered PMC contracts and by fines imposed upon non-compliant states and companies. This would ensure that victims have access to effective remedy and reparations, a component almost entirely absent from the current system (Gómez del Prado, 2021; Ryngaert, 2023).

5.3 Concluding Statement

Formidable are the political obstacles to the achievement of such a convention. States that derive benefit from the current ambiguity will, without doubt, resist a binding framework that imposes genuine accountability. The alternative, however, is the continued normalization of unaccountable proxy wars, the erosion of the legal and ethical foundations of the international order, and the complete commodification of human conflict. The principles enshrined in the UN Charter—the prohibition of the aggressive use of force and the protection of human rights—are what is at stake. Collective, decisive action, effectuated through a binding international treaty, is not merely a policy preference; it is an urgent necessity for the purpose of reclaiming the state's responsibility for war and peace in the 21st century.

REFERENCES

ACLED. (2023, August 2). *Moving out of the shadows: Shifts in Wagner Group operations around the world*. ACLED. https://acleddata.com/2023/08/02/moving-out-of-the-shadows-shifts-in-wagner-group-operations-around-the-world/

ACLED. (2024). *Wagner Group and Africa Corps*. ACLED. https://acleddata.com/analysis/africa/wagner-group-and-africa-corps/

Bijos, L., & de Souza, R. (2020). Private military companies and the outsourcing of war: A spark of destabilisation to the global security. *Annales de la Faculté de Droit d'Istanbul, 69*, 87–118.

Brookings Institution. (2023, July 18). *What's ahead for the Wagner Group in Africa and the Middle East?* https://www.brookings.edu/articles/whats-ahead-for-the-wagner-group-in-africa-and-the-middle-east/

Business Research Insights. (2025). *Private military services market: Share, size, growth, trends, and forecast 2024–2035*. https://www.businessresearchinsights.com/market-reports/private-military-services-market-111077

Chapman University Digital Commons. (2024). *Contracted wars, compromised oversight: Private military companies in Iraq, Afghanistan, and the decline of U.S. accountability standards*.

Chicago Unbound. (2016). Contracting for stability: The potential use of private military contractors as a United Nations rapid-reaction force. *Chicago Journal of International Law, 16*(2). https://chicagounbound.uchicago.edu/cjil/vol16/iss2/

Civilians in Conflict. (2023). *Privatizing war: The impact of private military companies on the protection of civilians*. https://civiliansinconflict.org

Constellis. (n.d.). *Contracts*. https://constellis.com/contracts/

Congressional Research Service. (2025, January 2). *Russia's security operations in Africa* (CRS Report No. IF12389). https://crsreports.congress.gov

DIIS. (2021). *8 old and new challenges for UN peacekeeping*. Danish Institute for International Studies. https://www.diis.dk/en/research/8-old-and-new-challenges-un-peacekeeping

DIVA. (2025). *The role of private military companies in modern warfare*. DiVA Portal.

EBSCO. (2021). *Nisoor Square shooting (Baghdad)*. EBSCO Research Starters. https://www.ebsco.com/research-starters/military-history-and-science/nisoor-square-shooting-baghdad

Eisenhower, D. D. (1961, January 17). *Farewell address* ("Military-industrial complex" speech). U.S. National Archives. https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address

Encyclopædia Britannica. (2025). *Wagner Group*. https://www.britannica.com/topic/Wagner-Group

Federal Department of Foreign Affairs (Switzerland). (2021). *Private military and security companies*. https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies.html

GIS Reports Online. (2024, February 6). *The future of private military companies*. https://www.gisreportsonline.com/r/private-military-companies/

Global Policy Forum. (2021). *Regulation and oversight of PMSCs*. https://www.globalpolicy.org

Gómez del Prado, J. L. (2013). A United Nations instrument to regulate and monitor private military and security contractors. *Notre Dame Journal of International & Comparative Law, 3*(1).

Harper, E. (2025). *Geopolitical implications of proxy military companies* (Geneva Academy Briefing 25). Geneva Academy.

Has, Ö. (2023). *Wagner Group: An instrument of Russian foreign policy*. SciELO.

Has, Ö. (2025, September 4). *Regulating private military companies: A comparative study of national approaches in the United States, Turkey, and Russia*. *Journal of Conflict and Security Law*.

ICoCA. (n.d.-a). *The Code*. International Code of Conduct Association. https://icoca.ch/the-code/

ICoCA. (n.d.-b). *The Nisour Square massacre*. International Code of Conduct Association. https://icoca.ch/case-studies/the-nisour-square-massacre/

IILJ. (2007). *Private military companies and state responsibility* (Lehnardt, C.). Institute for International Law and Justice. https://www.iilj.org/wp-content/uploads/2016/08/Lehnardt-Private-military-companies-and-state-responsibility-2007-1.pdf

International Review. (2025, August 28). *Analysis of Russia's Wagner Group and its promotion of Russia's geopolitical interests*.

Kalamar, K. (2021). Russia's gambit in the Syria conflict. *Pathways to Peace and Security, 1*, 211–213.

Kumar, A. (2023). *Cybersecurity and non-kinetic operations of PMCs*.

Leander, A. (2005). The market for force and public security: The destabilizing consequences of private military companies. *Journal of Peace Research, 42*(5), 605–622. https://doi.org/10.1177/0022343305056237

Marshall Center. (2024). *Russian civil-military relations (CMR) and the long, open-ended war*.

Montreux Document Forum. (n.d.). *The Montreux Document on Private Military and Security Companies*. https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/montreux-document.html

Mquirmi, F. (2022, April). *Navigating in a grey zone: Regulating PMSCs* (Policy Brief PB-27/22). Policy Center for the New South.

Policy Center for the New South. (2022). *Regulating PMSCs*.

ResearchGate. (2021). *Private military and security companies in UN peacekeeping operations: Problems and perspectives*.

Ryngaert, C. (2008). Litigating abuses committed by private military companies. *European Journal of International Law, 19*(5), 1035–1053. https://www.ejil.org/pdfs/19/5/1699.pdf

Singer, P. W. (2007, September 27). Can't win with 'em, can't go to war without 'em: Private military contractors and counterinsurgency. *Brookings Institution*. https://www.brookings.edu/articles/cant-win-with-em-cant-go-to-war-without-em-private-military-contractors-and-counterinsurgency/

SIPRI. (2023). *Private military and security companies in armed conflict*. In *SIPRI Yearbook 2023: Armaments, disarmament and international security*. https://www.sipri.org/yearbook/2023

Swed, O., & Burland, D. (2020). Outsourcing security: The rise of private military and security companies. *Office of the United Nations High Commissioner for Human Rights*. https://www.ohchr.org/sites/default/files/Documents/Issues/Mercenaries/WG/ImmigrationAndBorder/swed-burland-submission.pdf

U.S. Department of Defense. (2022). *Report on private security contractors in the Middle East and Afghanistan*.

United Nations Human Rights Council. (2024). *Progress report on the fifth session of the open-ended intergovernmental working group to elaborate the content of an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies* (A/HRC/57/53).

van der Lugt, R. (2025, March 12). *The 1%: Doing business with proxy military companies*. Geneva Academy of International Humanitarian Law and Human Rights.

Velychenko, S. (2023). *The rise and fall of the Wagner Group*. Danish Institute for International Studies. https://www.diis.dk/en/research/rise-and-fall-wagner-group

Welch, M. (2008). Fragmented power and state-corporate killings: A critique of Blackwater in Iraq. *Crime, Law and Social Change, 51*(3–4), 351–364. https://doi.org/10.1007/s10611-008-9157-2

Dei, M. (2025). The Indo-Pacific as a strategic arena: Evolving security alliances and deepening power rivalries. *Politics & Security, 13*(3), 70–81. Doi: 10.54658/ps.28153324.2025.13.3.pp.70-81

THE INDO-PACIFIC AS A STRATEGIC ARENA: EVOLVING SECURITY ALLIANCES AND DEEPENING POWER RIVALRIES

Maryna Dei
Department of Constitutional and Administrative Law
National Aviation University
Kyiv, Ukraine
maryna.dei@npp.nau.edu.ua
https://orcid.org/0000-0002-0626-8089

Abstract. *This paper examines the transformation of the Indo-Pacific into the central arena for global strategic competition. It argues that the intensifying rivalry between the United States and the People's Republic of China is the primary driver reshaping the regional security architecture. This rivalry has catalyzed the formation and strengthening of countervailing coalitions, notably the Quadrilateral Security Dialogue (QUAD) and the AUKUS pact, while simultaneously challenging the centrality of established ASEAN-led institutions. Through a qualitative analysis of strategic documents, academic literature, and policy reports from 2020-2025, this study dissects the interplay of military modernization, nuclear deterrence, and the weaponization of the economic-security nexus, particularly in critical technology supply chains. The findings indicate a shift towards a more fragmented and contested regional order, characterized by a complex web of overlapping bilateral and minilateral arrangements designed to balance against China's rise. While these alignments enhance deterrence, they also heighten the risks of miscalculation and escalation. The paper concludes with policy recommendations for strengthening cooperative security mechanisms, managing geoeconomic friction, and establishing robust crisis communication channels to ensure regional stability.*

Keywords: Indo-Pacific, Strategic Competition, Security Alliances, QUAD, AUKUS, US-China Rivalry, Balance of Power, Deterrence, Geoeconomics.

1. INTRODUCTION

The 21st century has witnessed a decisive shift in the world's geostrategic and geoeconomic center of gravity from the Euro-Atlantic to the Indo-Pacific (Abensour, 2025; Laksmana, 2024; Medeiros, 2025). Encompassing a vast maritime expanse from the eastern coast of Africa to the western shores of the Americas, the region is home to more than half the world's population, accounts for 60% of the global economy, and hosts seven of the world's largest militaries (Kritenbrink, 2023; European Parliament, 2023). Its strategic maritime routes, including the Strait of Malacca, are conduits for a significant portion of global trade and energy supplies, making regional stability a matter of paramount global concern (Medeiros, 2025).

The primary dynamic shaping this strategic arena is the intensifying competition between the United States, the region's long-standing security guarantor, and the People's Republic of China (PRC), a rising power with revisionist intentions (Cha, 2025; IISS, 2023; Izumikawa, 2020). This rivalry is a multi-dimensional contest for influence that spans the military, economic, technological, and ideological domains, prompting observers to suggest a potential "reset of the world order" (Medeiros, 2025, p. 2). China's military modernization, assertive actions in the South and East China Seas, and expansive Belt and Road Initiative (BRI) have been met with a concerted effort by the United States and its allies to uphold a "free and open" regional order.

This paper argues that the Indo-Pacific's security architecture is being fundamentally reshaped by the intensifying strategic competition between the United States and China, leading to the formation of new minilateral security groupings and the recalibration of existing alliances. This dynamic, while aimed at establishing a stable balance of power, simultaneously heightens the risk of conflict through a complex interplay of military modernization, economic interdependence, and technological rivalry.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

To explore this thesis, this article proceeds in four parts, following the IMRaD (Introduction, Methods, Results, and Discussion) structure. The following section details the qualitative methodology and theoretical framework employed. The third section presents the results of the analysis, mapping the evolving strategic landscape, the key actors' postures, the networked architecture of alliances, the instruments of deterrence, and the geoeconomic battlefield. The fourth section discusses the implications of these findings, analyzing the contested balance of power, the weaponization of interdependence, and the efficacy of regional institutions. The final section offers a conclusion and policy recommendations aimed at mitigating conflict and fostering a stable, rules-based order in this critical region.

2. METHODS

This study utilizes a qualitative, multi-method research design to provide a comprehensive analysis of the Indo-Pacific's security dynamics. The research is based on a systematic literature review of scholarly articles, peer-reviewed journals, official government strategy documents and white papers, and in-depth reports from leading international think tanks, with a publication date range of 2020 to 2025 to ensure contemporary relevance.

The analytical approach is guided by a hybrid theoretical framework that integrates neorealism and liberal institutionalism. Neorealism provides the conceptual tools to explain the structural pressures of the international system that drive the balance of power politics, the formation of countervailing alliances, and the persistent security dilemmas between the United States and China (Hanggarini & Perwita, 2024; Rehman & Asrar, 2024). Concurrently, liberal institutionalism is employed to assess the role, effectiveness, and limitations of multilateral cooperative frameworks, such as those led by the Association of Southeast Asian Nations (ASEAN), in mitigating conflict, fostering shared norms, and promoting a rules-based international order (Sukma, 2010; Dominguez, 2021).

A comparative case study methodology is applied to examine the strategic postures and policies of five key regional actors: the United States, China, India, Japan, and Australia. These five nations were selected as they represent the principal architects and subjects of the Indo-Pacific's evolving security dynamics. The United States and China are the primary competitors whose rivalry defines the region's structural tensions (Cha, 2025). Japan and Australia are cornerstone U.S. allies and key drivers of the Indo-Pacific concept, actively shaping countervailing coalitions (German Institute for International and Security Affairs, 2022). India is the region's pivotal rising power, whose policy of "strategic autonomy" makes it a critical swing state in the balance of power (Koga, 2024; Rajagopalan, as cited in Raska, 2023). This involves a close reading and analysis of their primary strategic documents, including the *U.S. Indo-Pacific Strategy* (The White House, 2022), Australia's *National Defence Strategy* (Australian Government Department of Defence, 2024), Japan's "Free and Open Indo-Pacific" (FOIP) plans (Ministry of Foreign Affairs of Japan, 2023), and China's white papers on security cooperation (State Council Information Office, 2025). This comparative analysis allows for the identification of critical convergences and divergences in threat perceptions, strategic objectives, and policy responses to the changing regional environment.

Furthermore, a discourse analysis of joint statements, official communications, and expert critiques is used to evaluate the mandates, capabilities, and strategic functions of key regional security groupings. This includes an examination of the Quadrilateral Security Dialogue (QUAD), the AUKUS trilateral security pact, and ASEAN-led forums. The QUAD and AUKUS were chosen as the most prominent examples of the shift towards flexible, often exclusive 'minilateral' security arrangements designed to respond to specific strategic challenges, contrasting with the broad, inclusive nature of the established ASEAN-led forums (Nagy, 2023; Laksmana, 2021). The analysis of these groupings provides insight into the fragmentation and layering of the regional security architecture. This method helps to deconstruct the stated versus perceived purposes of these institutions, revealing the underlying strategic logics and tensions that shape their development and impact on the regional order (Anggarini & Khoirunnisa, 2024; Horowitz, 2025; Murray, 2022; Sukma, 2010).

3. RESULTS: THE SHIFTING CONTOURS OF POWER AND SECURITY

3.1 The Strategic Landscape: From "Asia-Pacific" to "Indo-Pacific"

The contemporary strategic discourse is increasingly dominated by the term "Indo-Pacific," a conceptual shift from the previously prevalent "Asia-Pacific." This is not merely a semantic change but reflects a fundamental rescaling of the region's strategic identity from a primarily economic construct to one driven by security imperatives (Sundararaman, 2022; Medeiros, 2025). The Indo-Pacific concept recognizes the fusion of the Indian and Pacific Oceans into a single, continuous strategic theater, underscored by the centrality of vital sea lines of communication (SLOCs) and maritime chokepoints like the Strait of Malacca (Medeiros, 2025; European Parliament, 2023).

This reconceptualization was propelled by the rise of India as a major regional power and the growing interconnectedness of security challenges across the two oceans (Panda, 2022; Lukash, 2024). The concept's intellectual origins can be traced to early 20th-century German geopoliticians and Indian historians, but its modern political currency was established by former Japanese Prime Minister Shinzo Abe's 2007 "Confluence of the Two Seas" speech to the Indian Parliament (Raska, 2023; Abensour, 2025; Pandalai, as cited in FRS, 2025; Sundararaman, 2022).

However, the geographical boundaries of the Indo-Pacific remain contested, with definitions varying among key actors in ways that reflect their distinct strategic priorities. The United States, particularly under the Trump and Biden administrations, defines the region as stretching "from the west coast of India to the western shores of the United States," a definition that conveniently aligns with the area of responsibility of the U.S. Indo-Pacific Command (USINDOPACOM) (Haruko, 2020; Raska, 2023). In contrast, India promotes a more expansive and inclusive vision, extending "from the shores of Africa to that of the Americas," a formulation designed to assuage concerns that the concept is an exclusive, anti-China coalition (Haruko, 2020). ASEAN, seeking to maintain its central role, defines the Indo-Pacific in its *Outlook on the Indo-Pacific* (AOIP) as a closely integrated and interconnected region of which it is the fulcrum, emphasizing dialogue and cooperation over rivalry (Haruko, 2020; ASEAN, 2024). These divergent definitions carry significant policy implications, shaping the scope and nature of potential collaborations and creating zones of strategic overlap and divergence (Haruko, 2020).

This fluid strategic map is populated by major powers with distinct and often competing postures:

- **United States:** The cornerstone of U.S. policy is the "Free and Open Indo-Pacific" (FOIP) strategy, which aims not to change China but to "shape the strategic environment in which it operates" (The White House, 2022, p. 8). This is pursued by modernizing its bedrock bilateral alliances, fostering flexible minilateral partnerships like the QUAD and AUKUS, and promoting a rules-based order to build a balance of influence favorable to U.S. interests and values (The White House, 2022).
- **China:** Beijing officially rejects the Indo-Pacific construct, viewing it as a U.S.-led containment strategy designed to encircle China (He, 2020). It advances an alternative regional vision through its Belt and Road Initiative (BRI), which it frames as a "21st Century Maritime Silk Road" (Luo, 2023), and promotes concepts like a "Community with a Shared Future for Mankind" (State Council Information Office, 2017). China's 2025 national security white paper articulates a doctrine of "comprehensive security," which prioritizes the political security of the Chinese Communist Party (CCP) and uses economic statecraft, military modernization, and assertive diplomacy to establish regional primacy (Agnihotri, 2025; State Council Information Office, 2025; Swedish Defence Research Agency, 2025).
- **Japan:** As a progenitor of the FOIP concept, Japan's strategy is articulated through three pillars: promoting the rule of law and freedom of navigation, pursuing economic prosperity via "quality infrastructure," and committing to regional peace and stability (Ministry of Foreign Affairs of Japan, 2023; Ministry of Foreign Affairs of Japan, n.d.). As a "secondary power," Japan seeks to leverage ideational and institutional tools to manage great power competition and uphold the existing order (Koga, 2024).
- **India:** India's approach is characterized by "strategic autonomy" and "multi-alignment," enabling it to participate in both the U.S.-led QUAD and the China-Russia-led Shanghai Cooperation

Organization (Abensour, 2025; Koga, 2024; Singh, 2025). New Delhi frames its Indo-Pacific engagement not as a reaction to China but as a natural evolution of its "Look East" and "Act East" policies, rooted in deep historical and civilizational connections to the region (Panda, 2022; Pandalai, as cited in FRS, 2025). It aspires to be a "leading power" that co-shapes the regional architecture (The White House, 2022).

- **Australia:** Canberra has undergone a significant strategic shift from a policy of liberal engagement to a more ambitious neorealist stance (Hanggarini & Perwita, 2024). Its 2024 National Defence Strategy codifies a strategy of "deterrence by denial," which focuses on developing the capability to thwart aggression in its immediate region, particularly its northern maritime approaches (Dowse, 2024). This strategy is operationalized through the acquisition of long-range strike capabilities and a deepening of its alliance with the U.S., most notably through the AUKUS pact (Dowse, 2024; Marles, 2024; Congressional Research Service, 2025).

3.2 A Networked Architecture: Alliances and Alignments

The Indo-Pacific's security architecture is evolving into a complex, networked system that blends long-standing bilateral treaties with new, more flexible minilateral arrangements. This emerging structure is largely a response to China's growing power and assertiveness.

The *Quadrilateral Security Dialogue (QUAD),* comprising the United States, Japan, India, and Australia, has been revitalized and elevated to the leaders' level since 2021 (He & Feng, 2023; German Institute for International and Security Affairs, 2023). The QUAD's official mandate is deliberately framed around non-military cooperation to provide regional public goods. Key initiatives include the Quad Vaccine Partnership to combat the COVID-19 pandemic, the Quad Infrastructure Coordination Group to promote quality infrastructure standards, and working groups on critical and emerging technologies like AI and 5G/6G telecommunications (Anggarini & Khoirunnisa, 2024; F MPA, 2024; He & Feng, 2023). This focus on "soft balancing" is designed to offer Indo-Pacific nations attractive alternatives to economic and technological dependence on China (Anggarini & Khoirunnisa, 2024). Despite this public-facing agenda, the QUAD is widely perceived as a strategic coalition of "like-minded" maritime democracies aimed at preserving a rules-based order and balancing against China's influence (German Institute for International and Security Affairs, 2023; He, 2021). This dual identity creates strategic ambiguity. It is this very ambiguity that allows India, with its deep-rooted policy of strategic autonomy, to participate without committing to a formal military alliance. However, this has led some analysts to label India the group's "weakest link," as it resists any move toward collective defense obligations (Grossman, 2018, as cited in He, 2021).

In contrast, *AUKUS* is an unambiguous "hard security" pact between Australia, the United Kingdom, and the United States, announced in 2021 (Horowitz, 2025; Smith, 2024). Its primary purpose is to deepen defense-industrial integration and enhance military capabilities to bolster deterrence.

Pillar I, the pact's centerpiece, involves providing Australia with technology and support to acquire a fleet of conventionally-armed, nuclear-powered submarines (SSNs) (CSIS, 2025; Smith, 2024; U.S. Department of Defense, 2025). This represents a monumental strategic investment for Australia, aimed at projecting power and holding potential adversaries at risk over vast distances.

Pillar II is focused on accelerating the joint development and fielding of advanced capabilities in areas such as artificial intelligence, hypersonic missiles, quantum technologies, and electronic warfare (CSIS, 2025; Congressional Research Service, 2023). While AUKUS is seen by its members as a decisive step to counter China's military buildup, it has generated significant controversy. It has been criticized for potentially undermining nuclear non-proliferation norms, and its secretive formation alienated key allies, most notably France, whose own submarine contract with Australia was abruptly canceled (Murray, 2022; Panel, 2025). Furthermore, its exclusivity has raised concerns in Southeast Asia about the formation of an "Anglosphere" bloc that could sideline regional institutions (Horowitz, 2025).

This rise of minilateralism places the centrality of ASEAN under significant strain. For decades, ASEAN-led institutions like the ASEAN Regional Forum (ARF) and the East Asia Summit (EAS) have served as the region's primary platforms for inclusive security dialogue, operating on the principles of consensus, consultation, and non-interference known as the "ASEAN Way" (Sukma, 2010; Anwar, 2024). However,

the intensifying US-China rivalry has exposed deep fissures within ASEAN, with member states adopting divergent positions based on their economic and security relationships with the two great powers (Putri, 2025; Laksmana, 2020; Sim, 2025). The emergence of groupings like the QUAD and AUKUS, which address regional security challenges outside of ASEAN-led frameworks, is perceived by many as a direct challenge to ASEAN's relevance and convening power (Chong, 2024; Laksmana, 2021). Persistent critiques that ASEAN forums are merely "talk shops," incapable of enforcing decisions or resolving hard security disputes like the South China Sea conflicts or the crisis in Myanmar, have further fueled this perception (German Institute for International and Security Affairs, 2022; Laksmana, 2020; IISS, 2025).

Underpinning this entire networked structure is the enduring U.S. "hub-and-spokes" system of bilateral alliances, which remains the bedrock of the regional security order (Cha, 2025; Rapp-Hooper, 2020, as cited in Park & Savell, 2025; German Institute for International and Security Affairs, 2022). The U.S.-Japan Security Treaty stands as the cornerstone of this system, committing the U.S. to the defense of Japan and granting it access to forward-deployed bases that are indispensable for regional deterrence and power projection (United States Department of State, 1960; Ministry of Defense of Japan, n.d.). Recent alliance developments have focused on upgrading command-and-control frameworks and enhancing military interoperability to more effectively counter shared threats (The White House, 2025). Similarly, the ANZUS treaty forms the legal basis of the U.S.-Australia alliance, a partnership that has been profoundly strengthened and operationally deepened by the AUKUS agreement (EPRS, 2022).

Table 1: Comparative Analysis of Indo-Pacific Security Groupings

Feature	Quadrilateral Security Dialogue (QUAD)	AUKUS	ASEAN-led Forums (ARF, EAS)
Core Membership	United States, Japan, India, Australia (Congressional Research Service, 2023)	Australia, United Kingdom, United States (Horowitz, 2025)	10 ASEAN Member States + Dialogue Partners (including US, China, Japan, India, Australia, Russia, EU, etc.) (Australian Government Department of Foreign Affairs and Trade, n.d.)
Primary Mandate	Strategic dialogue; "soft balancing"; provision of regional public goods (German Institute for International and Security Affairs, 2023; Anggarini & Khoirunnisa, 2024). Explicitly non-military alliance (He, 2021; He & Feng, 2023).	Hard security pact; military-technological cooperation; enhancing deterrence capabilities (Horowitz, 2025; Smith, 2024).	Dialogue and confidence-building; norm-setting; conflict prevention (not resolution) (Sukma, 2010; Anwar, 2024).
Key Initiatives	Vaccine Partnership, Critical & Emerging Technology Working Group, Infrastructure Coordination, Maritime Domain Awareness Partnership (Anggarini & Khoirunnisa, 2024; F MPA, 2024).	**Pillar I:** Nuclear-powered submarines for Australia. **Pillar II:** Joint development of AI, hypersonics, cyber, quantum, and undersea capabilities (CSIS, 2025; Congressional Research Service, 2023).	ASEAN Outlook on the Indo-Pacific (AOIP); Treaty of Amity and Cooperation (TAC); ongoing negotiations for a South China Sea Code of Conduct (Sukma, 2010; IISS, 2025).
Strengths	Flexible, non-binding format; broad agenda appeals to diverse interests; includes key democratic powers (F MPA, 2024).	Deep military-technological integration among trusted allies; provides high-end, credible deterrence capabilities; clear focus and purpose (Horowitz, 2025).	Inclusive membership (includes China); established diplomatic channels; high degree of regional legitimacy and convening power ("ASEAN Centrality") (Sukma, 2010; Anwar, 2024).

Perceived Limitations	Ambiguous strategic purpose (soft vs. hard security); constrained by India's non-alignment policy ("weakest link" critique) (He, 2021); viewed with suspicion by China and some ASEAN states (He & Feng, 2023; Laksmana, 2021).	Exclusive "Anglosphere" grouping; alienates key allies (e.g., France); raises nuclear proliferation concerns; long delivery timelines for capabilities; challenges ASEAN centrality (Murray, 2022; Panel, 2025; Laksmana, 2021).	Consensus-based decision-making leads to slow progress and lowest-common-denominator outcomes; ineffective at addressing hard security crises ("talk shop" critique) (German Institute for International and Security Affairs, 2022; Laksmana, 2020; IISS, 2025).

3.3Instruments of Deterrence: Military Modernization and Signaling

The strategic competition in the Indo-Pacific is being operationalized through extensive military modernization programs and deliberate strategic signaling, creating a complex and increasingly tense deterrence environment.

A naval arms race is accelerating across the region. China's industrial might, with a shipbuilding capacity reportedly 230 times that of the United States, has enabled the People's Liberation Army Navy (PLAN) to become the world's largest naval force by number of vessels (Congressional Research Service, 2025; Peace and International Security Council, 2025; The Economic Times, 2025). The PLAN is rapidly expanding its fleet of aircraft carriers, advanced destroyers, and submarines, with the stated goal of becoming a global blue-water navy capable of operating far from its shores by 2050 (The Economic Times, 2025; U.S.-China Economic and Security Review Commission, 2020; IISS, 2023). This naval buildup is a direct challenge to the long-standing maritime dominance of the U.S. Navy. In response, the United States and its allies are undertaking significant naval expansion and modernization efforts of their own (IISS, 2023). Australia, through AUKUS, is set to acquire a fleet of SSNs and is also procuring long-range anti-ship missiles (Dowse, 2024; Congressional Research Service, 2025). Japan is retrofitting its *Izumo*-class helicopter carriers to operate F-35B stealth fighters, effectively giving it light aircraft carriers for the first time since World War II, and is acquiring Tomahawk land-attack cruise missiles to bolster its counterstrike capabilities (IISS, 2023; Newsweek, 2025). India is actively pursuing its vision of a 200-ship navy by 2035, which includes commissioning its second aircraft carrier, the indigenously built *INS Vikrant*, and planning for a third, potentially nuclear-powered, carrier (The Economic Times, 2025; Suciu, 2025; Indian Ministry of Defence, 2025).

This conventional arms race is shadowed by a nuclear overhang. The Indo-Pacific is a crowded nuclear arena, featuring established nuclear-weapon states (United States, China, Russia, India, North Korea, Pakistan) as well as key U.S. allies—Japan, South Korea, and Australia—sheltered under the U.S. extended deterrence umbrella (IISS, 2023). A major destabilizing factor is China's rapid and opaque expansion of its nuclear arsenal. U.S. defense intelligence projects that China's nuclear warhead stockpile could reach 1,500 by 2035, a dramatic increase that signals a potential shift from its long-held doctrine of "minimum deterrence" toward a posture of nuclear parity with the United States and Russia (The Economic Times, 2025; Perry World House, 2025). While Beijing officially maintains its No-First-Use (NFU) policy, its growing and diversifying triad of delivery systems (land-based ICBMs, submarine-launched ballistic missiles, and strategic bombers) provides it with a more credible and survivable second-strike capability (Zhang, 2021; Boyd & Barrie, 2025; NIDS, 2018; European Parliament, 2023). India, whose nuclear program is primarily oriented toward deterring China and Pakistan, also adheres to an NFU pledge and a doctrine of "credible minimum deterrence" (NIDS, 2018). The United States, in turn, is modernizing its own nuclear triad and developing more flexible, lower-yield options to strengthen the credibility of its extended deterrence commitments to allies, who harbor growing anxieties about the reliability of the U.S. nuclear umbrella in a more complex threat environment (Perry World House, 2025).

In this charged atmosphere, joint military exercises have become a primary instrument for enhancing interoperability and sending potent signals of collective resolve and capability. Exercise Malabar, once a bilateral U.S.-India naval drill, has evolved to permanently include Japan and Australia, effectively

becoming the premier military exercise of the QUAD nations (Project Statecraft, 2020; Australian Institute of International Affairs, 2023; He & Feng, 2023; PIB Delhi, 2021). The exercise has grown in complexity and geographical scope, now encompassing high-end maritime warfare scenarios, including advanced anti-submarine warfare (ASW), air defense, and carrier strike group operations across the Indian and Pacific Oceans (Project Statecraft, 2020; Defence, 2023; Naval Technology, 2024).

Similarly, Exercise Talisman Sabre, the largest bilateral military exercise between the U.S. and Australia, has expanded to include a host of other partner nations (Australian Army, 2024). It serves as a laboratory for testing and validating complex, multi-domain warfighting concepts, involving amphibious landings, long-range precision strikes, and integrated air and missile defense, thereby demonstrating the collective capacity of the allies to respond to a major security crisis (U.S. Army Pacific, 2025; Defence, 2025; MRF-D, 2025).

3.4 The Geoeconomic Battlefield: Trade, Technology, and Infrastructure

The strategic competition in the Indo-Pacific is being waged as intensely in the economic and technological domains as it is in the military sphere. Infrastructure development, critical supply chains, and emerging technologies have become central arenas for a new era of geoeconomic rivalry.

This rivalry is most visible in the competing visions for regional infrastructure development. China's Belt and Road Initiative (BRI) is a colossal geoeconomic project that aims to reshape global connectivity by financing and building infrastructure—ports, railways, pipelines, and digital networks—across Eurasia and Africa (IISS, 2021; Hong Kong Trade Development Council, n.d.; Camba, 2025). While promoted by Beijing as a vehicle for shared prosperity, the BRI has been widely criticized by the U.S. and its partners for its lack of transparency, unsustainable lending practices that create "debt traps" for developing nations, and its underlying strategic goal of expanding China's political and economic leverage (Council on Foreign Relations, 2023). In response, the U.S. and its allies have launched alternative initiatives. The Blue Dot Network (BDN), a joint effort by the U.S., Japan, and Australia, is not a financing mechanism but a certification system designed to promote "quality, high-standard" infrastructure projects that are transparent, sustainable, and financially viable, thereby helping to attract private sector investment (Wilson, 2021; Anam, 2022; U.S. Department of State, n.d.). Building on this concept, the G7 launched the Partnership for Global Infrastructure and Investment (PGII), which aims to mobilize $600 billion in public and private capital by 2027 for "values-driven" infrastructure projects in low- and middle-income countries, offering a direct alternative to China's state-led model (G7 Italy, 2024; The White House, 2022; Ministry of Foreign Affairs of Japan, 2023; Goto & Hughes, 2022).

At the heart of this geoeconomic contest lies the battle for technological supremacy, with the semiconductor supply chain emerging as a critical chokepoint (Corrado, 2022; CSIS, 2023; Brill, 2024). The global production of semiconductors is extraordinarily complex and geographically concentrated, especially within the Indo-Pacific. Taiwan, through its foundry giant TSMC, holds a near-monopoly on the manufacturing of the most advanced logic chips (below 10 nanometers) (Corrado, 2022). South Korea is dominant in memory chips, while Japan is a key supplier of specialized materials and manufacturing equipment (Corrado, 2022; CSIS, 2023). This concentration creates profound strategic vulnerabilities; a disruption in Taiwan, for instance, would have catastrophic consequences for the global economy (Corrado, 2022; Journal of Global Business and Competitiveness, 2024).

Recognizing this vulnerability and China's ambition to dominate the industry, the United States has initiated a "tech cold war." The centerpiece of U.S. strategy is a "small yard, high fence" approach, implementing sweeping export controls to deny China access to advanced semiconductor technology, chip-design software (EDA), and manufacturing equipment (FPRI, 2024; Institute of New Europe, 2025; IDSA, 2025; Foreign Policy Research Institute, 2024). The goal is to slow China's military modernization, which is heavily dependent on these advanced chips for capabilities like artificial intelligence (Institute of New Europe, 2025). These controls have significantly disrupted China's tech sector but have also inflicted revenue losses on U.S. and allied firms, which rely heavily on the Chinese market (ITIF, 2023; CSIS, 2024). In response, Beijing has accelerated its massive state-led drive for technological self-sufficiency, pouring billions into its domestic semiconductor industry under policies like "Made in China 2025" and a "Delete

ISSN 2815-3324 Online, ISSN 2535-0358 Print

America" campaign to replace foreign technology (CSET, 2022; China US Focus, 2025; The Alan Turing Institute, 2024; UCIGCC, 2024; MERICS, 2024). The competition extends deeply into AI, where the U.S. currently leads in developing the most advanced models, but China is rapidly catching up by leveraging its vast data resources and state-directed investment, creating a fundamental contest between open, democratic models of technological development and a state-controlled, techno-authoritarian model (CSET, 2021; U.S.-China Economic and Security Review Commission, 2024; RSIS, 2025; Hass, 2025).

4.DISCUSSION: ANALYZING THE DYNAMICS OF A NEW ERA

The findings reveal an Indo-Pacific undergoing a profound and rapid strategic transformation. The region is not simply reacting to US-China competition but is being fundamentally reordered by it, creating a new and complex set of security dynamics. This discussion synthesizes these findings to analyze the contested balance of power, the weaponization of economic interdependence, and the evolving role of regional institutions.

4.1 The Contested Balance of Power

The security architecture of the Indo-Pacific is shifting from the post-Cold War unipolar structure, dominated by the United States and its hub-and-spokes alliance system, toward a more contested and multipolar balance. The emerging order is not a singular, coherent system like NATO but a complex, multi-layered network of overlapping bilateral, minilateral, and multilateral arrangements. This can be conceptualized as a "tiered" or "latticed" security architecture.

At the highest tier of military integration and capability—focused on deterring and, if necessary, fighting a high-intensity conflict—are the core U.S. bilateral alliances with Japan and Australia, powerfully augmented by the AUKUS pact (Horowitz, 2025). This tier is exclusive, technology-intensive, and represents the "hard edge" of the U.S.-led coalition. A second tier is occupied by more flexible, politically-oriented groupings like the QUAD, which serves as a vehicle for strategic coordination among major democracies and for competing with China in non-military domains through the provision of public goods (Anggarini & Khoirunnisa, 2024). This tier allows for broader participation, notably from India, which shies away from formal alliance commitments (He, 2021). The third and most inclusive tier consists of the ASEAN-led forums, such as the ARF and EAS, which provide an essential, albeit limited, platform for dialogue and confidence-building that includes all major powers, including China (Sukma, 2010). This tiered structure allows regional states to engage at different levels of commitment, reflecting their varied threat perceptions and strategic hedging behaviors. The critical challenge for regional stability lies in managing the interactions and potential frictions between these tiers.

Within this dynamic, middle powers are playing an increasingly active role in shaping the regional order. Australia's adoption of a "deterrence by denial" strategy and its deep investment in AUKUS demonstrate a shift toward a more proactive and forward-leaning defense posture (Dowse, 2024). India's pursuit of "multi-alignment" allows it to engage with competing blocs, maximizing its strategic autonomy while positioning itself as a crucial swing state in the regional balance (Singh, 2025; Abensour, 2025). This active agency challenges a simplistic bipolar view of the region, highlighting a more complex multipolar dynamic nested within the overarching U.S.-China rivalry. However, this diffusion of power also complicates deterrence and crisis management. From a critical perspective, U.S. strategy can be interpreted as envisioning the Indo-Pacific as a "strategic frontier" or "sacrifice zone," a theater where great power competition can be waged far from the American homeland, thereby placing a disproportionate risk and burden on its forward-deployed allies and partners (Jackson, 2025).

4.2 The Weaponization of Interdependence

The strategic competition in the Indo-Pacific has fundamentally altered the nature of globalization, challenging the liberal institutionalist premise that economic integration inherently fosters peace. Instead, the region is a prime example of the "weaponization of interdependence," where economic and

technological linkages are no longer just sources of mutual prosperity but are actively leveraged as instruments of state power (Sundararaman, 2022; Corrado, 2022; Farrell & Newman, 2025, as cited in TNSR, 2025).

China's Belt and Road Initiative exemplifies this trend. Beyond its stated economic goals, the BRI functions as a tool to create economic dependencies, secure access to strategic resources and infrastructure, and build political loyalties, thereby translating economic influence into geopolitical leverage (IISS, 2021; Council on Foreign Relations, 2023). The United States and its allies have responded in kind, though with a different model. U.S. export controls on semiconductors are a clear attempt to exploit China's dependence on foreign technology to create a strategic "chokepoint," aiming to slow its military and technological advancement (Corrado, 2022; Farrell & Newman, 2025, as cited in TNSR, 2025). Initiatives like the PGII and the Indo-Pacific Economic Framework for Prosperity (IPEF) are designed to offer an alternative, rules-based model of economic engagement that strengthens supply chain resilience among like-minded partners—a strategy often referred to as "friend-shoring" (Goto & Hughes, 2022). This geoeconomic contestation is forcing a structural realignment of global supply chains, creating bifurcated systems in critical technology sectors and compelling nations and multinational corporations to navigate an increasingly politicized economic landscape.

4.3 The Efficacy and Limits of Regional Institutions

The current institutional landscape of the Indo-Pacific is a patchwork of arrangements with varying degrees of effectiveness in managing regional security. The proliferation of minilateral groupings like the QUAD and AUKUS is a direct consequence of the perceived limitations of ASEAN-led multilateralism. ASEAN's consensus-based, non-binding, and dialogue-focused approach, while valuable for fostering a sense of regional community, has proven inadequate for addressing hard security challenges, from China's gray-zone coercion in the South China Sea to the internal collapse of Myanmar (German Institute for International and Security Affairs, 2022; Laksmana, 2020; IISS, 2025). This has created a demand for more agile, capable, and like-minded coalitions that can generate credible deterrence.

However, this trend toward minilateralism creates its own paradox. In seeking to build more effective security coalitions, the U.S. and its allies risk undermining the very principle of an "inclusive" regional architecture they claim to support. By operating outside of and often bypassing ASEAN, these exclusive groupings challenge ASEAN's centrality, potentially leading to a more fragmented and polarized region where smaller states feel pressured to choose sides (Laksmana, 2021; Chong, 2024). This highlights a central tension in the region's security architecture: the trade-off between the inclusivity and legitimacy of broad multilateral forums and the effectiveness and decisiveness of smaller, capability-focused minilaterals. The current "messy" architecture, with its overlapping and sometimes competing institutions, may be an adaptive response to this dilemma, but it also creates risks of strategic incoherence and duplication of effort, making the management of regional flashpoints in the Taiwan Strait, the South China Sea, and along the Sino-Indian border more complex and perilous (Hanggarini & Perwita, 2024; Singh, 2025).

5. CONCLUSION AND RECOMMENDATIONS

This analysis confirms that the Indo-Pacific has become the central theater of 21st-century great power competition. The strategic rivalry between the United States and China is the principal organizing force, driving a fundamental restructuring of the regional security architecture. This has resulted in a complex, multi-layered system where traditional U.S.-led bilateral alliances are now augmented by flexible, often exclusive, minilateral groupings like the QUAD and AUKUS.

These new formations are designed to create a more robust balance of power against China's military modernization and geoeconomic expansion. The findings demonstrate that this competition is being waged across multiple domains: a naval and nuclear arms race is accelerating, economic interdependence is being weaponized through infrastructure competition and a "tech cold war" centered on semiconductors, and established regional institutions like ASEAN are facing profound challenges to their

centrality and effectiveness. While the emerging networked security architecture enhances deterrence, it also creates a more fragmented and contested environment, increasing the risks of miscalculation and unintended escalation.

The strategic developments outlined in this paper offer a compelling validation of neorealist theory, which posits that states in an anarchic international system will seek to balance against a rising power. The revitalization of the QUAD and the formation of AUKUS are clear manifestations of countervailing coalitions forming to check China's growing military and economic might (Mearsheimer, 2014). Concurrently, these trends highlight a crisis for liberal institutionalism. The struggles of ASEAN-led forums to manage hard security disputes and the pivot by key actors toward smaller, exclusive minilaterals suggest that broad, consensus-based institutions are proving insufficient in an era of intensified great power competition, challenging the liberal premise that such institutions are the primary guarantors of regional stability (Nagy, 2023; Beeson, 2022).

Based on the analysis, the following policy recommendations are proposed to mitigate risks and promote a more stable and cooperative regional order:

1. Strengthen Crisis Management and De-escalation Mechanisms: The high density of military forces and the frequency of encounters in contested areas like the South China Sea and the Taiwan Strait create a significant risk of accidental escalation (Mastro, 2024; Cooke et al., 2025). It is imperative for the United States, China, and other key regional powers to establish and, crucially, utilize robust crisis communication channels. This includes reactivating and professionalizing military-to-military hotlines to ensure they are reliable in a crisis, unlike in past instances where they have gone unanswered (USIP, 2024; Cooke et al., 2025). These mechanisms should be expanded to include protocols for managing encounters between coast guard and maritime militia vessels, which are often involved in gray-zone incidents.
2. Foster a Hybrid and Interoperable Security Architecture: Rather than treating minilateral groupings and ASEAN-led forums as mutually exclusive, policymakers should actively seek to build bridges between them. The QUAD, for instance, should institutionalize its engagement with ASEAN, acting as a "strategic filler" that provides public goods and capacity-building in areas where ASEAN is constrained, thereby amplifying rather than supplanting ASEAN's role (Laksmana, 2021). This requires a concerted diplomatic effort to ensure the various tiers of the regional architecture—from AUKUS to the EAS—are complementary and interoperable, creating a resilient network that can manage diverse security challenges without forcing smaller nations into binary strategic choices (Cha, 2025; Wilson Center, 2023).
3. Govern Geoeconomic Competition through Multilateral Standards: To prevent the weaponization of interdependence from leading to a costly and destabilizing global economic fracture, like-minded nations should collaborate to establish clear, transparent, and enforceable rules for geoeconomic conduct (Institut Montaigne, 2024; Dadabaev et al., 2025). This involves moving beyond competing infrastructure initiatives to create a unified multilateral framework for quality infrastructure investment, building on the principles of the PGII and BDN (Goto & Hughes, 2022). In the technology sphere, the focus should be on building resilient and diversified supply chains ("friend-shoring" or "ally-shoring") for critical components like semiconductors, rather than pursuing unattainable and inefficient national self-sufficiency. This requires deep coordination on investment screening, export controls, and joint R&D to maintain a collective technological edge while mitigating the risks of chokepoint vulnerability (Corrado, 2022; CSIS, 2023).
4. Reinforce the Rules-Based Order through Collective Resilience: Upholding a "rules-based order" requires more than military deterrence; it demands a credible, collective response to coercive actions. Regional partners should develop a "collective resilience" framework, wherein an act of economic coercion or gray-zone aggression against one member triggers a coordinated diplomatic and economic support package from the others (Cha, 2025). This strategy, similar to the EU's anti-coercion instrument, would raise the costs and diminish the benefits of such behavior for any potential aggressor, thereby strengthening deterrence across both the economic and security domains without resorting to direct military confrontation (Singh, 2025; USIP, 2024).

5. Broaden the Coalition by Engaging Middle Powers and European Partners: To create a more resilient and broad-based coalition for a rules-based order, the United States and its core allies should deepen engagement with key regional middle powers—such as South Korea, Indonesia, and Vietnam—and extra-regional actors like the European Union (Congressional Research Service, 2023). This involves aligning respective Indo-Pacific strategies and creating flexible pathways for participation in specific initiatives, such as inviting South Korea to collaborate on AUKUS Pillar II advanced capabilities or integrating the EU's Global Gateway initiative with the PGII to amplify geoeconomic competition (Lee, 2023; Laksmana, 2021; Trinh & Nguyen, 2024). By fostering a wider network of cooperation, this approach can distribute the burden of maintaining regional stability and present a more unified front against coercive behavior.

5.1Future Research Directions

The strategic dynamics of the Indo-Pacific are evolving rapidly, presenting numerous avenues for future research. A critical area for inquiry is the long-term impact of artificial intelligence and autonomous weapons systems on deterrence stability in a region with multiple nuclear powers, a domain where the risk of rapid, unintended escalation is particularly acute (RAND Corporation, 2025; Horowitz, 2022). Further research is also needed to assess the long-term viability of middle-power hedging and "multi-alignment" strategies as US-China competition hardens, and to explore the potential pathways for building a more cooperative security order that can manage great power rivalry while addressing shared transnational threats like climate change and pandemics.

REFERENCES

Banasiak, J. (2020). Historic-legal aspect of military order as a special institution of criminal law against the background of international law and Polish legislation. *Studies in the Field of Juridical Sciences. Miscellanea, 10*, 9–32.

Czyżak, M. (2012). Military penal law of the period of the Kingdom of Poland 1815–1831. *Military Legal Review, 3*, 11.

Dunaj, K. (2015). Military courts as organs of justice. *Studia Iuridica Lublinensia, 24*(4), 9.

Frąckowiak, K. (2023). Some remarks on the limits of the countertype of ultimate military necessity in the context of deprivation of a soldier's life (Art. 319 of the Criminal Code). *Military Legal Review, 3*, 5–18.

Gensikowski, P. (2007). Problematics of the legal basis for requesting the competent commander to impose a disciplinary penalty in cases of offences and fiscal offences. *Military Legal Review, 2*, 21.

Hoc, S. (2016). Commentary on Article 323 of the Criminal Code. In M. Filar (Ed.), *Penal Code. Commentary*. Wolters Kluwer S.A., LEX/el.

Justification of the military part of the government's draft Penal Code. (1997). In *New Penal Code of 1997 with justifications* (p. 213). Ministry of Justice.

Kutzmann, W. (2025). Commentary to Article 332 of the Penal Code. In R. A. Stefański (Ed.), *Penal Code. Commentary*. C. H. Beck, Legalis/el.

Kutzmann, W. (2025). Commentary to Article 337 of the Penal Code. In R. A. Stefański (Ed.), *Penal Code. Commentary*. C. H. Beck, Legalis/el.

Majewski, J. (2023). Mutual relationship of the provisions of Articles 329–330 and 58 § 3 and 4 of the Penal Code. *State and Law, 3*, 64–70.

Majewski, J. (2024). Commentary to Article 323 of the Penal Code. In J. Majewski (Ed.), *Penal Code. Commentary*. Wolters Kluwer S.A., LEX/el.

Przyjemski, M., & Kmieciak, H. (2014). Military part of the substantive criminal law. In A. Marek (Ed.), *System prawa karnego, Vol. XI*. In M. Bojarski (Ed.), *Special areas of criminal law: Military, fiscal and extra-code criminal law* (p. 202). C. H. Beck.

Sieracki, W. (1983). Some problems of evolution of military criminal (substantive) law in the period 1963–83. *Military Legal Review, 3*, 235.

Szeleszczuk, D. (2024). Commentary to Article 317 of the Penal Code. In A. Grześkowiak & K. Wiak (Eds.), *Penal Code. Commentary* (p. 1856). C. H. Beck.

Zgoliński, I. (2020). Limitation of punishment in the light of the Constitution of the RP. In A. Grześkowiak & I. Zgoliński (Eds.), *Polskie prawo karne na tle wartości Konstytucji RP* (p. 79). KPSW.

Ziółkowska, A. (2023). Commentary to Article 337 of the Penal Code. In V. Konarska-Wrzosek (Ed.), *Penal Code. Commentary*. Wolters Kluwer S.A., LEX/el.

Lizut, R. (2025). Security challenges of IoT integration in national and state critical infrastructures. *Politics & Security, 13*(3), 82–94. Doi: 10.54658/ps.28153324.2025.13.3.pp.82-94

SECURITY CHALLENGES OF IOT INTEGRATION IN NATIONAL AND STATE CRITICAL INFRASTRUCTURES

Rafał Lizut
John Paul II Catholic University
Lublin, Poland
rafal.lizut@kul.pl
https://orcid.org/0000-0002-6067-1469

Abstract. *This investigation scrutinizes the incorporation of Internet of Things (IoT) systems within national infrastructures, accentuating both operational advantages and notable security challenges. It delves into the stratified architecture of IoT, underscoring vulnerabilities that emerge from device constraints, varied deployment environments, and inadequate cybersecurity practices. The examination addresses external threats such as distributed denial-of-service attacks, malware, and data manipulation, in conjunction with internal risks including insider threats and misconfigurations. The ramifications of these threats on critical infrastructure sectors, such as energy, transportation, and healthcare, are evaluated, with a focus on operational disruptions and economic impacts. Emergent defense strategies involving Software-Defined Networking and machine learning-based anomaly detection are assessed for their capability to bolster security posture. Furthermore, the role of national cybersecurity strategies and regulatory frameworks is analyzed, concentrating on multi-stakeholder coordination, legal measures, and adaptive governance to manage evolving risks. The findings highlight the imperative of integrating technical, organizational, and policy approaches to protect IoT-enabled critical systems and sustain national security resilience.*

Keywords: Internet of Things (IoT), Critical Infrastructure Protection, Cybersecurity, Distributed Denial-of-Service (DDoS), Malware and Data Manipulation.

1. INTRODUCTION

The progressive incorporation of Internet of Things (IoT) systems into national infrastructures presents considerable advantages in terms of both operational efficiency and situational awareness. By harnessing real-time data streams from an increasing array of connected devices, decision-makers are able to conduct more precise monitoring of environments such as transportation systems, energy grids, healthcare facilities, and industrial control systems.

These capabilities enhance the potential for early detection of incidents like equipment failures or environmental hazards, thus providing opportunities for intervention before issues escalate into significant crises. However, alongside these benefits comes a notable expansion of the attack surface accessible to adversaries. A major concern is that IoT devices, despite their functional and deployment diversity, frequently exhibit systemic security weaknesses. They are often developed under stringent cost and time-to-market constraints, prompting manufacturers to prioritize usability and compatibility features over stringent cybersecurity engineering (Group, 2018). Default configurations, inadequate integrity checks, and the absence of prompt firmware updates create persistent vulnerabilities, rendering these devices attractive targets for exploitation (Kudini, 2024).

In practice, these weaknesses not only jeopardize individual devices but also potentially serve as entry points into broader networks that vital services rely on. Threats manifest through various vectors. Externally, attacks encompass distributed denial-of-service (DDoS) campaigns using botnets composed of compromised IoT nodes, unauthorized access attempts by exploiting insecure APIs or interfaces, and targeted malware deployments intended to disrupt specific operational processes (Buiya et al., 2024). Data interception and manipulation may also occur when communications between IoT endpoints are neither properly encrypted nor authenticated.

Concurrently, internal risks, such as malicious insiders possessing extensive system knowledge or negligent administrative practices, can compromise even robust security architectures (Garcia-Morchon et al., 2019). This duality, characterized by external hostility coupled with internal vulnerability, renders the cybersecurity challenge particularly intricate. Connected IoT infrastructures supporting smart buildings or municipal services further exemplify these vulnerabilities. A compromised subsystem, such as an HVAC controller or alarm mechanism, can instigate cascading operational repercussions: triggering false alarms to divert responders, altering environmental controls to disrupt occupancy comfort, or compromising physical access management systems (Group, 2018).

When such systems become integrated with other critical assets such as data centers or emergency services networks, the potential exists for an attack to propagate across domains previously isolated from one another. In conjunction with technical vulnerabilities, privacy considerations add an additional layer of complexity. The aggregation of personally identifiable information (PII), including location records from connected vehicles or biometric data from medical wearables, constitutes a significant target for espionage or criminal exploitation (Al-Garadi et al., 2020). A breach involving these datasets poses risks of both direct harm to individuals and the erosion of public confidence in IoT-enabled services.

Concerns are particularly pronounced in healthcare contexts, where sensitive medical information flows between patient-facing devices and cloud platforms. For national security stakeholders, these scenarios concerning the exploitation of information cannot be disregarded. Strategic adversaries might leverage compromised IoT deployments for purposes of surveillance or disinformation. Information extracted from industrial sensors could disclose production patterns in sectors crucial to defense supply chains. Disruptions to grid-connected sensors or distributed generation units could result in significant impacts on the energy sector (Mohamed et al., 2023). These implications underscore the critical intersection between defending IoT systems and safeguarding broader critical infrastructure sectors. Emerging solutions such as Software-Defined Networking (SDN), when integrated into IoT architectures, show promise for enhancing control over dynamic network configurations and enabling automated policy enforcement to counteract specific threats (Oredola & Ashraf, 2024).

The centralization of control logic within SDN allows administrators to apply granular traffic filtering rules across diverse device fleets with greater agility compared to static configurations. Nonetheless, SDN controllers themselves remain valuable targets for attackers; absent appropriate protection measures, such as secure channel protocols and monitoring frameworks incorporating anomaly detection algorithms, adversaries could potentially manipulate them to orchestrate detrimental actions on a large scale. Furthermore, artificial intelligence-driven telemetry analysis represents another promising avenue for advancing threat detection within complex IoT ecosystems.

Machine learning pipelines trained on varied attack signatures can assist in distinguishing benign traffic anomalies from authentic intrusion attempts (El-Sofany et al., 2024). These models, which continuously adapt by utilizing streaming inputs from deployed IoT environments, may discern new patterns indicative of evolving attacker strategies. However, researchers emphasize that the accuracy of these models is significantly contingent upon the quality and comprehensiveness of the training datasets (Al-Garadi et al., 2020). The generation of datasets accurately reflecting real-world attacks presents significant challenges due to the diversity of incidents and the rapid emergence of new exploits. Systematically organized vulnerability reporting mechanisms serve as a crucial adjunct to automated defense systems. Facilitating the submission of detailed incident evidence by both internal teams and external actors, such as white-hat researchers, ensures that organizations can quickly triage credible threats and implement mitigations before incidents escalate further (Group, 2018).

This collaborative methodology enhances collective readiness, mitigating the risk of undetected vulnerabilities persisting due to prolonged detection cycles. Any discourse regarding the security of IoT deployments must integrate comprehensive risk assessments alongside privacy impact evaluations. Risk assessments categorize threats based on their likelihood and potential operational impact to prioritize mitigation efforts towards the most severe risks, while privacy impact evaluations ensure adherence to legal mandates concerning the handling of personally identifiable information (PII) and identify areas susceptible to data misuse (Garcia-Morchon et al., 2019).

Both evaluations provide structured foundations for the effective allocation of resources between preventative engineering measures and responsive capabilities. It is plausible that without enhanced standardization concerning secure development practices—such as default encryption for communication channels, secure boot processes for firmware integrity validation, and authentication protocols resistant to replay and spoofing attempts—the gap between deployment velocity and security assurances will broaden. Given the rapid evolution of functionalities in this domain, adaptive security strategies, capable of learning from both historical attack patterns and real-time monitoring outputs, will be particularly critical in balancing the benefits of innovation against the exposure to national-level threats.

2 FOUNDATIONS OF IOT IN THE CONTEXT OF NATIONAL AND STATE SECURITY

2.1 Definition and Scope of IoT

The Internet of Things (IoT) can be understood as an expansive network architecture comprising diverse physical devices, ranging from basic sensor nodes to sophisticated autonomous machines, interconnected through both wired and wireless communication technologies to facilitate bidirectional interaction between the physical environment and digital systems.

These interconnected entities are distinguished by their embedded sensing and actuation functionalities, enabling them to gather environmental data, process information either locally or remotely, and execute actions contingent upon pre-defined instructions or algorithmic triggers. Their implementation spans a variety of settings, including industrial facilities, healthcare environments, transportation infrastructure, agricultural operations, and domestic living spaces, thereby enhancing both operational utility and the potential attack surface. A salient characteristic of IoT systems is their layered architecture, typically divided into layers such as the perception layer (consisting of physical devices and sensors), the network layer (responsible for data transmission), and the application layer (providing functional outputs to end users) (Al-Garadi et al., 2020).

Each of these layers presents unique security challenges due to variations in protocols, computational resources, and exposure to external interfaces. At the foundational level of the perception layer, physical devices are frequently constrained in processing power and memory capacity. This limitation can hinder the incorporation of advanced cryptographic algorithms that would otherwise enhance their robustness against attacks (Voronko, 2024).

Moreover, design decisions made at this layer significantly impact the overall risk profile of the system. From a conceptual perspective, IoT is not confined to static deployments but includes highly dynamic configurations where devices may spontaneously join or leave networks, and connections might be transient. Such dynamism permits versatility but also influences the security landscape by augmenting vectors for unauthorized access or malicious manipulation (Ani et al., 2019).

For instance, devices integrated into supply chains within critical infrastructure sectors such as energy or transportation may exhibit intermittent connectivity during maintenance or operational cycles. In these contexts, the transient nature of these connections can conceal ongoing threats until they intensify. A critical viewpoint in defining the Internet of Things (IoT) involves acknowledging its integration with existing communication technologies and emerging computational paradigms, including cloud computing and machine learning.

Numerous IoT applications depend on cloud infrastructure to provide scalable storage, facilitate remote computation, and enable service orchestration (Kudini, 2024). Moreover, some applications incorporate machine learning models at various junctures within the architecture to facilitate adaptive decision-making based on real-time sensor data (El-Sofany et al., 2024). This combination allows for advanced functionalities such as predictive maintenance in manufacturing operations or contextually aware automation within smart cities.

Nevertheless, it also obscures the conventional demarcations between cyber infrastructures and physical systems, which is a significant consideration when evaluating risks at the national level. From a pragmatic standpoint, IoT subsumes a broad array of device categories: industrial control sensors assessing flow rates in pipelines, wearable health monitors transmitting biometric data, environmental probes monitoring air quality, logistics tags with embedded GPS for asset tracking, and consumer devices like smart refrigerators interfacing with energy demand-response systems. Each operates under distinct regulatory requirements, network conditions, and protocols for lifecycle management.

Consequently, defining IoT must accommodate this diversity while recognizing shared foundational features, such as persistent connectivity, data generation aligned with sensing functions, and the capacity for autonomous or semi-autonomous operation. An additional scope-related dimension surfaces when considering the interaction between IoT systems and broader digital ecosystems. They are not isolated entities; rather, they engage with enterprise IT assets, operational technology systems that control physical processes, mobile endpoints borne by individuals, and even other IoT networks managed by third parties (Group, 2018).

These interconnections augment overall system complexity and foster interdependence across various domains. Disruption in one segment, whether induced by technical failure or a targeted attack, may propagate through software dependencies, shared communication channels, or misconfigured interfaces. The extensive scope of IoT necessitates a reevaluation of traditional threat modeling methodologies, which were predominantly optimized for discrete software applications. As noted in previous studies (Aufner, 2020), many established frameworks inadequately anticipate hardware-based threat vectors unique to IoT deployments because these frameworks were developed under assumptions that treated hardware as either trusted or immutable during analysis.

Consequently, a comprehensive approach necessitates the incorporation of artifacts from the device design stages alongside conventional software lifecycle inputs to accurately enumerate systemic vulnerabilities. In the context of national security discourse, defining IoT surpasses the mere listing of device types or communication protocols. Instead, it necessitates an understanding of their role within critical infrastructures, such as emergency response services, food distribution networks, dam monitoring systems, military operations centers, educational campuses with connected laboratories, and hospital systems equipped with remote diagnostic tools (Ani et al., 2019).

The interconnectivity across these sectors implies that IoT's operational boundaries often misalign with the jurisdictional or organizational boundaries employed in governance frameworks. Additionally, scope determination must encompass privacy as a core parameter, alongside considerations of reliability and resilience. Each connected node, capable of generating detailed telemetry—whether through the recording of geolocation trails via GPS-enabled units or the scanning of thermal signatures via infrared sensors—carries potential implications for individual privacy rights and corporate intellectual property protection (Al-Garadi et al., 2020).

Addressing these implications requires embedding privacy-preserving principles not as sporadic afterthoughts, but as integral components within the core architectural definitions utilized during procurement and standardization phases. Therefore, the definition and scope of IoT comprise a complex matrix: it spans layers from sensing hardware to analytics-rich applications; encompasses industries from civilian retail environments to mission-critical defense logistics; navigates constraints imposed by the minimal capability of embedded systems alongside complexities introduced by integration into global cloud infrastructures; and encompasses both operational safety margins and normative discussions regarding data sovereignty. By comprehending this vastness early in strategic planning processes centered on national interests, stakeholders are better equipped to manage both the immediate security issues elucidated in Section 1 and the enduring sustainability challenges inherent in extensive, connected ecosystems.

2.2 Relevance of IoT to Critical Infrastructure

The convergence of Internet of Things (IoT) implementations with critical infrastructure systems is particularly noteworthy due to the provision of indispensable services by these sectors, where disruptions

can lead to cascading societal and economic impacts. Systems such as energy grids, water distribution networks, transportation mechanisms, and emergency communication frameworks necessitate real-time operational insight to maintain effective functioning under varying conditions of load and stress. IoT technologies enable this level of awareness by delivering continuous data streams from widely distributed assets, thereby allowing system operators to identify anomalies, foresee maintenance requirements, and manage distributed resources more efficiently.

This degree of connectivity enhances the adaptive and responsive nature of infrastructure while simultaneously exposing it to novel attack vectors that were previously confined to isolated information technology environments. From a national security standpoint, critical infrastructure is viewed both as a strategic asset and as a potential point of vulnerability. The European Union's classification of pivotal sectors at both the supranational and state levels underscores the importance of domains such as energy and transport to societal stability (P0103tra0219cu, 2021). Integrating IoT devices into these systems augments capabilities; for instance, smart metering can optimize electricity distribution, and connected sensors can manage traffic flows in real-time. However, these devices may also become points of weakness if their firmware integrity is compromised or if communication channels are intercepted.

When operational technology closely integrates with information technology layers via IoT, threats originating in the digital realm can quickly extend into the physical world, a scenario not anticipated in previous engineering designs. An additional perspective arises in the defense sector's utilization of IoT-enabled infrastructures, where real-time situational updates from remote sensors can guide tactical decisions or logistical coordination. Yet, the sophistication of adversaries in cyberspace, as evidenced by instances where state actors employ coordinated information confrontation strategies, indicates that IoT assets will be targeted for intelligence gathering or disruption.

The amalgamation of AI-enhanced analytics with extensive sensory data volumes could produce unprecedented predictive capabilities for asset management and threat anticipation but might equally be manipulated to mislead decision-makers through data tampering or sensor deception. Cybersecurity considerations significantly influence the discourse surrounding the integration of IoT into critical infrastructure. As systems become progressively interconnected across borders and administrative boundaries, any deviation or malfunction holds the potential for rapid escalation beyond its initial point of origin (Ahmed et al., 2023). The impact of new paradigms such as IoT combined with cloud services heightens this dynamic: while centralization enhances orchestration efficiency, it also forms high-value targets whose compromise could simultaneously affect multiple dependent systems. Distributed denial-of-service attacks on services crucial to operational continuity have already illustrated the swift manner in which vulnerabilities within consumer-centric IoT ecosystems can extend into core infrastructure operations (Group, 2018).

The advancement of industrial control environments to include machine learning-based monitoring systems for IoT security represents an opportunity to manage these threats proactively. The process of learning normative patterns of device-to-device interactions within intricate infrastructure networks enables models to identify anomalies indicative of intrusion efforts prior to the occurrence of significant damage (Al-Garadi et al., 2020). For instance, an unexpected increase in command signals transmitted to remote grid components outside standard operational hours may be recognized as abnormal and subsequently activate automated containment protocols.

However, reliance on machine learning and deep learning methodologies introduces new dependencies concerning the quality of training data; biases or deficiencies in the data could undermine detection accuracy, particularly in confronting emergent attack vectors (El-Sofany et al., 2024). Policy implications hold considerable significance as well. Emphasized in scholarly examinations of resilience modeling for critical national infrastructure (CNI), evolving threat landscapes necessitate not merely incremental enhancements but occasionally comprehensive transformations of established protection strategies (Ani et al., 2019). Current critical infrastructure protection (CIP) strategies frequently exhibit deficiencies in covering a broad range of attributes pertinent to contemporary threats, notably those associated with human-mediated cyber intrusions rather than environmental hazards.

Integrating IoT-specific elements into these frameworks is crucial due to the increasing convergence between cyber threats and physical operational repercussions with each successive iteration of device

integration. An often-overlooked yet vital component in sustaining resilient IoT-enhanced critical infrastructures is effective key management within heterogeneous network configurations (Attkan & Ranga, 2022).

Energy distribution nodes that are interconnected through decentralized IoT architectures possess distinct fault tolerance characteristics compared to localized centralized structures; the selection of appropriate key management systems (KMS) for encryption directly influences whether an attacker exploiting a single node can freely infiltrate others. Privacy-related risks are intrinsically linked to security concerns. IoT deployments integrated into infrastructure routinely gather sensitive data sets, from passenger movement patterns within public transit systems to industrial production statistics, which, if compromised, could produce competitive intelligence or facilitate hostile reconnaissance activities.

In transportation sectors such as railways, robust encryption protocols like SSL/TLS are employed to secure communications between embedded control units and supervisory platforms, while layered authentication regulates access rights to individual device interactions. Although this mitigates certain classes of exploitation, consistent vigilance against approaches such as distributed denial-of-service aimed at disrupting operational accessibility is essential (Voronko, 2024).

Furthermore, the progression toward advanced multi-layered architectures incorporating virtualized network functions (VNFs) alongside conventional physical network functions (PNFs) adds complexity for defenders responsible for safeguarding the interfaces between devices and users (El-Sofany et al., 2024). Internal threats from compromised on-domain devices must be approached distinctly from external penetrations arising from wide-area networks, neglecting either poses risks of systemic destabilization. Bearing in mind incidents like the Mirai botnet's exploitation of unsecured IoT components to destabilize major internet services indirectly leveraged by infrastructure operators (Group, 2018), it is apparent that the security of these devices cannot be dismissed as secondary.

Threat assessments must contemplate how vulnerabilities within ostensibly peripheral assets could trigger national-scale disruptions if foundational services, such as DNS resolution, are compromised during coordinated attacks. Ultimately, the significance of IoT integration within critical infrastructure is encapsulated in a paradox: while it provides transformative enhancements in efficiency, adaptability, and foresight for systems crucial to national welfare, it concurrently expands potential pathways for adversaries to inflict large-scale damage.

Addressing this duality necessitates not only technical fortification through encryption-by-default policies, anomaly detection systems, and decentralized fault-tolerant structures, but also adaptive governance frameworks that harmonize policy evolution with technological advancements (P0̈103tra0̈219cu, 2021). Only through these measures can nations fully actualize the potential of interconnected infrastructure without jeopardizing its fundamental resilience.

3. THREAT LANDSCAPE FOR IOT IN NATIONAL SECURITY

3.1 External Threats and Internal Threats Overview

The incorporation of IoT components into critical systems poses a bifurcated security challenge, influenced by threats arising both externally and internally within the operational surroundings. External threats predominantly originate from malicious entities exploiting vulnerabilities inherent in device design, communication protocols, or network configurations. Such threats may encompass distributed denial-of-service (DDoS) campaigns, which target the availability of essential services, to more targeted invasions leveraging compromised credentials or vulnerabilities in exposed interfaces (Hadi et al., 2023).

The deployment of botnets comprised of unsecured IoT devices has already illustrated how economically viable, internet-connected endpoints can be transformed into potent attack platforms, capable of disrupting not only the intended target but also ancillary systems dependent on shared infrastructure (Group, 2018). Adversities posed by external adversaries seeking operational disruption may utilize spoofing techniques to introduce falsified sensor data into automated control loops or instigate man-in-the-middle attacks to intercept and alter communications between nodes. Such manipulations can

provoke unpredictable physical-world behaviors, such as erroneous actuator responses in industrial environments, thereby diminishing safety and reliability (Chen et al., 2022). In segments where instantaneous response is indispensable, as in vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications, any latency introduced by such interference may undermine decision-making processes vital for safety (Group, 2018).

Cyber-espionage constitutes a related category of external threats, wherein strategic actors endeavor to extract sensitive operational data without activating alerts. In contexts concerning national defense, these infiltrations might target sensor networks established for perimeter surveillance or logistic coordination, thereby mapping asset locations and activity patterns over time. Manipulations of this nature can transpire without immediate overt damage, yet they pave the way for subsequent sabotage or disinformation campaigns. Equally troubling is the potential for external attackers to exploit firmware vulnerabilities uncovered through public vulnerability feeds or reverse engineering; once a defect is comprehended, extensive automated scanning tools can identify susceptible devices across global networks in a matter of minutes (El-Sofany et al., 2024).

The heightened complexity and heterogeneity of IoT networks augment exposure due to the challenge of enforcing standardized defenses across diverse hardware architectures and software stacks (Garcia-Morchon et al., 2019). The internal threat landscape exhibits distinct characteristics but remains equally severe. Insider threats may emerge from individuals with legitimate access who engage in malicious or negligent activities.

This could entail altering configuration files to bypass authentication protocols, installing unauthorized software modules that establish backdoors, or disabling logging services to evade detection during unauthorized activities (Hadi et al., 2023).

In contexts where IoT devices function autonomously within critical infrastructure frameworks, even ostensibly minor modifications at the device level, such as adjusting calibration parameters, can propagate through dependent processes due to the tight coupling between sensors and control mechanisms (Ani et al., 2019). Users possessing privileged administrative rights pose particular risks if their accounts are compromised, as these credentials often provide comprehensive control over device behavior and connectivity pathways. Internal risks also include latent vulnerabilities inherent in the devices themselves. Many IoT endpoints have limited processing capabilities, resulting in constrained adoption of robust encryption algorithms or sophisticated anomaly detection mechanisms locally (Al-Garadi et al., 2020).

Firmware may be distributed with hardcoded default passwords or outdated protocol implementations that are never patched due to inadequate lifecycle maintenance policies. These weaknesses constitute primary internal threats when they offer footholds for adversaries already present within a segmented network, enabling lateral movement towards higher-value targets undetected. There is also the dimension of accidental insider threats, prompted by misconfiguration or insufficient security awareness among operational personnel. For instance, connecting a maintenance laptop infected with malware to a supposedly isolated industrial IoT subnet can inadvertently bridge air-gapped protections.

Similarly, activating unsecured remote-access features on field devices for convenience can expose them to unsolicited internet connections (Garcia-Morchon et al., 2019). Such unintentional exposure is exacerbated in scenarios where operational teams underestimate the interconnectedness of modern systems; what appears to be an isolated endpoint may indeed interface with multiple subsystems via machine-to-machine protocols.

A complicating factor in the analysis of both external and internal threats is the convergence of cyber layers with physical process control. Attacks initiated externally may swiftly manifest as internal disruptions once malware propagates within trusted perimeters through compromised update servers or supply chain insertions. Likewise, malicious insiders could secrete authentication tokens externally or collaborate with foreign entities, transforming an internal breach into a broader coordinated offensive (Group, 2018).

In industrial control system contexts superimposed upon IoT frameworks, these composite attacks hinder attribution efforts while reducing available response times before critical thresholds are surpassed. Addressing these multifaceted threats necessitates incorporating proactive monitoring capable of detecting anomalies associated with both categories. Machine learning-based models offer early detection

potential by observing deviations from established behavioral baselines for devices and applications (El-Sofany et al., 2024). However, their efficacy can be compromised if internal actors manipulate training datasets or if novel external attack methodologies generate traffic patterns indistinguishable from legitimate surges caused by irregular operating conditions.

Accordingly, effective defenses require the amalgamation of automated pattern recognition with traditional rule-based controls informed by comprehensive risk management frameworks, such as those derived from National Infrastructure Protection Plan methodologies (Ani et al., 2019). This synthesis ensures that mitigation strategies address not only known vectors but also evolving hybrid tactics bridging external penetration attempts with internal exploitation opportunities. Ultimately, the examination of external versus internal threats in IoT-centric national security contexts elucidates that these domains cannot be regarded as mutually exclusive silos; rather, they constitute an interdependent continuum where compromise in one domain facilitates action in the other.

Safeguarding critical systems necessitates strategies cognizant of this interplay, reinforced through multi-layered authentication regimes, encrypted communication channels impervious to spoofing attempts, rigorous patch management schedules across heterogeneous fleets, and continuous education aimed at reducing risky behaviors among personnel granted operational access rights (Hadi et al., 2023). Without concurrent attention to both aspects of this equation, defenses will remain susceptible to exploitation by adversaries skilled at traversing categorical boundaries between outsider intrusion and insider facilitation.

4 IMPACT OF IOT THREATS ON NATIONAL AND STATE SECURITY

4.1 Operational Disruption and Economic Consequences

Interruptions to operational continuity instigated by IoT-associated security incidents can materialize abruptly, extending significantly beyond the immediate technical confines of the compromised system. In numerous critical infrastructure contexts, the integration of network-linked control and monitoring devices has established an operational dependence on the accuracy, timeliness, and integrity of data.

The degradation of these elements through malicious interference—via data manipulation, denial-of-service attacks, or direct sabotage of control logic—provokes consequential effects upon safety-critical processes and essential public services. In rail transport networks, for instance, cyberattacks possess the potential to manipulate or incapacitate train speed regulation systems or sensor-driven signaling mechanisms. Such interference not only temporarily stalls operations; it also heightens immediate risks to passenger safety and could precipitate accidents resulting in casualties.

Similar disruptions in cargo tracking or routing systems may hinder supply chains, disrupt just-in-time manufacturing pipelines, and induce costly delays in the transport of high-value goods (Voronko, 2024). The economic implications manifest from both direct remediation costs and indirect market impacts. Direct expenditures encompass the restoration of impacted hardware and software components, the deployment of forensic teams for incident investigations, and the maintenance of operational downtime as systems are resecured. Indirect repercussions, albeit more challenging to quantify, frequently exceed the immediate repair costs.

These include reputational damage leading to customer attrition, contractual penalties for unfulfilled service-level agreements, and diminutions in investor confidence. Media coverage that amplifies public perceptions of insecurity in the systems of a transportation operator or energy provider can perpetuate a credibility deficit long after technical faults have been rectified. Within sectors such as industrial control environments supplemented with IoT sensors and actuators, disruptions can propagate rapidly from a single vulnerable point to entire production lines interconnected through shared controllers. If attackers capitalize on firmware vulnerabilities to introduce erroneous readings or impede actuator commands during critical production phases, entire batches may be rendered defective prior to the detection of the issue (Chen et al., 2022). The economic ramifications extend significantly beyond the mere wastage of raw materials, encompassing legal disputes over breach-of-contract if defective products penetrate the market, as well as regulatory fines when safety standards are not met. Economic repercussions also materialize

from cascading failures that traverse multiple infrastructure domains. For instance, a cyberattack targeting IoT-based monitoring within the energy grid may destabilize electricity supply in specific areas. Such instability can subsequently jeopardize water distribution facilities that rely on electrically powered pumps or affect hospitals that operate without adequate backup capacity in their medical device networks. Each subsequent disruption amplifies societal costs while diluting accountability across numerous stakeholders (Group, 2018).

Attack campaigns, such as those driven by large-scale IoT botnets, illustrate how adversaries can exert economic pressure on entire sectors without necessarily breaching their core control systems. By incapacitating domain name resolution services or cloud-based application interfaces essential to traffic management platforms or logistics coordination tools, malevolent actors induce widespread degradation of services (Hadi et al., 2023). Even in the absence of physical asset damage, sustained outages diminish trust in the continuity of digital services within supply chains that increasingly depend on IoT interlinks. Beyond adversarial engineered disruptions, inadvertent device mismanagement can yield effects of equivalent operational severity.

Misconfigurations that disrupt encryption between distributed IoT sensors within a manufacturing environment may allow unsophisticated intrusions that precipitate incorrect system behaviors, leading to a complete production halt. As downtime extends over several days awaiting full recovery, partly due to frequent shortages of replacement parts for specialized embedded IoT devices, consequent revenue losses can be substantial (Al-Garadi et al., 2020). The cost structures associated with these incidents increasingly encompass expenditures aimed at compliance restoration under international cybersecurity regulations governing critical infrastructure sectors.

Post-incident investigations often uncover inadequacies such as a lack of encrypted communications or failures to authenticate update packages for IoT endpoints, deficiencies frequently highlighted in regulatory reviews following incidents (Group, 2018). Mandatory system upgrades mandated by such reviews impose capital burdens that are particularly challenging for operators handling heterogeneous fleets of legacy devices (Amro, 2024). Operational disruptions also manifest through long-term performance degradation when persistent threats remain undetected within IoT environments. A state-sponsored intrusion illicitly extracting minor amounts of proprietary industrial telemetry over an extended period may evade detection while skewing predictive maintenance algorithms utilized for asset management (Al-Garadi et al., 2020). The eventual decline in decision quality, exemplified by inaccurate predictions of component fatigue, could precipitate premature machinery failures during peak demand periods when replacements cannot be scheduled without interrupting core services. From a strategic economic vantage point, states must consider how adversarial exploitation of IoT vulnerabilities could afford asymmetrical advantages, undermining public confidence in the provision of national infrastructure without necessitating physical attacks. This undermining effect imposes pressures on government budgets through contingencies such as emergency procurement programs and heightened defense allocations to replace compromised technologies before their natural replacement cycles. Moreover, some disruptions entail geopolitical spillover effects.

Targeted interference with international freight transit systems utilizing IoT-enabled logistics coordination can divert trade flow competitiveness from targeted nations to rivals perceived as more secure channels for goods movement. The cumulative impact of market share losses across strategic industries, such as energy exports impeded by compromised pipeline monitoring systems, heightens economic vulnerability far beyond the accounting of directly affected firms. Ensuring availability and proper functionality across such interconnected ecosystems is therefore not solely an engineering challenge but a socio-economic imperative closely linked to national security planning priorities.

Effective mitigation of these disruptions necessitates proactive technical protective measures, such as segmentation between high-trust operational sub-networks and lower-trust external connections, complemented by incident response playbooks that address both rapid failover capabilities and public communication strategies during crises (Ani et al., 2019). In the absence of integrating technical resilience with coordinated economic risk containment strategies, individual attack occurrences will persist in threatening disproportionate systemic economic consequences relative to their initial access point vector within an IoT deployment architecture.

5 SECURITY GOVERNANCE AND POLICY FRAMEWORKS

5.1 National Cybersecurity Strategies and Regulatory Frameworks

National cybersecurity strategies fundamentally represent multi-layered frameworks that synthesize technological protections, legal measures, institutional coordination mechanisms, and strategic policies into a unified defense posture against both domestic and transnational cyber threats. The development of these strategies often mirrors the unique geopolitical and socio-economic environments of the nation adopting them, as well as the variety and sophistication of its critical infrastructure sectors. Nations with substantial IoT penetration in essential services are required to address not only the immediate technical concerns of device and network security but also the systemic interdependencies that give rise to cascading vulnerabilities.

A comprehensive national strategy generally commences with an evaluation of existing capacities in cyber defense. This involves an audit of physical and digital assets, assessment of human capital readiness, mapping of inter-agency coordination mechanisms, and identification of legal deficiencies in prosecuting cybercrime. Enhancing these foundations often necessitates the expansion of specialized law enforcement units and the streamlining of institutional responsibilities across government bodies. The Indonesian government, for instance, expanded its cyber defense framework to include total defense principles, increased personnel in its police cybercrime divisions from 40 to 100, restructured the National Crypto Agency into the National Cyber and Crypto Agency (BSSN), and enacted a national cybersecurity strategy that emphasizes resilience across public services, law enforcement, cultural awareness programs, and protection of the digital economy (Rizky et al., 2023).

These strategies seldom function independently; they depend on integration between government entities and private stakeholders. Numerous states formally incorporate multi-stakeholder engagement models into their policy design processes to leverage expertise from industry consortia, academia, civil society organizations, and standards development bodies (Group, 2018). This collaboration is particularly crucial in countries where standards-setting activities predominantly occur within organizations led by the private sector rather than state-run technical committees.

By integrating public-private partnerships into national frameworks, governments enhance situational awareness and expedite the remediation of identified vulnerabilities through coordinated updates or patch management campaigns on a large scale. Beyond domestic coordination mechanisms, robust strategies incorporate the international dimensions of cybersecurity policy. Governments acknowledge that digital threats readily cross jurisdictions without impediment. Consequently, bilateral agreements, engagement in multilateral cyber norms discussions, joint exercises with foreign CERTs (Computer Emergency Response Teams), and participation in global or regional security forums are integral components of proactive frameworks (Rizky et al., 2023).

This external focus enables nations to compare their capabilities with those of their peers while benefitting from intelligence-sharing arrangements that function as early-warning systems for emerging threat patterns. The development process must also account for structural challenges, such as a lack of comprehension among policymakers or stakeholders regarding specific technical requirements for secure operations, like limiting reliance on overseas-hosted critical services or enforcing encryption standards (Budiman, 2022).

Explicit procedural mandates reduce ambiguities during incidents; for instance, defining legal jurisdiction for data breaches involving servers located abroad ensures more rapid prosecution and clarity regarding notification duties. Strategic leadership is pivotal in translating high-level policies into operational practice. Leaders not only approve resource allocation but also define risk tolerance levels across sectors. They bear the responsibility of monitoring the threat horizon to identify trends, such as increases in IoT-based distributed denial-of-service attacks, and adjusting defenses accordingly (Rizky et al., 2023). Effective implementation requires detailed policy documents that delineate roles during crisis response phases; this correlates with contemporary resilience theories that advocate adaptive planning cycles devoid of fixed endpoints (Ahmed et al., 2023). For IoT-intensive national infrastructure sectors, as previously discussed in Section 4.1, strategies should encompass sector-specific annexes that address

unique protocols or operational environments. For example, industrial control systems may necessitate mandatory air-gapping for certain functions, whereas public transportation systems might focus on intrusion detection tuned for vehicular communication networks.

The integration of cryptographic requirements, addressing confidentiality, integrity verification, authentication mechanisms such as digital signatures, and robust key management protocols, ensures foundational interoperability across devices while mitigating the risk of trivial exploitation during cross-system communication (Group, 2018). Certain jurisdictions explicitly include regulatory compliance audits within their frameworks to evaluate operator conformity with security standards comparable to those instituted under directives such as the EU NIS Directive. These audits serve dual purposes as enforcement instruments and capacity-building exercises by identifying systemic vulnerabilities before adversaries do (Schaberreiter et al.).

Provisions might require regular penetration testing for operators of critical services or mandate the adoption of certified secure hardware modules in new IoT deployments targeted for vital industry applications. Furthermore, governance frameworks increasingly recognize that achieving perfect prevention against sophisticated adversaries is unattainable. They incorporate resilience-focused objectives to minimize service degradation when incidents occur. Measures in this context may range from pre-negotiated mutual assistance agreements among infrastructure proprietors ensuring spare capacity during outages (Ahmed et al., 2023), to continuous monitoring systems that supply threat intelligence platforms capable of correlating anomalies across diverse networks in real time.

Another characteristic of mature strategies is embodied in a structured regulatory environment that maintains accountability while avoiding the stifling of innovation. In developing nations, which are constructing foundational digital economies alongside critical infrastructures, regulations sometimes encounter resistance if perceived as onerous by emerging industries dependent on rapid deployment cycles for IoT solutions. Constructing proportionate regulations that balance economic incentives with stringent minimum-security assessments helps prevent scenarios where insecure consumer-grade IoT products inadvertently infiltrate industrial contexts due to ambiguous applicability scopes. Ultimately, national strategies, supported by adaptive legal frameworks, establish not merely compliance architectures but dynamic systems capable of evolving in conjunction with shifting threat landscapes. They institutionalize periodic review cycles, typically every two to five years, that accommodate the integration of lessons learned from domestic and global incidents (Rizky et al., 2023).

By embedding this reflexivity within governance structures and ensuring that each cycle includes multi-sectoral consultation along with opportunities for cross-border dialogue, states position themselves more effectively to respond decisively whether disruptions originate within their jurisdictional boundaries or beyond.

6 CONCLUSION

The incorporation of Internet of Things (IoT) technologies into national infrastructures presents a dual-faceted scenario, offering significant enhancements in operational efficiency and situational awareness, while simultaneously introducing considerable security challenges. The diverse and resource-constrained nature of IoT devices, coupled with their extensive deployment across critical sectors such as energy, transportation, healthcare, and industrial control, creates a complex attack surface that is susceptible to both external and internal threats.

These vulnerabilities arise from design trade-offs that prioritize usability and cost over security, resulting in persistent weaknesses such as default credentials, insufficient firmware updates, and inadequate encryption. External adversaries exploit these gaps through tactics including distributed denial-of-service attacks, unauthorized access, data manipulation, and cyber-espionage, often leveraging botnets comprising compromised IoT nodes. Internal threats, whether from malicious insiders or inadvertent misconfigurations, further complicate defense efforts by facilitating lateral movement within networks and undermining trust in system integrity. The convergence of cyber and physical domains magnifies the potential impact of attacks, as disruptions in digital layers can cascade into physical operational failures with severe safety and economic consequences. The economic ramifications extend

beyond immediate remediation costs to include reputational damage, regulatory penalties, and long-term degradation of system performance.

Cascading failures across interconnected infrastructure sectors underscore the systemic risks posed by insecure IoT deployments. Addressing these challenges necessitates a comprehensive approach that combines technical safeguards, such as encryption by default, anomaly detection, and secure key management, with adaptive governance frameworks capable of aligning policy with technological advancements.

National cybersecurity strategies must integrate multi-stakeholder collaboration, international cooperation, and sector-specific considerations to build resilience and ensure the continuity of essential services. Furthermore, the dynamic nature of IoT ecosystems demands continuous monitoring and incident response capabilities that can promptly detect and mitigate emerging threats. Machine learning and artificial intelligence offer promising avenues for enhancing threat detection, though their effectiveness heavily relies on the quality of training data and the ability to counter adversarial manipulation.

Regulatory frameworks should balance security requirements with innovation incentives, ensuring that minimum-security standards are met without stifling technological progress. Ultimately, safeguarding IoT-enabled critical infrastructures is a complex endeavor that intersects technical, organizational, legal, and socio-economic dimensions. Success depends on recognizing the interdependence of external and internal threat vectors and implementing layered defenses that address vulnerabilities across device lifecycles and network architectures. By embedding privacy and security considerations into the foundational design and operational phases, states can better protect national interests, maintain public trust, and harness the benefits of connected technologies without compromising resilience or safety.

REFERENCES

Ahmed, M. F., Molla, A. H., Uddin, M. R., & Chowdhury, T. R. (2023). Advancing cyber resilience: Bridging the divide between cyber security and cyber defense. International Journal for Multidisciplinary Research (IJFMR), 5(6), 1. http://www.ijfmr.com

Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security.

Amro, A. (2024). IoT vulnerability scanning: A state of the art.

Ani, U. D., Watson, J. D. McK., Nurse, J. R. C., Cook, A., & Maple, C. (2019). A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape.

Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 8, 3559–3591. https://doi.org/10.1007/s40747-022-00667-z

Aufner, P. (2020). The IoT security gap: A look down into the valley between threat models and their implementation. International Journal of Information Security, 19(1), 3–14. https://doi.org/10.1007/s10207-019-00445-y

Budiman, I. (2022). National cyber defense of the indonesian government in protecting the society. MANDALA: Jurnal Ilmu Hubungan Interna Sional, 5(2), 231.

Buiya, M. R., Laskar, A. K. M. N., Islam, M. R., Shil, S. K., Chowdhury, M. S. R., Shawon, R. E. R., & Sumsuzoha, M. (2024). Detecting IoT cyberattacks: Advanced machine learning models for enhanced security in network traffic. Journal of Computer Science and Technology Studies, 6(4), 142. https://doi.org/10.32996/jcsts.2024.6.4.16

Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 35.

El-Sofany, H., El-Seoud, S. A., Karam, O. H., & Bouallegue, B. (2024). Using machine learning algorithms to enhance IoT system security. Scientific Reports, 14, 12077. https://doi.org/10.1038/s41598-024-62861-y

Garcia-Morchon, O., Kumar, S., & Sethi, M. (2019). Internet of things (IoT) security: State of the art and challenges. In Internet Research Task Force (IRTF) Request for Comments (8576; p. 1).

Group, I. I. C. S. W. (2018). Interagency report on the status of international cybersecurity standardization for the internet of things (IoT). https://doi.org/10.6028/NIST.IR.8200

Hadi, Q. A., Alfoudi, A. S., & Mahdi, A. M. (2023). IoT cybersecurity threats and detection mechanisms: A review. Wasit Journal for Pure Sciences, 2(2), 231.

Kudini, A. A. (2024). Internet of things based data integration ontology in cyber security. International Journal of Engineering Research and Applications, 14(11), 01–04. https://doi.org/10.9790/9622-14110104

Mohamed, N., Oubelaid, A., & Almazrouei, S. K. (2023). Staying ahead of threats: A review of AI and cyber security in power generation and distribution. International Journal of Electrical and Electronics Research (IJ EER), 11(1), 143–147. https://doi.org/10.37391/IJEER.110120

Oredola, C., & Ashraf, A. (2024). A systematic mapping study on SDN controllers for enhancing security in IoT networks. https://arxiv.org/abs/2408.01303v1

P0̈103tra0̈219cu, P. (2021). EMERGING TECHNOLOGIES AND NATIONAL SECURITY: THE IMPACT OF IoT IN CRITICAL INFRASTRUCTURES PROTECTION AND DEFENCE SECTOR. Land Forces Academy Review, XXVI(4(104)), 423. https://doi.org/10.2478/raft-2021-0055

Petrişor, P. (2021). Emerging technologies and national security: The impact of IoT in critical infrastructures protection and defence sector. Land Forces Academy Review, XXVI(4(104)), 423. https://doi.org/10.2478/raft-2021-0055

Rizky, R., Samuel, L. T. T., Handayani, K. S. N., & Zakky, A. H. (2023). Analysis of presidential regulations concerning cyber security to bolster defense policy management. Defense and Security Studies, 4, 84–93. https://doi.org/10.37868/dss.v4.id244

Schaberreiter, T., Röning, J., Quirchmayr, G., Kupfersberger, V., Wills, C., Bregonzio, M., Koumpis, A., Sales, J. E., Vasiliu, L., Gammelgaard, K., Papanikolaou, A., Rantos, K., & Spyros, A. A cybersecurity situational awareness and information-sharing solution for local public administrations based on advanced big data analysis: The CS-AWARE project.

Voronko, I. (2024). The security of IoT systems in railway transport. Transport Systems and Technologies, 4(3), 90. https://doi.org/10.32703/2617-9059-2024-43-7

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

DOG WHISTLES AND CAT SENSES – HIDDEN EXTREMISM AND THE FRAMEWORK OF LEGAL OVERSIGHT IN EUROPEAN COURT OF HUMAN RIGHTS CASE LAW

Vasil Georgiev
National Security and Public Order
Higher School of Security and Economics
https://orcid.org/0000-0003-4246-0622
v.georgiev@vusibg

Abstract. *This paper examines the challenges posed by hidden extremist messages communicated through coded language, memes, irony, and discursively veiled expressions within the framework of the European Court of Human Rights' (ECtHR) case law. It develops a methodological framework for assessing such speech, drawing on discourse analysis, speech act theory, and the concept of "dog whistle" communication. Through an analysis of ECtHR and selected national decisions, the study highlights the tension between safeguarding freedom of expression under Article 10 of the European Convention on Human Rights and addressing disguised incitement to hatred or violence. It argues that courts must adapt their interpretative tools to account for the evolving forms of extremist rhetoric in digital environments, where messages often operate simultaneously on multiple semantic levels.*

Keywords: Hidden extremism; Dog whistle communication; ECtHR case law; Freedom of expression.

1. INTRODUCTION

The entry of social networks, image boards, forums and other forms of online communication into political discourse has led to the formation of online communities using their own language, memes, symbols, inside jokes, audiovisual forms, narratives, stories that serve to communicate and identify these communities, as well as to disseminate their ideas.

The use of such coded messages is common phenomenon for closed groups. As in the past, so today, specific languages are also used by different professional groups. Also, criminal groups use specific jargons (Koskensalo, 2015, p. 499), which do not allow law enforcement agencies to understand the plans and activities of the criminal group.

This type of coded communication is now widely used by radical and extremist groups (Koskensalo 2015, p. 501). In addition to preventing incrimination (Åkerlund (2022, p.1822), the use of coded messages also achieves three additional goals:

– as a means of both intra-group recognition and public self-identification for group members (signaling that the speaker is "in the club") (Weimann, 2020, p. 20);

- attracting new followers (cryptic speech requires a certain intellectual effort from the listener, which is rewarded with obtaining membership in the community);

- it is a means of circumventing platforms' algorithms that remove illegal content;

This explains why, in the present context, extremist messages are more likely to disguise their intent rather than openly call for violence. However, this shift does not necessarily indicate a moderation of political views; rather, it reflects a deliberate strategy to gain broader support while avoiding legal repercussions. The messages are carefully framed in coded and legally permissible expressions, often embedded in memes and other forms of public discourse, both oral and written. As a result, the speech exerts a strong influence on the targeted group, while the wider audience perceives it as neutral or harmless.

Thus, extremist messages function in parallel in two discourses, which creates their semantic duality – the hidden inter-extremist discourse. and the wider public discourse. The hidden meaning is a discursive

tool that can remain invisible to the courts and law enforcement agencies. The latter, as citizens, most often participate in public discourse, which determines their tendency to be neutral towards hidden extremist messages.

2. PURPOSE OF THE STUDY

This study aims to present a conceptual framework for the assessment by the Court of Human Rights, of hidden extremist messages when they are realized through coded, visual or discursively veiled speech (so-called dog whistle messages).

The proposed framework is based on the case law of the Court of Human Rights, which has a leading role in defining the boundaries of permissible speech in Europe (for the member states of the Council of Europe), as it forms the minimum standards binding on these states.

Given the dynamic development of channels of expression in recent years, there is a lack of case law of the Court of Human Rights on newer forms of veiled or coded extremist speech – such as internet memes, ironic slogans and other audiovisual forms. This necessitates the report to also analyse selected decisions of national courts in Europe that have decided cases related to digital hate speech.

3. NORMATIVE FRAMEWORK THE PROTECTION OF FREEDOM OF EXPRESSION IN THE ECHR

Article 10, paragraph 1 from The European Convention on Human Rights guarantees the law on free expression - freedom of opinion and freedom to receive and distribute information and ideas without interference by public authorities.

Outside the scope of Art. 10, paragraph 1 ECHR is speech inciting to violence, hate speech and racism, as well as Holocaust denial (Bychawska-Siniarska, 2017, p. 23-31). This is so insofar as Art. 17 ECHR prohibits abuse of rights by excluding from the protection of Art. 10 expressions that undermine the fundamental values of the Convention. The Court of Human Rights has applied this provision to deny protection to speech inciting to violence, hate speech, racism or Holocaust denial.

In addition, Article 10, paragraph 2, provides for the possibility for Council of Europe member states to restrict the right to protected speech if the following conditions are met:

a. the restriction is provided for by law.
b. the restriction must have a legitimate aim, it shall be provided “in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary” (Art.10, par.2).
c. interference is necessary in a democratic society, that is.

- to be proportionate i.e. proportionate to the objective pursued.
- to respond to a pressing social need i.e. there must be a social need to impose the restriction.

The ECHR admits on the national authority’s freedom on judgment (so-called margin of appreciation) at imposing restrictions on the law based on Article 10, paragraph 2 of the Convention. This means that the countries have the competence to evaluate the specifics on the given case according to the existing social, historical and political context. This assessment is not entirely within the discretion of the State, since it is for the Court to assess whether it is complied with the standard "necessary in the democratically society".

In contrast to the European legal framework, in the United States the First Amendment to the Constitution guarantees almost full protection of speech unless it meets the strictly defined test of "incitement to immediate unlawful action" (US Supreme Court, Brandenburg v. Ohio (1969)). Any other expression, including that which in Europe would be qualified as hateful or inflammatory, is considered protected by the First Amendment in the United States (US Supreme Court, Chaplinsky v. New Hampshire (1942), Virginia v. Black (2003), RAV v. City of St. Paul (1992)).

ISSN 2815-3324 Online, ISSN 2535-0358 Print

4. THEORETICAL FRAMEWORK FOR SPEECH CONTENT ASSESSMENT

4.1. Speech Act Theory

The ECtHR's case law on the assessment of freedom of expression (Article 10, paragraph 1 of the ECHR), the limits that states may place on this freedom (Article 10, paragraph 2) and the application of Article 17 is influenced by the speech act theory and by various approaches to discourse analysis. (including critical discourse analysis (Åkerlund 2022), semiotic analysis (Pratiwi, D. P. E., Sulatra, I. K., & Dewangga, I. G. A. (2023).

These analytical frameworks help to the evaluation not only of the explicit content of the expression but also its implied meanings, context, and potential impact. Speech act theory and methods of discourse analysis reveal the hidden extremist messages that are most popularly known today as 'dog whistles' a notion popularized by the American legal scholar Ian Haney López (López , 2014).

Speech act theories (speech as action) originated in the 1950s and explain speech not only as a statement or description, but also as an action (Austin, 1962). John Austin calls act-sentences "performative expressions" and identifies the characteristics for an expression to have performative meaning (Austin, 1962, p.15). A performative expression is valid (i.e., represents a relevant action) depending on:

a. whether the author is legitimate to utter it and they did follow the normative procedure (if any). For example, the same expression uttered by three different people - a politician, an actor or a person who ridicules the expression, may or may not have a performative effect. While the speech of the ridiculer has a parodic or ironic character, that of a politician - under valid conditions - can be perceived as a form of incitement. The speech of the actor should in principle have an interpretative character, but under certain conditions it can also be performative.
b. whether the expression is said sincerely (what is the speaker's intention) – that is, is there a match between the person's will and their statement. Such a match will not be present if, for example, what was said was said in joke, was given as a (teaching) example, or was uttered within the framework of an actor's interpretation of a work.
c. the existing context – including the set of external factors that give meaning to what is said, since speech does not exist on its own, it is a response or provocateur to certain conditions.
d. from the audience - to whom the speech is addressed.
e. and if relevance requires – in the presence of additional statements and assumptions.

All of these premises, with some extrapolation, are methodologically applicable to the assessment of extremist speech.

John Searle introduced the concept of an "illocutive act" (Searle, 1969,13) – a speech act through which the speaker achieves social impact, expressing an intention in a specific communicative context. In discursive theory, this act does not exist in isolation, but fits into a broader system of meanings, where meaning is formed by the interaction between the speaker, the audience, the context and established social roles. It is this discursive engagement that gives legal significance to speech and allows the court or security authorities to assess not only what is said, but also its mobilizing, radicalizing or coded function.

This perspective is complemented by Michel Foucault's concept of discourse (Foucault, 1972, Foucault, 1981), according to which statements do not exist in a vacuum but are part of broader systems of knowledge and power that determine who can speak, what can be said and in what context. Therefore, extremist rhetoric should be considered not only at the level of the immediate interaction between speaker and listener, but also as an element of already established discursive formations. Within these formations, extremists resort to coded expressions, memes and "dog whistle" rhetoric, which allow them to disguise their messages, which receive a seeming legitimacy insofar as they appear to be expressed within the boundaries of legitimate public discourse.

2. Dog Whistle and The Discourse

The dog whistle is used by the owner and is only heard by the dog, as its sound is in the high frequency range, inaudible to human hearing. This way, the message is clear to the addressee but remains hidden from the audience.

The dog whistle can be understood as a speech act that activates pre-shared meanings within a specific audience, while remaining unrecognizable to the general public. The concept of the dog whistle is a manifestation of Michel Foucault's idea of discourse as a mechanism for maintaining power through control over meaning and access to it. For example, the slogan "Let's defend the family" operates on two levels. To the general public, it sounds like an acceptable message about traditional values. However, within the framework of far-right discourse, the same phrase has a hidden meaning – opposition to the LGBTQ+ community and migrants, presented as a "threat" to society. It is this ambiguity and selective intelligibility that illustrates Foucault's understanding that discourse controls access to knowledge: some hear a simple appeal, while others hear a coded extremist message.

Messages of this type contain a conscious and purposeful ambiguity of speech. For example, it is possible for an actor's speech to simultaneously inhabit two realities – performative and non-performative. A monologue inviting war can be perceived both as a performance and as a call (if the prerequisites for a valid performative are present – the actor has a public position, utters the monologue out of conviction, and the context includes deteriorated international relations, the audience is made up of nationalistic people and, accordingly, can be provoked to action).

This duality of the speech act, visible to some, invisible to others, is aptly described by China Miéville in her novel The City and the City. It tells the story of two cities – Beshel and Ul Kama – that share the same space, but the inhabitants are trained not to see the other city, even when they pass by people and buildings from it. This metaphor of the social division is useful for understanding the "dog whistle" effect.

John Searle justifies this possibility (Searle, 1969, p.26), pointing out that this is precisely the main characteristic of hidden speech – its simultaneous belonging to performative (mobilizing) and constative (descriptive) discourse. Like the cities of Bechel and Ul Kama in Miéville's novel, the message is visible to some and invisible to others, heard by some and unheard by others – perceived as normal political rhetoric by some, but as a call to violence by others. This ambiguity significantly complicates the courts and institutions, as it calls into question whether the expression is part of legitimate political debate or constitutes a disguised hate speech or incitement to violence.

These concepts of speech justify the need for a discursive analysis of speech that reveals the actual meaning, intention and potential effect. The task of the court is to recognize "dog whistle" communication as a discursive element that – under certain circumstances – contributes to the escalation of hatred and hostility.

The court's assessment of discursive determinacy is very important because, although extremist speech is primarily subject to moderation by algorithms (which at this point lack discursive sensitivity, leading to the removal of legitimate content (overblocking) and unreasonably narrowing the right to expression), it is the court, not the algorithm, that shall be legitimately obligated to outline the boundaries of a human right.

The incorrect definition of discourse leads to the danger that messages that do not carry illegality could be incorrectly qualified as such and thus the exercise of a fundamental human right, such as freedom of expression, will be restricted.

All this necessitates clarifying the problem of discourse within the framework of extremist messages. The ECtHR has serious practice in this direction, it takes into account discourse, but on the other hand, it was formed mainly before the emergence of communications through social networks and image boards. Considering that social networks and image boards are the main channels for the dissemination of extremist views, it is necessary to apply the existing principles to this type of communication, considering the specifics of the latter.

The present study is limited mainly to manifestations of right-wing extremism, as right-wing extremists use similar political and linguistic tools in propagating their ideas. Although the study focuses on covert extremist messages (typical of the far-right, who wish to present their ideology as mainstream

and their lifestyle as cool) (Ebner, 2020, p. 153), it examines the judicial practice of overt extremist messages, insofar as the latter represent the typical case of judicial assessment of extremist speech, but the developed practice is partly directly, partly correspondingly applicable to covert extremist messages.

5. CASE LAW FRAMEWORK

The ECtHR has long recognised that speech operates within a particular discursive environment, which is relevant to the assessment of a particular expression. Therefore, in analysing messages with the potential to incite hatred, it is essential to consider who is speaking, to whom, in what context and what effect their speech may have.

According to the Court's case-law, restrictions on freedom of speech are permissible if there are compelling reasons (Féret v. Belgium, 2009, § 63) and with proportionate measures (Féret v. Belgium, 2009, § 64) – that is, this restriction cannot be applied to every speech, even if it contains a radical or provocative meaning.

5.1. The personality (immage) of the speaker

In assessing the illegality of an expression, the personality of the speaker is relevant to the court's judgment. In social sciences, personality immage can be viewed as a social construct that is formed by the way others perceive an individual. The image of the individual is built because of the impressions of others about her/his acts.

What the speaker says is not perceived in isolation, but in the context of what she/he has said or done before and what her/his intention is. The meaning of his expression is derived from the constructed discursive profile of that person. For example, when the statement is made by a public figure – a politician (Necmettin Erbakan, former Prime Minister of Turkey, Erbakan v Turkey, 2006, §76, 80), leader of a far-right party (Feret vs Belgium, 2009), comedian (Dieudonné M'Bala M'Bala, famous French comedian, M'Bala M'Bala vs France, 2015), prominent footballer (Josip Simunić, Croatian national team player, Simunic vs Croatia, 2018, § 45) the court accepts that their social status and public image influence the perception of the message by the audience. This also leads to a change in the legal assessment of the expression and in these specific cases the court accepts that the sanctions imposed by the national jurisdictions on these individuals do not contradict Article 10 of the ECHR.

The public role alone is not sufficient to accept that an expression is unlawful. This is stated in the decision in the case Perinçek v. Switzerland (2015), which found that the denial of the 1916 Armenian genocide by the leader of the Turkish Workers' Party, Doğu Perinçek, did not automatically constitute incitement to hatred, absent additional indicators such as a call for violence or a real public risk that the provocative statement would lead to an escalation of public tension.

The public perception of a person as radical may in certain cases even lead to an adverse legal assessment of their statements. In §51 of the judgment in the case of Gündüz v. Turkey (2003), the ECtHR noted that the applicant’s statements must be viewed in the light of his public role and prominence as the leader of a religious group whose radical ideology is well known. Because of this, his speech had a more limited impact, as the audience perceived his words in the context of his already known radical views, which reduced the risk of his speech being perceived as incitement.

5.2. Sincerity (the author's intention)

All the world's a stage, and all the men and women merely players. Yuval Harari points out that the main difference between humans and other animals is that we believe in fictional stories (Harari, 2015, p. 27-28). Fictional stories have a huge impact on shaping our society, norms, experience and worldview. Within this, aesthetically we often enjoy violence, victory over the opponent and humor. A large part of show business, culture and sports are built on these preferences of ours.

The law does not prohibit such content – their meaning is interpreted in an aesthetic or fictional context, which usually excludes a performative (i.e., effective) function of speech. The sincerity, or more

precisely the intention of the speaker, is also important. A typical example is acting – within a fictional context, the insincerity of the actor is assumed – she/he will not be tried for incitement to violence or hatred if he plays the role of a war provocateur.

Here the question arises: to what extent does the actor express herself/himself and to what extent does she/he play the role? There are different types of acting and different relationships between the actor and the character. At what point does the actor cease to be an interpreter and become an author? This can be said with even greater force for the author of a novel – are the thoughts and characters an extension of the author's personality, or has the author consciously severed her/his connection with them?

No less important are the issues related to jokes and anecdotes. Despite some objections to inappropriate humor, it is not prohibited. In the case of Simić v. Bosnia and Herzegovina (2020), Bosnian lawyer Marko Simić was convicted of contempt of court for telling the famous joke in which the professor asked the student to list the names of the victims of the Hiroshima atomic bomb. The ECtHR found that in this case there was a violation of Simić's right under Art. 10 of the Convention – i.e. it accepted that this joke was permitted speech that did not constitute an insult in the context of the protected freedom of expression.

However, similar protection was denied to comedian Dieudonné M'bala M'bala vs France (Dieudonné M'bala M'bala vs France, 2015), for a humorous sketch in which an actor wearing striped pajamas and a yellow Star of David with the inscription "Jew" presented an "Oscar" to the famous Holocaust denier in France, Robert Faurisson. In this case, the ECtHR found that the action exceeded the limits of humor and fell within the scope of Art. 17 of the ECHR (abuse of rights), and therefore was not subject to protection.

The issue of sincerity and humor is of great importance in the context of extremist speech, given that far-right communication and propaganda include humor, irony, and ambiguity as their main weapons. Jokes often serve as a defense mechanism, a "loophole" through which authors can invoke a frivolous tone when held accountable. This requires a more careful judicial assessment of the context, the audience, and the possible perlocutionary effect – regardless of the outward comedic or ironic style of the speech.

The issue of intent is particularly well developed in American jurisprudence, as it is key in distinguishing protected from unprotected speech. For example, American law distinguishes the burning of a cross without the intention to intimidate someone from the burning of a cross that threatens (Virginia v. Black, 538 US 343 (2003). The law in the member states of the Council of Europe would not be so sensitive to a specific symbolic act in this case – it would be protected mainly if it is given as an example or is part of a work of art.

5.3. The audience

Next, according to the method of discourse analysis, the meaning of a message is influenced by the audience to which the message is addressed. The meaning of the message can be clarified by how the relevant social group perceives and interprets it (M'bala M'bala vs France, 2015, § 35, Šimunić vs Croatia, 2018 § 45).

In dog whistle speech, the message, although formally a single speech act, is deliberately structured in such a way as to produce different semantic effects in different audiences. Such a two-level perception of speech was examined in the case of Šimunić v. Croatia, in which the Court analyzed the double discourse embedded in the slogan used – officially presented as historical or patriotic, but with a clearly recognizable meaning in an extreme nationalist context.

The Court accepts that the phrase "For Home" which Croatian national football player Josip Simunić uttered three times to the crowd in 2013 after a football match that qualified Croatia for the World Cup, was also used as an official greeting during the Ushashi regime (1941-45) in the Independent State of Croatia. (Šimunić v. Croatia, 2018 § 44). Thus, although at first glance the expression may seem permissible, its discursive attachment to a specific ideology, as well as the effect on the audience – Croatian football fans, make it incompatible with the standards of Article 10 ECHR.

It should be borne in mind that a significant proportion of the expressions not protected under Article 10 of the ECHR are used in the context of intra-organisational communication between already radicalised individuals. This type of speech usually remains hidden from the public and is therefore rarely subject to

judicial review. It would be wrong to consider that the impact of intra-organisational speech is limited, insofar as it is at this stage that newly recruited or hesitant individuals come into contact with extremist content — as part of the process of selection, socialization, and ideological indoctrination.

5. 4. The context

The meaning of an expression is also shaped by the social and communicative context in which it is uttered – what, when, where, to whom and how (Lingens vs. Austria, 2008 § 40, Leroy vs. France, 2008, § 32, Sürek vs. Turkey (No. 3), 2009, § 40).

Communication on image boards like 4chan, section /pol/ is the most diverse in context - it includes personal, everyday, political, ethnic, historical, ironic sexual and other topics.

This does not mean that an extremist message cannot appear within a seemingly innocuous context. For example, the statement "Today, 44 veterans in America commit suicide every day out of despair. Imagine what would be achieved if half of them, instead of committing suicide, killed our enemies " (quote from a post by 4chan) would be perceived in Europe in any context as hate speech or even incitement to violence.

In contrast, ambivalent expressions, symbols, and slogans such as Z, 14/88, white advocacy, race realism like most internet memes, get their meaning largely from the context. The same expression can be perceived as irony, a political message, or hidden extremist incitement.

A statement denying the 1916 Armenian genocide, if it does not contain incitement to violence and is made in a context free from immediate ethnic tension, is admissible (the decision was not unanimous) (Perinchek v Switzerland, § 158). The Court recognises the importance of the issue for the Armenian community and that the statements affect their dignity (Article 8 of the Convention), but considers the following: the applicant's words do not contain incitement to hatred or violence, they were made in a context free from immediate ethnic tension.

In the case Sürek v. Turkey (No. 1), § 62, the Court stressed the importance of the context in which the impugned letters were published in the newspaper. Expressions such as "fascist Turkish army", "murder gang" and "hire assassins of imperialism" were assessed as stigmatising and inciting revenge, fuelling hatred and posing a risk in the context of a protracted conflict with a high level of violence in south-eastern Turkey. In that context, the Court found the interference with freedom of expression to be justified, as it amounted to hate speech and glorification of violence. The Court considered that the speech was directed at a real action, it has the purpose of activating (it is performative), its restriction by the state is permissible within the meaning of Art. 10, par. 2.

In Feret v Belgium (paragraph 76) the Court emphasised the importance of the environment and context in which the speech was disseminated – an election campaign aimed at the entire population. While political parties enjoy broad freedom of expression in elections, in such a context racist and xenophobic rhetoric has a particularly strong and harmful effect, as it reinforces slogans at the expense of reasonable debate and undermines public order.

In the case of Norwood vs. United Kingdom (2004) Roger Norwood, a member of the British National Party, put up a large poster in the window of his home with the words "Islam out of Britain – Protect the British People", accompanied by an image of the Twin Towers in flames after the September 11 attacks. The court concluded that the context – in the days immediately following September 11, 2001 – was decisive in concluding that this was not a political debate but incitement to hatred, excluded from the protection of Article 10.

In its decision in the case of Leroy v. France, 2008 cartoonist Denis Leroy was convicted of publishing a cartoon praising the September 11, 2001 attacks, just two days after they occurred. The ECtHR held that the context of high tension and emotion immediately following the attacks justified the State's intervention and that the conviction did not violate Article 10 of the ECHR, as the restriction was "necessary in a democratic society".

Importantly, in relation to internet communication, as stated in §51 of Gündüz v. Turkey, the ECtHR emphasized that the applicant's statement was made in the context of a television programme where there was an open debate with opposing views. This context of pluralistic dialogue and counter-positions is

important as it limits the possibility of the speech being perceived as inflammatory – it is part of a clash of ideas, not a one-sided suggestion. Applied to internet communication, this reduces the state's ability to restrict opinions, even extremist ones, that are expressed within the framework of a discussion.

5.5. The effect (the potentially harmful consequences)

The effect that the message produces is also relevant (see Sürek v. Turkey (No. 3) § 40).

The potentially harmful consequences could be different. They could be in the potential to lead to violence – in incitement to violence. In hate speech, the potentially harmful consequences are of two types – the individual harm to a member of society belonging to a discriminated group and the creation, maintenance or escalation of a climate of hatred towards a particular group.

In Gündüz v. Turkey, par. 51, The court held that an opinion challenging democracy and advocating the introduction of Sharia law is protected by Article 10 of the ECHR, as it does not contain a direct call for the forcible establishment of Sharia law, despite the fact that it concerns provocative and radical statements.

However, the interpretation of the effect that a statement may have allows the court to rely on a fact that is more often presumed than actual.

The review of the selected case law shows that the court is sensitive to the issue of the discursive specificity of speech, which gives it a wide scope for assessment that is not based solely on the isolated interpretation of the individual expression.

6. THE MEMES

The issue with memes is more complicated, since their meaning cannot always be determined. It is often determined by a certain discursive history, which cannot always be traced precisely. Often it is a question of repeatedly reformulated symbols, which are incomprehensible to an outside observer, but for the "initiated" carry a strong political or ideological message.

Memes are carriers of information and ideas. Memes can express simple ideas, they are propaganda, communication, entertainment and therefore image tool (we are not that scary). It is this playful and ironic packaging that makes memes more ambivalent and more difficult to legally qualify than written or spoken speech.

Criminalizing the posting of memes would put extremists in the position of "victims of censorship," which could become part of their radical propaganda.

Discursive logic leads to the danger of a very broad possibility of interpretation, without the court's assessment of the presence of a perlocutionary (influential) effect of speech being subject to real control.

This issue is also reflected in one of the first cases in Europe in which a court verdict was issued for publishing a meme – the case of a Belgian citizen convicted of uploading an image with content inciting hostility towards a certain ethno-religious group (Rechtbank van eerste aanleg Antwerpen). In this case, it is about unequivocal incitement to hatred, not veiled or ambiguous incitement. However, the court justified its decision (and rejected the defendant’s objection to the use of sarcasm) with the reactions of the targeted audience to her post on social network.

This decision is important both from the perspective of being one of the first to incriminate memes, and in recognizing the discursive approach to assessing hate speech.

6.1 Limitations in the legal recognition of hidden extremist messages

The above leads to the conclusion that the Court of Human Rights has built an appropriate methodological framework for assessing extremist speech. This does not mean that there are no legal and institutional obstacles. They are largely inherent in judicial bodies and are not specific to the Court of Human Rights alone. They can be defined as follows:

1. Difficulty in recognition by the court

ISSN 2815-3324 Online, ISSN 2535-0358 Print

Courts are not always sensitive to coded extremist messages. The principle of the court's internal conviction to some extent forces the court to judge its interpretation of the message as valid. As a result, the effect of the message on its actual addresses is neglected. Thus, some messages are perceived as acceptable opinions, although they have an inciting effect for certain groups.

2. Preference for "cleaner" and easily provable cases

The prosecutor's office, human rights organizations and other entities authorized to initiate proceedings often avoid borderline cases in which there is no direct violence or insult.

This is due primarily to the difficulties in proving and substantiating the procedural position in such a process. Proving a covert case of extremist propaganda requires serious linguistic knowledge, knowledge of the environment – the target of the message and is much more laborious, and the outcome of the case is unclear. Substantiating a procedural position for which there is no analogous previous case law creates uncertainty for the potential initiating party about the outcome of the process.

Similarly, in most European judicial systems there are mechanisms for evaluating the work of judges and prosecutors, on which their professional growth depends. In them, the number/percentage of overturned decisions by the higher instance, or lost cases, is a valid criterion for evaluating the work of the judge. The possibility that a decision may negatively affect the professional development of the judge also hinders the bolder entry of law into more ambiguous territories of speech.

In addition to the above, if the claim is rejected, there will be a negative public response to institutions, and extremists become the victims, the unjustly repressed, and the human rights institution or organization - a dark-hearted persecutor of freedom of speech. Putting themselves in the position of victims is often part of the extremists' strategy.

3. Unwillingness to narrow the boundaries of freedom of expression Freedom of expression is protected by Article 10 of the ECHR, with its limitations provided for in Art. 10, paragraph 2 A decision that expands the unlawful use of speech is perceived negatively, especially when it concerns a controversial case.
4. The significant differences between the USA and Europe, especially with regard to hate speech. As we have pointed out, in the USA the First Amendment guarantees almost unlimited freedom of speech. In the case law of the ECtHR, freedom of expression under Article 10 ECHR is subject to restrictions when speech threatens the rights of others or the democratic order (see Article 10, §2 and Article 17 of the Convention). This makes it possible to sanction expressions with a latent extremist charge, including when they are dressed in language that at first glance seems legally permissible.

European audiences are increasingly influenced by extremist messages published by American citizens on platforms such as 4chan, Reddit, Gab, X (Twitter), etc., which operate under US jurisdiction and therefore do not remove content that would be banned in Europe. This cross-border difference in standards creates real difficulties in intercepting online hate speech, especially in cases of coded, memetic or ironically presented hostility (including "dog whistle" rhetoric).

5. Shifting responsibility to the algorithms in the platforms. Due to the huge volume of expressions on the Internet, there is a widespread opinion that the court does not have the opportunity to deal with the Internet, and content moderation is the job of social networks. As I indicated above, automatic content removal is the second-best solution in this case, because it cannot perform a legitimate assessment of the content of a message and, accordingly, may be activated when it is not necessary, but not activated when it is necessary.

However, platforms as a mechanism for self-regulation also have some positive sides: they can react quickly and at scale, limiting the spread of harmful content even before the courts intervene; they have the flexibility to implement various measures such as marking or limiting visibility, which allows for preventive intervention without a complete ban; and they often involve representatives of academia, human rights organizations and journalist associations in the development of rules, which gives greater legitimacy to the process.

6. CONCLUSION

The ECtHR has developed a suitable methodological toolkit for assessing whether an expression falls within the permissible interference of the state or not. This works relatively well in clear cases where someone openly calls for violence. or instills hatred.

However, the use of code words, memes, images or jokes that say different things to different audiences often go unnoticed because they do not sound aggressive to someone outside the group. Here, courts need to be more careful and expand the way they assess speech. The available methodological toolkit (assessing: author, intention, audience, context and effect of the speech) could be used admirably to carry out such an assessment.

However, there is also the practical problem that in the age of the Internet, almost every online statement is practically public. This is extremely burdensome for the court. No less important is the fact that the court and the prosecutor's office do not always have an incentive to deal with such complex and unclear cases. Thus, many messages go "under the radar" - precisely those that are best hidden and most difficult to prove.

REFERENCES

Åkerlund, M. (2022). Dog whistling far-right code words: The case of 'culture enricher' on the Swedish web. *Information, Communication & Society*, *25*(12), 1808–1825. https://doi.org/10.1080/1369118X.2021.1889639

Austin, J. L. (1962). *How to do things with words*. Oxford University Press.

Brandenburg v. Ohio, 395 U.S. 444 (1969).

Bychawska-Siniarska, D. (2017). *Protecting the right to freedom of expression under the European Convention on Human Rights*. Council of Europe.

Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).

Dieudonné M'Bala M'Bala v. France, no. 25239/13, Eur. Ct. H.R. (2015).

Drongal, A. M. (2020). "Hate speech" and the right to freedom of expression: A ratio and the criteria of differentiation in the context of the decisions of the ECHR. *UDC 341.6*.

Ebner, J. (2020). *Going dark: The secret social lives of extremists*. Bloomsbury Publishing.

Erbakan v. Turkey, no. 59405/00, Eur. Ct. H.R. (2006).

Féret v. Belgium, no. 15615/07, Eur. Ct. H.R. (2009).

Foucault, M. (1972). *The archaeology of knowledge* (A. M. Sheridan Smith, Trans.). Pantheon Books.

Foucault, M. (1981). The order of discourse. In R. Young (Ed.), *Untying the text: A post-structuralist reader* (pp. 48–78). Routledge & Kegan Paul.

Garaudy v. France (dec.), no. 65831/01, Eur. Ct. H.R. (2003-IX).

Gündüz v. Turkey, no. 35071/97, Eur. Ct. H.R. (2003-XI).

Handyside v. United Kingdom, no. 5493/72, Eur. Ct. H.R. (1976).

Harari, Y. N. (2014). *Sapiens: A brief history of humankind*. Harper.

Jersild v. Denmark, no. 15890/89, Eur. Ct. H.R. (1994).

Koskensalo, A. (2015). Secret language use of criminals: Their implications to legislative institutions, police, and public social practices. *Sino-US English Teaching*, *12*(7), 497–509. https://doi.org/10.17265/1539-8072/2015.07.005

Lehideux and Isorni v. France, no. 24662/94, Eur. Ct. H.R. (1998-VII).

Leroy v. France, no. 36109/03, Eur. Ct. H.R. (2008).

Lopez, I. H. (2014). *Dog whistle politics: How coded racial appeals have reinvented racism and wrecked the middle class*. Oxford University Press.

M'Bala M'Bala v. France, no. 25239/13, Eur. Ct. H.R. (2015).

MJ Moody v. NetChoice, LLC, 142 S. Ct. 2412 (U.S. 2022).

Norwood v. the United Kingdom (dec.), no. 23131/03, Eur. Ct. H.R. (2004-XI).

Perinçek v. Switzerland [GC], no. 27510/08, Eur. Ct. H.R. (2015).

Pratiwi, D. P. E., Sulatra, I. K., & Dewangga, I. G. A. (2023). Deconstructing internet memes through semiotic analysis: Unveiling myths and ideologies in visual and verbal signs. *Jurnal Arbitrer*, *10*(1), 147–157. https://doi.org/10.25077/ar.9.2.147-157.2022

R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).

Rechtbank van eerste aanleg Antwerpen, afdeling Turnhout. (2021, October 11). Eerste veroordeling in België voor haatzaaiende memes [First conviction in Belgium for hateful memes]. (C.19.1528.N).

Saygılı and Falakaoğlu v. Turkey, no. 39457/03, Eur. Ct. H.R. (2008).

Searle, J. R. (1969). *Speech acts: An essay in the philosophy of language*. Cambridge University Press.

Simić v. Bosnia and Herzegovina, no. 39764/20, Eur. Ct. H.R. (2020).

Simunic v. Croatia (dec.), no. 20373/17, Eur. Ct. H.R. (2018).

Sokolovskiy v. Russia, no. 67029/19, Eur. Ct. H.R. (2024).

Sürek v. Turkey (No. 1), no. 26682/95, Eur. Ct. H.R. (1999-IV).

Sürek v. Turkey (No. 3), no. 24735/94, Eur. Ct. H.R. (1999).

Virginia v. Black, 538 U.S. 343 (2003).

Weimann, G., & Am, A. B. (2020). Digital dog whistles: The new online language of extremism. *International Journal of Security Studies*, *2*(1), Article 4. https://digitalcommons.northgeorgia.edu/ijoss/vol2/iss1/4