*Dr **Darko Trifunovic***
Institute for National and International Security
Email:darko@intelligence-security.rs
`

DOI: https://doi.org/10.37458/ssj.6.2.14
Original Theoretical Article
Received: October 23, 2025
Accepted: December 2, 2025

DEFINING SECURITY SCIENCE AND INTRODUCING SECURITY SCIENCE INDEXATION (SSI)

Abstract: *The accelerating transformation of global security threats — including hybrid warfare, terrorism, cyber operations, and systemic vulnerabilities — exposes the inability of classical disciplines such as political science, sociology, law, or international relations to explain whether a State can survive, function, and develop under conditions of risk. This article defines Security Science as an autonomous scientific discipline whose purpose is to understand, explain, predict, and enhance the security condition of the State as an organized society. It establishes the epistemological identity, methodological architecture, and analytical scope of the discipline by distinguishing its general and special methods, and by clarifying its relationship to applied fields such as military, police, intelligence, cyber, and crisis management. Furthermore, the article introduces Security Science Indexation (SSI) as a necessary institutional mechanism for evaluation, indexing, and dissemination of research in this field, addressing the structural limitations of existing global indexing systems. SSI is presented as a platform that ensures security-oriented scholarly work is reviewed by qualified experts and positioned within a coherent academic ecosystem. The text argues that Security Science is indispensable for interpreting multidomain threats and for equipping States with predictive and preventive analytical capacities. As such, it serves as both a theoretical discipline and a strategic instrument essential for State survival and development in the contemporary world.*

Keywords: *Security Science; Security Science Indexation (SSI); State security condition; Hybrid threats; Terrorism indicators; Predictive methods; Intelligence analysis; Methodological architecture; Applied security studies; Resilience; Systemic vulnerability; National security.*

Introduction

The accelerating pace of global instability, the erosion of traditional security structures, and the emergence of hybrid, nonlinear, and transnational threats have profoundly altered the way states exist and interact. Contemporary security challenges demand a conceptual clarity and methodological rigor that the conventional disciplines of the twentieth century were never designed to provide. As the global environment evolves faster than existing theoretical frameworks can accommodate, the necessity of a discipline dedicated exclusively to the study of the State's security condition becomes undeniable. For many decades, security research was scattered across broader disciplines where it was not the primary object of inquiry. Political scientists examined it through institutional dynamics, sociologists through social phenomena, legal scholars through normative structures, historians through long-term patterns, and experts in international relations through interstate competition. Valuable insights emerged from all these perspectives, but none were adequate to explain risks, threats, vulnerabilities, hybrid operations, technological disruptions, or systemic crises confronting modern states. The fragmentation of perspectives led to profound theoretical incoherence, and, as a consequence, the global academic community lacked a truly native disciplinary home for security research.

The **Security Science Journal (SSJ)** was established precisely to address this deficiency. Its mission is to institutionalize Security Science globally, to create a shared epistemological foundation for scholars and practitioners, and to serve as an intellectual platform for developing theories, methods, and strategic insights that reflect the realities of the twenty-first century. The emergence of this journal marks an essential step in articulating Security Science as a coherent and independent scientific field. Yet this effort cannot succeed without a parallel transformation in how scientific knowledge in this field is indexed, evaluated, validated, and disseminated. The global academic ecosystem relies heavily on large multidisciplinary indexation systems such as Web of Science and Scopus. While these platforms are indispensable in many domains, they are structurally inadequate for Security Science. The underlying problem is not technological but epistemological: Security Science has matured into a field that requires **review, evaluation, and classification by experts who belong to the field itself**, rather than by scholars from distant disciplines who may not fully understand the methodological frameworks,

theoretical foundations, operational contexts, or security-specific implications of the works they assess.

The absence of qualified reviewers in existing indexation systems has created a long-standing structural barrier for journals and authors working in Security Science. Articles are frequently evaluated by political scientists, sociologists, international relations theorists, legal scholars, or even experts in public administration—highly competent in their own areas but not trained in the conceptual and analytical requirements of Security Science. This misalignment leads to methodological misunderstandings, inappropriate expectations, inconsistent evaluations, and, in many cases, the rejection or misclassification of high-quality scientific work simply because the evaluators lack the disciplinary background to understand it fully.

Security Science Indexation (SSI)

In response to the specific structural and epistemological characteristics of Security Science, there is a growing need for a dedicated indexation and evaluation framework: **Security Science Indexation (SSI)**. SSI is conceived as a global, specialized platform designed for the evaluation and indexing of journals, articles, research reports, and other scholarly outputs within the field of Security Science. Its fundamental purpose is to ensure that research in this domain is assessed within an evaluation environment that is conceptually aligned with the nature, scope, and methodological foundations of the discipline. Security Science represents a field whose analytical focus, methodological architecture, and practical relevance distinguish it from traditional disciplinary categories. It operates at the intersection of security studies, intelligence analysis, risk assessment, resilience studies, technological security, and strategic foresight, while simultaneously drawing on insights from the social sciences, natural sciences, engineering, and data-driven analytical methods. Existing indexation systems, while highly valuable and indispensable to global scholarship, are designed to serve broad disciplinary ecosystems and therefore cannot always capture the full analytical specificity of security-oriented research. SSI is intended to address this structural gap by providing an indexation space tailored to the internal logic of the field. One of the central rationales for SSI lies in the conceptual precision required in Security Science research. The discipline relies on clearly differentiated analytical categories such as risk, threat, vulnerability, exposure, resilience, and systemic fragility. These concepts are not interchangeable, nor are they purely

theoretical abstractions; they are operational tools used in policy design, intelligence analysis, crisis management, and strategic planning. An indexation framework familiar with these distinctions contributes to more accurate academic evaluation and reduces the risk of conceptual misalignment during the review and classification process.

Furthermore, Security Science is characterized by a unique methodological duality. It combines qualitative approaches—such as scenario building, strategic assessment, and intelligence cycle analysis—with quantitative modeling, simulations, data analytics, and computational methods. Evaluating such research requires an understanding of how methodological rigor is expressed across different analytical traditions and how hybrid methodologies contribute to knowledge production in security-related contexts. SSI is designed to promote evaluation standards that recognize methodological diversity while maintaining scientific rigor and transparency. Another key reason for establishing SSI is the applied and policy-relevant nature of Security Science. Research in this field frequently informs national security strategies, critical infrastructure protection, counterterrorism policies, crisis response mechanisms, and international security cooperation. As a result, scholarly output often addresses time-sensitive, complex, and multidimensional problems. An indexation system attuned to these realities supports the recognition of high-quality applied research that may not always conform to conventional disciplinary templates but nevertheless meets the highest scientific standards. SSI also responds to the increasingly international and transdisciplinary character of Security Science. The field brings together scholars, practitioners, and institutions from diverse geographical, cultural, and professional backgrounds. A specialized indexation framework can facilitate greater comparability, visibility, and accessibility of research outputs across regions and institutional contexts, thereby strengthening international collaboration and knowledge exchange within the discipline. From an institutional perspective, SSI contributes to the long-term consolidation of Security Science as an independent scientific field. By articulating clear inclusion criteria, evaluation principles, and thematic classifications, SSI helps establish a coherent academic ecosystem that supports disciplinary identity, academic fairness, and intellectual continuity. This, in turn, benefits researchers, institutions, policymakers, and funding bodies by providing a clearer reference point for assessing scholarly contributions in the security domain. In this sense, SSI emerges not as a corrective mechanism, but as an enabling infrastructure. It complements existing global indexation systems by offering a focused analytical layer that reflects the complexity, interdisciplinarity, and strategic relevance of

Security Science. Through this role, SSI supports the maturation of the discipline, enhances the global visibility of its scholarly output, and contributes to the development of a more structured, credible, and internationally respected body of security-related knowledge.

The manifesto that follows establishes the conceptual foundations of Security Science and serves as the intellectual framework upon which **Security Science Indexation (SSI)** is grounded.

Security Science definition

Security Science represents a mature, autonomous discipline whose purpose is to understand, explain, predict, and enhance the security condition of the State as an organized society. Although different cultures employ various expressions—*bezbednost, securitas, security, asphalea,* or *bitachon*—their meanings remain constant: ***Security Science is a scientific discipline dedicated to the systematic study of the security condition of the State as an organized political and social community. It examines the determinants, dynamics, vulnerabilities, and resilience of that condition, seeking to understand how states maintain continuity, stability, and development in the presence of internal and external risks. As an independent field, Security Science identifies and analyzes the fundamental factors that shape a state's ability to function, protect its population, uphold its institutions, and preserve its sovereignty.***

As the author of this article, I kindly request that all scholars and practitioners who wish to cite this definition do so in the following form:

Trifunović, D., Akrap, G., Spiro, Sh., Lombardi, M., Dragišić, Z., & Nomikos, J. (2025). *Defining Security Science and Introducing Security Science Indexation (SSI).* Security Science Journal, Volume 6, No. 2, 2025.

The discipline is grounded in a clearly defined epistemology: security is not a derivative of political science, sociology, law, or international relations, but a primary condition that determines whether these systems can exist and operate. For this reason, Security Science investigates the State not through ideological, legal, or sociological constructs but through the measurable and observable elements that constitute its overall security posture. This includes the analysis of strategic determinants, institutional capacities, societal cohesion, environmental pressures, technological dependencies, and the actions of hostile or competitive actors.

Methodologically, Security Science employs both general and special scientific methods

General methods are shared with the social sciences and include analytical reasoning, comparative analysis, case study methodology, historical interpretation, legal examination, and sociopolitical assessment. These methods allow the discipline to interpret complex human, social, and institutional processes.

Special methods, however, give Security Science its scientific distinctiveness

They originate from mathematics, natural sciences, intelligence analysis, cybersecurity, system theory, and data science. **Special methods** provide Security Science with its distinctive scientific identity and operational relevance. Unlike general social science methodologies, these methods are specifically designed to address complex, dynamic, and often adversarial security environments. They originate from mathematics, natural sciences, intelligence analysis, cybersecurity, systems theory, operations research, and data science, forming an integrated methodological architecture unique to Security Science.

At the level of **data collection**, Security Science employs advanced methods of information acquisition adapted to fragmented, incomplete, and heterogeneous data environments. These include deep information retrieval techniques based on hybrid algorithms that combine open-source intelligence (OSINT), signals analysis, cyber data, geospatial inputs, and structured and unstructured textual sources. Data collection in Security Science is rarely linear; it is iterative, adaptive, and threat-driven, designed to capture weak signals, early indicators, and emerging risks across physical, digital, social, and geopolitical domains.

Data processing methods constitute the second methodological layer and focus on transforming raw, often noisy information into structured and usable datasets. This stage relies on advanced classification systems, data normalization procedures, entity resolution techniques, and automated filtering mechanisms. These methods enable the integration of diverse data formats—quantitative measurements, textual narratives, visual data, and network logs—into coherent analytical structures. Processing methods ensure data reliability, comparability, and traceability, which are essential for subsequent analytical rigor.

Assessment of information methods represent a critical methodological layer in Security Science, positioned between data processing and analytical interpretation. Their primary function is to evaluate the reliability, relevance, credibility, and strategic value of collected information before it is integrated into formal analysis or decision-support processes. In security environments characterized by information overload, deception, manipulation, and asymmetrical data quality, assessment methods are essential for ensuring analytical integrity and operational relevance. These methods focus on **source evaluation, content validation,** and **contextual assessment.** Source evaluation examines the origin of information, including the credibility, access level, historical reliability, and potential bias of the source. In Security Science, sources may range from human intelligence and technical collection systems to open-source platforms and cyber-derived data, each requiring distinct evaluation criteria. Assessment frameworks help differentiate between primary, secondary, and derivative sources and determine appropriate weighting in subsequent analysis. Content validation methods assess the internal coherence, consistency, and plausibility of information. This includes cross-checking data against independent sources, identifying contradictions or anomalies, and verifying factual accuracy where possible. Validation is not limited to factual correctness; it also involves evaluating the completeness, timeliness, and precision of information, recognizing that partial or outdated data may still hold analytical value if properly contextualized. A key dimension of information assessment is **contextual and intent analysis**. Security Science recognizes that information is rarely neutral. Assessment methods therefore examine the strategic environment in which information emerges, including political, operational, technological, and adversarial contexts. This allows analysts to identify potential deception, influence operations, or narrative shaping efforts and to distinguish between noise, misinformation, and meaningful signals. Assessment of information methods also include **confidence grading and uncertainty management**. Rather than treating information as binary (true or false), Security Science applies probabilistic confidence scales and reliability matrices that express degrees of certainty and analytical confidence. This approach supports transparent decision-making and enables policymakers to understand both the strengths and limitations of available knowledge. In contemporary Security Science, information assessment increasingly incorporates **computational support tools**, including automated credibility scoring, anomaly detection, and pattern consistency checks across large datasets. These tools augment, but do not replace, expert judgment. Human analytical reasoning remains

essential for interpreting intent, strategic significance, and non-quantifiable contextual factors. Through systematic assessment of information, Security Science ensures that analytical outputs are based on evaluated, weighted, and contextually grounded inputs. These methods reduce the risk of analytical distortion, improve the quality of threat and risk assessments, and enhance the reliability of predictive modeling and strategic foresight. As such, assessment of information methods form a foundational pillar of Security Science, bridging raw data collection and high-level security analysis while reinforcing scientific rigor and decision relevance.

At the core of Security Science are **data analysis methods**, which combine quantitative and qualitative approaches to assess security phenomena. These include structured risk and threat assessment frameworks, vulnerability and resilience analysis, network and systems analysis, and scenario-based evaluation models. Analytical methods are designed to identify causal relationships, interaction effects, and systemic dependencies rather than isolated variables. They allow researchers to distinguish between risks and threats, assess intent and capability, evaluate exposure and impact, and analyze how local security events propagate across broader systems.

The fourth and defining methodological domain of Security Science consists of **predictive and forecasting methods**. These include predictive modeling, simulations, probabilistic forecasting, and trend extrapolation techniques. By applying mathematical models, agent-based simulations, and scenario forecasting, Security Science seeks not only to explain past and present security phenomena but also to anticipate future developments. Predictive methods are particularly critical in environments characterized by uncertainty, strategic deception, and rapid technological change. They support early warning systems, strategic foresight, and decision-making under conditions of incomplete information.

Complementing these core methodological domains are **computational techniques for anomaly detection, pattern recognition, and threat identification**, including machine learning applications and network-based analytics. These techniques enhance the capacity of Security Science to process large-scale datasets and detect non-obvious correlations, emerging patterns, and deviations from normal system behavior that may indicate latent or evolving security threats. Through the integrated application of these methods, Security Science detects, classifies, assesses, analyzes, and predicts security phenomena across multiple levels of analysis. It transforms vast volumes of heterogeneous information into

actionable knowledge, enabling states and institutions to identify threats at their earliest stages, evaluate their potential impact, and design preventive, adaptive, or mitigative strategies. In this way, the methodological framework of Security Science bridges scientific rigor and practical relevance, reinforcing the discipline's role as both an analytical and anticipatory science.

Our definition of Security Science vs. others

Before outlining the theoretical distinctions that differentiate Security Science from classical and contemporary security theories, it is essential to express sincere appreciation to all authors, scholars, and schools of thought that have shaped the global academic landscape. Every theorist—Barry Buzan, Edward A. Kolodziej, Stephen Walt, Bruce Hoffman, David Baldwin—as well as many others whose names are not explicitly mentioned in this text, has contributed immeasurably to the evolution of security-related knowledge. Their work has provided foundations, frameworks, and intellectual challenges without which the emergence of new paradigms—such as the concept of Security Science developed by Trifunović, D., Akrap, G., Spiro, Sh., Lombardi, M., Dragišić, Z., & Nomikos, J. —would not be possible. This text is therefore not a critique of their value, but a respectful positioning of a new, distinct, and scientifically operational discipline within the broader academic continuum.

Trifunović, D., Akrap, G., Spiro, Sh., Lombardi, M., Dragišić, Z., & Nomikos, J. vs. Barry Buzan

Prof. Dr. Darko Trifunović, and the authors of the concept of Security Science, defines security as an objective, measurable, and verifiable condition of the state and the societal system, while the theoretical approaches of Barry Buzan and the Copenhagen School of Security Studies begin from the opposite premise – that security does not exist as a reality but emerges only once a political actor declares something a threat. This fundamental ontological and epistemological difference makes Security Science incompatible with Buzan's securitization model. The Copenhagen School sees security as a discursive phenomenon, a product of language, political power, and the "speech act." In this paradigm, security is not a condition but a narrative. A topic becomes a "security question" only if a political actor issues a declaration, symbol, speech, or political warning through which the audience accepts that something is threatening. Therefore, analyses within this school rely on the interpretation of discourse, media narratives, and political communication—not on

real indicators, statistical data, or operational security assessments. Security Science, whose foundations were established by the works of Prof. Dr. Darko Trifunović and others, is based on a completely different starting hypothesis: security is a real fact, not a rhetorical construct. Security can be quantified, measured, verified, simulated, and predicted. It is a condition that a state possesses or loses, similar to how an organism possesses or loses health. In this sense, Security Science applies methods grounded in positivism, interdisciplinary research, mathematical modeling, intelligence analytics, OSINT, criminological methodology, and scientific standards of evaluation. If Security Science were to accept Buzan's definition, it would lose its ability to be considered a science—because it would lack a measurable research subject. For something to be science, it must contain phenomena that can be tested, falsified, replicated, and predicted. If security is merely discourse, it cannot be measured, it cannot be proven, terrorist attacks cannot be forecasted, nor can state defense be managed. Thus, the two paradigms are ontologically in conflict: Buzan's theory studies how one speaks about threats, while Trifunović's Security Science studies what a threat is and how it operates in reality. This clash of paradigms, although theoretical, has practical consequences: incorporating Security Science into the Copenhagen School would automatically reduce it to a subdiscipline of political science—eliminating its methodological, institutional, and academic independence.

This is precisely why Security Science has developed SSI – Security Science Indexation – the first global system for evaluating scholarly production in this field. It formally confirms that Security Science constitutes an academic discipline with its own standards, criteria, methodology, and scientific instruments—defining its difference from Buzan institutionally.

When practice is considered, the distinction becomes even clearer. Buzan's school cannot predict a terrorist attack nor protect critical infrastructure, because it does not operate with real threat indicators. Security Science can—because it studies the state, its capacity to survive, its resilience, and its real risks. In Trifunović's and others paradigm, security is not a rhetorical figure – it is the condition for life, survival, development, and the protection of national identity and institutions. Therefore, the incompatibility of the two paradigms is not a weakness but a strength. It allows Security Science to become what political theory never can be: a science that works in the real world, predicts actual threats, and protects state interests. In this incompatibility lies the logic of its existence. Security

Science, as defined by Prof. Dr. Darko Trifunović and others, cannot be compatible with Buzan's securitization because it does not study "speech about threats," but the threat itself as a measurable reality.

Trifunović, D., Akrap, G., Spiro, Sh., Lombardi, M., Dragišić, Z., & Nomikos, J. vs. Kolodziej

The concept of Security Science defined by Prof. Dr. Darko Trifunović and others represents a completely new epistemological and methodological paradigm compared to dominant theoretical models of security originating from International Relations, including the approach of Edward A. Kolodziej. While Kolodziej views security as a political-strategic phenomenon emerging within the international system, balance of power, and geopolitical dynamics, Security Science begins from the premise that security is a real, measurable, and verifiable condition of the state and society that can be quantified, predicted, and governed. Kolodziej in his book *Security and International Relations* (2005) analyses security primarily through the lens of international actors, diplomacy, military capacity, alliances, global order, and political decision-making. Security in this paradigm is understood theoretically—by interpreting geopolitical dynamics, interests of great powers, and relations of power. There is no requirement to measure security as a condition, nor to derive operational tools capable of protecting a state in real time. Trifunović and others, concept of Security Science reverses this starting point: it does not ask how states speak about security, but what security is in reality. Security is defined as a condition of a system that can be objectively determined through security indicators, intelligence capacity, risk analyses, criminological data, cyber parameters, and other measurable factors. In this paradigm, the purpose of Security Science is for the state to understand threats, forecast them, and respond. The goal is not theoretical explanation, but protective capability.

The difference is therefore fundamental—while Kolodziej *describes* security, Trifunović and others *demands that it be measurable and manageable*. Kolodziej offers a theoretical framework for understanding international relations. Trifunović and others offers a scientific framework for application—from detecting terrorist networks and preventing foreign influence to protecting national critical infrastructure. Security Science is an independent discipline because it possesses its own subject, method, objective, and instrument—including SSI (Security Science Indexation), confirming its institutional and methodological autonomy. Thus, Kolodziej and Trifunović and others do not represent

theoretical opponents, but two epistemologically separate spheres. The first attempts to explain the world; the second creates a scientific tool to change and defend it. International Relations can explain why war occurs—Security Science must ensure it does not occur.

Trifunović, D., Akrap, G., Spiro, Sh., Lombardi, M., Dragišić, Z., & Nomikos, J. vs. Walt

The concept of Security Science advocated by Prof. Dr. Darko Trifunović and others represents an ontological and methodological discontinuity compared to traditional approaches to international security, including Stephen Walt, one of the leading realist theorists. While Walt considers security primarily as a function of the international system, balance of power, and states' ability to act in an anarchic international environment, Security Science defines security as an objective, measurable condition of a state and society, independent of the international order or interpretative discourse. In Walt's concept, security is primarily a result of foreign-policy factors: alliances, power distribution, perception of threat, and projection of military strength. His key insight is that states react to threats based on rational calculation within a structurally anarchic environment. Thus, analysis focuses on the international arena, balance of power, and strategies of states. Security is an outcome of external behavior—not an internal systemic state. In contrast, Trifunović and others, develops Security Science as an independent scientific discipline whose research subject is not the international order, but the state, society, and systems themselves as carriers of security conditions. Security in this concept is not seen as a consequence of political decisions, but as a measurable fact operationalized through risk analysis, criminal networks, terrorist capacity, intelligence indicators, cyber parameters, and system resilience. Security must be verifiable, predictable, and governable—this is what separates Security Science from theoretical traditions of International Relations. Ultimately, the difference lies in the *function of knowledge*. Walt explains state behavior and international security phenomena—his theory is analytical and descriptive. Trifunović and others Security Science is operational, normative, and action-oriented: it must allow the state to identify threats and stop them. If knowledge cannot prevent a terrorist attack, cannot forecast destabilization, and cannot protect infrastructure—it is not scientific knowledge in the Security Science paradigm. Thus, Walt belongs to the philosophical-academic sphere of world-understanding; Trifunović and others belongs to

the practical-scientific sphere of world-management. Walt tells us why war breaks out; Security Science must prevent it from happening.

Trifunović, D., Akrap, G., Spiro, Sh., Lombardi, M., Dragišić, Z., & Nomikos, J. vs. Hoffman

The concept of Security Science developed by Prof. Dr. Darko Trifunović and others represents an epistemological and methodological step forward from existing terrorism-related literature, including the work of Bruce Hoffman, the most renowned theorist in this field. Hoffman defines terrorism as a form of political violence used to achieve ideological goals, based on the intentional use of fear, propaganda, and media attention. In Hoffman's analysis, the primary focus is not the state as the bearer of security, but the terrorist organization, its motivation, strategy, and historical development. Security is not treated as a measurable category, but as a consequence of success or failure of terrorist groups and state responses. Security Science in Trifunović and others, concept views terrorism as only one element of a broader security system. It does not accept terrorism as the central point of analysis; instead, it treats it as one risk component that affects the security level of the state—together with criminal networks, foreign influence, espionage, cyberattacks, institutional destabilization, migratory pressures, and others. Thus, Hoffman studies terrorism to *understand the phenomenon*; Trifunović and others studies terrorism in order to *govern the security condition of the state*. Moreover, while Hoffman's methodology relies on political science, history, and case studies, Security Science uses predictive analytics, quantification of risk, OSINT, intelligence models, and measurable security indicators. Hoffman describes how terrorists communicate fear; Trifunović and others models how the state measures vulnerability, detects risk, and prevents attacks. The difference is therefore *purpose*—Hoffman aims to explain; Security Science demands protection. Finally, Hoffman's work remains within terrorism studies and security studies. Trifunović and others creates an independent discipline—Security Science—with its own subject (security as condition), method, instrument (SSI – Security Science Indexation), and function (operational protection of the state). Thus, Security Science is not only an academic innovation but a practical science whose result must be measurable in the real world.

Trifunović, D., Akrap, G., Spiro, Sh., Lombardi, M., Dragišić, Z., & Nomikos, J. vs. Baldwin

The concept of Security Science developed by Prof. Dr. Darko Trifunović and otehrs represents an ontological and methodological separation from existing theories, including the approach of David Baldwin, one of the key theorists attempting to "precisely redefine" the concept of security within political science and International Relations. Baldwin argues that security is not categorical but relative and contextual—security is always "security for someone, from something, at some time, for some value." He therefore treats security as a conceptual category that is flexible and open to various interpretations, yet remains normatively undefined and epistemologically non-operational. In contrast, Trifunović's Security Science does not treat security as an abstract term nor as a "label" that can be applied to any phenomenon (as happens in Baldwin's critique of overly broad interpretations of security). Instead, security is clearly defined as a measurable condition of the state and system, which can be confirmed, forecasted, and governed through quantitative indicators—crime, terrorism, cyberattacks, foreign influence, espionage, infrastructure functionality, institutional integrity, etc. Therefore, while Baldwin attempts to refine the conceptual limits of the *word* "security," Trifunović and others defines the subject, method, purpose, and scientific instrument of a discipline—transforming security from a concept into a scientific category with empirical properties. The deepest difference lies in the *function of knowledge*. Baldwin offers a tool for analytical discussion—he enables more precise philosophical and political understanding of what security may mean. Trifunović and others Security Science demands that knowledge be operational—it must protect the state and society, enable anticipation of threats, and produce real results in practice. If a theory of security cannot prevent an attack, destabilization, or systemic collapse—then it is not scientifically useful. Through this, Security Science moves from the domain of theoretical descriptive disciplines to the domain of action-oriented sciences. In other words: Baldwin explains *what the word security might mean*; Trifunović and others explains *what security is and how it is defended*. While Baldwin sees security as a relative, conceptually flexible term within political theory, Prof. Dr. Darko Trifunović and others defines Security Science as an autonomous discipline that treats security as a real, measurable condition of the state and an operational parameter of its survival.

Security Science functions as a foundational for the entire spectrum of security related studies

Security Science functions as a **foundational and integrative scientific discipline** for the entire spectrum of security-related studies and practices. It represents the theoretical, methodological, and epistemological base upon which **Military and Defense Studies, Police Studies, Intelligence Studies**, as well as all other applied security-oriented fields, are constructed. These applied domains derive their analytical coherence, scientific legitimacy, and methodological consistency only when they are grounded in the conceptual framework of Security Science. In this sense, Security Science operates as a **roof discipline**, unifying and structuring knowledge related to all actors of the security system, regardless of their institutional or operational specificity. Within this architecture, military strategy, defense planning, police operations, intelligence analysis, crisis management, cybersecurity, and critical infrastructure protection are not independent sciences, but **applied fields** that implement and operationalize the principles, methods, and analytical models developed within Security Science. Security Science provides these fields with standardized concepts, shared analytical language, and scientifically validated methods for understanding threats, risks, vulnerabilities, resilience, and systemic stability. Without such a common scientific foundation, applied security practices risk fragmentation, conceptual inconsistency, and methodological arbitrariness.

In the domain of geopolitics, Security Science offers a more precise and operationally relevant interpretation of power, influence, and spatial competition. While political science traditionally approaches power as an institutional, normative, or ideological relationship, Security Science examines power as a **measurable expression of security capability**, resilience, strategic depth, and control over critical resources and infrastructures. From this perspective, geopolitics—concerned with territorial strategy, power projection, strategic positioning, and security competition—naturally falls within the analytical domain of Security Science rather than existing as a purely political abstraction.

As a **predictive and preventive discipline**, Security Science extends beyond the interpretation of existing threats to the systematic identification of early indicators of emerging terrorist, hybrid, criminal, cyber, and geopolitical risks. Through the application of structured scientific methods, Security Science enables the analysis of weak signals, pattern evolution, and threat convergence across multiple domains. This analytical capacity

allows the State and other security actors to anticipate crises, design proportionate and timely responses, and maintain strategic awareness and advantage in an increasingly complex and contested security environment. In this role, Security Science serves not only as an academic discipline but as a **strategic knowledge framework** that connects theory with practice, integrates diverse security actors, and supports evidence-based decision-making across the entire security system.

In sum, Security Science is the comprehensive scientific discipline that explains how states survive, adapt, and develop under conditions of uncertainty. It provides the theoretical, methodological, and analytical foundation necessary for understanding and protecting the security condition of the modern State, making it an essential academic and practical field in the contemporary world.

Throughout history, the study of security has been distributed across disciplines not structurally designed to address it. Political science interpreted security through the design of institutions and power relations; sociology viewed it through the lens of social structures; legal studies reduced it to normative order; historians embedded it in civilizational cycles; international relations framed it in terms of the balance of power. None of these perspectives was sufficient to explain the increasingly complex realities of modern threats, hybrid warfare, and systemic vulnerabilities. Their limitations became evident when methods designed to analyze political preferences, social behaviors, or legal norms proved inadequate for understanding the dynamics of survival, crisis, and resilience within states.

Geopolitics exemplifies this misplacement. Traditionally treated as a branch of political science or international relations, geopolitics has been framed through political theories. Yet geopolitics is fundamentally the study of how states apply force, influence, and constraint across geographic space. Force is a security attribute, not merely a political one. The struggle for strategic advantage, territorial control, and regional influence reflects security capabilities and vulnerabilities rather than political preferences. What political science perceives as competition, Security Science recognizes as a manifestation of risk, power, threat, opportunity, and systemic equilibrium. Geopolitics, therefore, belongs conceptually and methodologically within Security Science.

Security Science emerges as a response to the systemic inability of earlier disciplines to explain or predict state behavior under conditions of risk. The transformation of the global environment, including hybrid conflicts, cyber operations, transnational

terrorism, demographic pressures, technological disruptions, and rapid geopolitical realignments, exposed the inadequacy of traditional theoretical tools. Security Science provides a new epistemological apparatus capable of integrating these multifaceted phenomena.

Its epistemological identity is defined by the recognition that the State is an organized society whose survival depends on maintaining a specific condition of security. Sociology describes the social organism; political science examines governance; law prescribes norms; international relations map interstate dynamics. Security Science, however, evaluates whether these systems can endure under pressure, whether norms can survive crises, whether institutions can absorb shocks, and whether societal structures remain cohesive in the face of threats.

Methodologically, Security Science unifies interpretative and analytical worlds. It incorporates the reasoning of the social sciences alongside the precision of natural sciences. Its special methods include advanced data acquisition techniques such as deep internet searches driven by hybrid algorithms capable of semantic analysis and anomaly detection, methods of classification that impose analytical order on vast datasets, assessment procedures that quantify risk exposure, analytical techniques that reveal systemic patterns, and predictive models that anticipate the behavior of complex systems.

Security phenomena are inherently interdisciplinary, dynamic, nonlinear, multifactorial, and sensitive to perturbations. They cannot be understood solely through political, sociological, legal, or historical frames. Security Science is structured to synthesize these dimensions into a coherent explanation of how states maintain stability, manage crises, and navigate environments characterized by uncertainty.

Within this framework, the Security System of the State is defined as an integrated whole composed of institutions, actors, and processes responsible for safeguarding sovereignty, territorial integrity, constitutional order, public safety, and societal functioning. Armed forces, police, intelligence services, civil protection, specialized formations, and the citizenry together sustain this condition. Defense studies, Police studies, and Intelligence studies are sub-disciplines of Security Science because they address operational domains within a broader security architecture whose theoretical logic is provided by the parent discipline.

One of the most persistent conceptual misunderstandings in contemporary academic discourse is the claim that "military sciences" exist as a scientific domain in their own right. The very fact that this term is used in the plural indicates a fundamental confusion about what constitutes a science. A discipline earns the status of science only when it possesses a clearly defined epistemological identity, a coherent object of study, and both general and special scientific methods. The fields commonly presented as "military sciences" do not meet these criteria. Their proponents often insist that strategy, tactics, and operational art are themselves sciences, but this is a misconception that collapses under minimal analytical scrutiny. If the mere existence of structured rules, patterns, or techniques were sufficient for something to be called a science, then chess, as a domain with clear principles, models, and strategic logic, would itself qualify as a scientific field — which it does not.

The misclassification of military skill as "military science" has more profound implications. It has led many institutions to abandon the concept of military academies in favor of "military universities," under the assumption that this terminological shift confers scientific legitimacy. In reality, military academies have historically and correctly focused on military skill, a profoundly complex, multidisciplinary domain requiring mastery of more than 70 scientific fields and subfields. This does not diminish the value of military education; on the contrary, it demonstrates its breadth and sophistication. But breadth and sophistication do not equal scientific autonomy. Military skill is an *application* of science, not a science in itself. The same applies to tactics and strategy, which remain high-level applications of knowledge, informed by science but not constituting scientific disciplines in their own right. Neither strategy nor tactics possess their own general and specialized methods, theoretical frameworks, or epistemological boundaries; they draw on psychology, geography, logistics, mathematics, ethics, political science, engineering, intelligence analysis, and, above all, security science. They are domains of practice built on scientific foundations—not sciences in isolation.

A structurally identical misunderstanding exists in policing. Instead of maintaining police academies that cultivate professional skill grounded in interdisciplinary scientific foundations, many states have created so-called "universities of security" or "police universities," which segment security into narrow professional channels detached from the disciplinary core. Both policing and military activity are **components of the State's broader Security System**. Neither can be meaningfully separated from the holistic

architecture that Security Science provides. Creating artificially isolated "sciences" around military or police activities reflects a category error: it confuses operational specialization with scientific independence. Just as an engineer or physician applies knowledge from multiple sciences without claiming to constitute a new standalone science, so too must military and police professionals recognize that their fields are sub-disciplinary applications of Security Science rather than autonomous scientific realms.

The logic is straightforward. The Security System of the State depends on Security Studies as its specialized analytical layer, and Security Studies themselves depend entirely on **Security Science** as the foundational discipline that defines concepts, methods, processes, risks, threats, vulnerabilities, systemic behaviors, and the security condition of the State. Without Security Science, there can be no coherent theory of the military, no scientifically structured police studies, no methodology for intelligence analysis, no epistemological basis for operational art, and no conceptual clarity for strategy or tactics. The hierarchy is therefore clear: security is the science; the military, police, and intelligence domains are its applications. To confuse this hierarchy is to weaken the entire discipline. To respect it is to empower the security profession and restore intellectual integrity to the field.

Security Science has both theoretical importance and immediate practical relevance. It strengthens strategic foresight, enhances the accuracy of national risk assessments, improves institutional resilience, and enables more informed decision-making in complex environments. It offers frameworks for understanding and countering hybrid threats, guiding crisis prevention, and interpreting the dynamics of power and vulnerability that shape both domestic and international stability.

The Security Science Journal advances this mission by providing a global platform for the convergence of theory, method, and practice. Its establishment coincides with the emergence of Security Science Indexation (SSI), which reflects the need for a specialized system of academic evaluation that recognizes the field's unique character. SSI will ensure that research in this domain receives fair, competent, and discipline-specific review, free from the methodological biases that arise when evaluators come from unrelated fields. Just as Security Science is the intellectual architecture of modern security, SSI becomes the institutional architecture that allows this knowledge to be validated, disseminated, and advanced.

Security Science is not an extension of another discipline nor a derivative concept. It is the foundational science of the State's survival, stability, and development. Its emergence was necessary, its growth is unavoidable, and its institutionalization—through journals like SSJ and indexation systems like SSI—is strategically essential. Security Science stands as the scientific pillar of twenty-first-century security, created to interpret the complexity of the contemporary world and to provide the knowledge required for the preservation and advancement of organized human society.

Applied Dimension of Security Science: Indicators of Terrorist Threats

Indicators form the bridge between scientific theory and operational intelligence. They allow states to detect danger before it manifests, transforming ambiguity into knowledge.

How Security Science Defines Indicators of Terrorist and Hybrid Threats

Security Science, as the foundational discipline that studies the security condition of the State, provides the conceptual, methodological, and analytical framework for identifying, interpreting, and operationalizing indicators of both terrorist and hybrid threats. Indicators represent early-warning signals that reveal destabilizing processes before they manifest into violence or systemic disruption. Without them, national security institutions would operate blindly, unable to detect developing dangers or anticipate strategic surprises. A state's ability to recognize these indicators determines whether it will face crises reactively or proactively.

The identification of indicators begins within the intelligence cycle, where intelligence services serve as the State's sensory and analytical organs. They collect, process, evaluate, and disseminate information directly to political and military leadership, enabling timely decision-making. As global threats become more multidimensional, adaptive, and ambiguous, the role of intelligence services does not diminish; instead, it expands, requiring deeper integration with national institutions and international partners. Terrorism and hybrid warfare represent two domains in which Security Science's methodological rigor becomes indispensable.

Terrorist Threat Indicators in the Framework of Security Science

Security Science defines terrorism as a security phenomenon that operates simultaneously at the individual, organizational, ideological, transnational, and geopolitical

levels. Because terrorist actors intentionally obscure their networks, logistics, intentions, and identities, the task of detecting terrorist threats depends on identifying the structural indicators that expose their presence, regardless of concealment.

The first essential indicator involves the presence of terrorists or individuals connected to terrorist activity, whether scattered across territory or embedded within specific communities. A more serious condition emerges when structured terrorist groups, cells, or subgroups appear, signaling enhanced organizational capability. The United States, through Section 219 of the Immigration and Nationality Act, formally defines a terrorist organization as one that engages in terrorist activity or retains the capability and intent to do so, thus posing a threat to national security. The European Union, under Council Common Position 2001/931/CFSP, similarly defines terrorist groups as structured collectives acting in concert to commit acts capable of destabilizing or destroying fundamental political, constitutional, economic, or social systems. These definitions are crucial for establishing the legal and analytical threshold at which individuals or small groups become systemically dangerous.

A second major indicator is the involvement of states that sponsor terrorism. State sponsorship transforms a non-state actor into a geopolitical tool. It includes military, intelligence, logistical, financial, and diplomatic support that increases the lethality and reach of terrorist organizations.

A third indicator involves non-governmental organizations that function as logistical fronts—entities that present themselves as humanitarian or educational but, in reality, facilitate movement, funding, recruitment, concealment, and international legitimacy. International bodies such as the UN, EU, and FATF play a critical role in identifying and sanctioning such organizations.

Finally, ideological drivers, whether religious or political, constitute an essential indicator, since they generate motivation, identity, cohesion, recruitment, and justification for violence. These ideological fronts often exist to conceal state or organizational sponsors under the guise of humanitarian or civil society initiatives.

Although more indicators exist—such as patterns of financing, weapons acquisition, operational rehearsals, and propaganda—the five structural elements described above constitute the core of operational fieldwork. They are especially pronounced in the study of

Islamist and jihadist terrorism, where ideological, organizational, and logistical indicators appear concurrently. Security Science synthesizes these elements into analytical models that allow states to quantify risk, predict escalation, and implement preventive measures before violence materializes.

Hybrid Threat Indicators in the Framework of Security Science

Hybrid threats differ from terrorism in that they represent **state-directed or state-enabled multidomain campaigns** designed to destabilize another state without a formal declaration of war. Security Science interprets hybrid warfare not as a collection of isolated hostile acts, but as a strategically synchronized effort that combines political, informational, cyber, economic, energy, intelligence, criminal, military, and diplomatic instruments into a single operational continuum. This continuum is nonlinear, covert, deniable, adaptive, and designed to erode the target state's resilience over time.

Indicators of hybrid warfare are therefore multidimensional and reveal themselves simultaneously across different sectors. In the informational and psychological domain, Security Science identifies indicators such as abrupt escalation in coordinated disinformation, synchronized narratives aimed at delegitimizing institutions, mass use of bots and troll networks, attacks on national identity or historical memory, and timed release of compromising materials during politically sensitive periods. These phenomena represent attempts to fracture societal cohesion and reduce trust in authority.

In the political-security domain, indicators include covert support to radical or anti-system actors, creation of new NGOs or media outlets with opaque funding, sudden proliferation of "spontaneous" protests with unusual levels of coordination, foreign influence on electoral processes, and the discreet presence of intelligence officers under diplomatic, cultural, or journalistic cover. These indicators reveal efforts to manipulate the political ecosystem from within.

Digital and cyber indicators manifest in sudden spikes of cyberattacks targeting government, financial, communication, and energy infrastructures. Advanced persistent threats linked to foreign states, large-scale data leaks, deepfake operations, falsified diplomatic identities, and the use of cryptocurrencies to conceal financial flows are hallmarks of hybrid operations. Economic and energy indicators are affected by strategically timed disruptions of energy supply, targeted investments by geopolitical rivals,

manipulation of energy dependence, and attempts to acquire or influence critical infrastructure such as ports, refineries, telecommunications, or IT systems.

In the military and security sphere, hybrid operations often reveal themselves through the presence of "military instructors," covert operatives, or private military companies, as well as border provocations, drone incursions, electronic warfare, weapons distribution to criminal networks, and clandestine support to extremist groups. Social and cultural indicators include foreign-financed campaigns aimed at polarizing ethnic, religious, or minority communities, influence operations in universities and media, and the spread of narratives designed to create moral panic or societal fragmentation. Criminal and intelligence indicators emerge when organized crime groups become instruments of foreign intelligence services, creating networks for smuggling, safe houses, money laundering, and proxy operations. Diplomatic indicators include sudden, aggressive rhetoric, international pressure campaigns, threats of sanctions, and the use of global institutions to block, discredit, or weaken the target state. Security Science integrates these indicators into a unified model that interprets hybrid threats not as isolated symptoms but as interconnected manifestations of a single hostile strategic intent. Hybrid warfare is therefore understood as an attack on the State's security condition through coordinated multidomain pressure designed to destabilize without crossing the threshold of conventional conflict.

The Scientific Significance of Indicators

By defining indicators of terrorist and hybrid threats, Security Science transforms ambiguity into knowledge and signals into actionable intelligence. Indicators allow analysts to track escalation, identify sponsors, map networks, quantify risks, and understand the temporal dynamics of hostile behavior. They reflect the scientific core of Security Science: the ability to detect, classify, assess, analyze, and predict complex security phenomena. Both terrorist and hybrid indicators demonstrate why Security Science is an independent scientific discipline. They require methodological precision that no single traditional field—political science, sociology, law, or international relations—can provide on its own. Only Security Science, with its fusion of social, natural, intelligence, and computational methodologies, can synthesize these phenomena into a coherent framework capable of protecting the modern State.

Conclusion

Security Science emerges as a discipline not because existing sciences failed to address isolated aspects of security, but because none of them possess the epistemological, methodological, or conceptual capacity to comprehend security as a *systemic condition*. Politics can explain authority, sociology can explain social structure, law can explain norms, and international relations can explain interactions among states — yet none of them can explain whether a state is capable of surviving, functioning, resisting pressure, or developing under conditions of threat. Security Science fills this intellectual void by studying the one dimension of statehood upon which all others depend: the security condition. The importance of this discipline lies in its ability to integrate multiple layers of analysis into a coherent scientific framework. Rather than interpreting threats as isolated events, Security Science situates them within a systemic context — linking vulnerabilities to capabilities, external pressures to internal cohesion, and strategic intent to operational indicators. By doing so, it transforms the study of security from a fragmented, descriptive practice into a predictive, analytically rigorous scientific enterprise. Security Science explains that security is not a static state but a dynamic equilibrium shaped by factors such as the geopolitical environment, strategic resources, societal resilience, institutional strength, technological capacity, and the presence of hostile actors. Each of these determinants interacts with others, producing complex and sometimes nonlinear patterns of behavior. Only a dedicated scientific discipline, equipped with both general and special methods, can detect, quantify, classify, and interpret these patterns. This alone distinguishes Security Science from political science, sociology, history, or international relations — disciplines that observe parts of the puzzle, but lack the methodological architecture to see the system as a whole. Crucially, Security Science provides the analytical instruments necessary to understand contemporary threat landscapes, where terrorism, hybrid warfare, intelligence competition, cyber operations, economic coercion, and disinformation campaigns converge. It explains how indicators of terrorist activity — the presence of individuals, organizations, state sponsors, logistical fronts, and ideological triggers — form part of a broader operational ecosystem. Likewise, it clarifies how hybrid threats are revealed not through singular events, but through orchestrated patterns involving political manipulation, cyber intrusion, economic pressure, psychological operations, and covert intelligence activity. Only Security Science can synthesize these multidomain indicators into a framework that allows states to anticipate, rather than merely react to, strategic

challenges. Another essential contribution of this discipline lies in its methodological depth. Security Science combines interpretive social science methods with advanced analytical techniques derived from mathematics, the natural sciences, data science, and intelligence studies. This includes predictive modeling, anomaly detection, algorithmic classification, risk assessment, systematic mapping, and hybrid intelligence analysis. These methods render Security Science not merely a theoretical field but a practical, operationally indispensable science. They enable states to convert signals into warning, information into understanding, and understanding into strategic action. The establishment of *Security Science Indexation (SSI)* further demonstrates the maturity and necessity of this discipline. Traditional global indexation systems lack reviewers with the expertise to evaluate Security Science adequately, leading to conceptual confusion, misclassification, and methodological misalignment. SSI provides a corrective institutional mechanism that ensures scientific work is evaluated according to standards appropriate to the discipline. This step is not only academic; it is strategic. Without proper evaluation, no scientific discipline can achieve legitimacy, growth, or international influence. Security Science also clarifies its relationship to applied fields. Defense, policing, intelligence, crisis management, cyber operations, and strategic communication are not independent sciences; they are operational domains grounded in the theoretical and methodological foundations of Security Science. This hierarchy is intellectually and operationally unavoidable. Military strategy, intelligence assessments, and police operations cannot be scientifically coherent without a parent discipline that explains the structure, conditions, and dynamics of security itself. As geopolitical transformations accelerate and states simultaneously face the challenges of terrorism, hybrid conflict, technological disruption, demographic shifts, and information warfare, Security Science becomes indispensable not only for academia but also for statecraft. Its models, methods, and theories provide decision-makers with the tools needed to maintain stability, increase resilience, strengthen sovereignty, anticipate crises, and manage uncertainty. In this sense, Security Science is not merely a field of study; it is a strategic asset. Security Science stands as the central scientific discipline of the twenty-first century for understanding, preserving, and enhancing the State's capacity to survive and develop in a complex global environment. It unifies previously fragmented knowledge, establishes a coherent scientific foundation, and provides the analytical instruments necessary to interpret and predict multidomain threats. Far from being an academic abstraction, Security Science is the intellectual framework through which the modern State

protects its integrity, sovereignty, and future. It is therefore accurate to state that Security Science is not simply a new field; it is an unavoidable evolution in the scientific understanding of human societies under threat. Its emergence was necessary, its consolidation is urgent, and its further development is of direct strategic importance for states, institutions, and the international system as a whole.

The article is without enumeration or quotations

The absence of references in this paper is a deliberate and academically justified choice rooted in the nature and purpose of the work. This text is not designed as a review of existing literature nor as an empirical study that depends on previously published findings. Instead, it functions as a foundational theoretical document whose primary aim is to define, structure, and intellectually establish Security Science as an autonomous field. Because the discipline, as described here, has not yet been formally articulated in the scientific community, there is no existing corpus of literature that could be meaningfully cited as a conceptual source. The arguments in the paper represent original contributions and introduce a new epistemological framework, methodological architecture, and disciplinary identity that do not derive from prior scholarship but rather seek to create the conditions for future scholarship to emerge. Foundational scientific works often appear in this manner. When a discipline is being established, it is the conceptual clarity, logical coherence, and internal structure of the argument that give the work its academic legitimacy, rather than reliance on earlier sources. This paper defines the subject of Security Science, outlines its methodological foundations, distinguishes it from adjacent fields, and proposes institutional mechanisms necessary for its development. These contributions originate within the text itself and do not depend on external literature for validation. As such, the paper serves as a reference point for future studies rather than a derivative analysis built on existing citations. In this context, the absence of references should not be interpreted as a lack of rigor but rather as an indication of the paper's role in shaping a conceptual foundation where none previously existed. By establishing the core definitions, theoretical constructs, and analytical principles of Security Science, the work positions itself as an inaugural contribution to a discipline that is only now entering academic recognition. Future research will be able to cite this text precisely because it stands at the beginning of that intellectual lineage, offering original insights rather than merely compiling what is already available.

Dedication

This work is dedicated to the professors whose intellectual strength, scholarly integrity, and unwavering commitment have shaped both the definition of Security Science and the very foundation of the Security Science Journal. Their contributions are not merely supportive; they are formative. Through their insight, mentorship, and visionary understanding of the discipline, they have helped establish the conceptual architecture upon which Security Science now stands as an independent field.

To Professor **Gordan Akrap**, whose depth of thought and strategic clarity have illuminated the path toward recognizing security as a scientific condition rather than a political circumstance; to Professor **Shlomo Spiro**, whose pioneering academic rigor and global perspective strengthened the discipline's theoretical boundaries; to Professor **Marco Lombardi**, whose multidisciplinary approach and exceptional analytical precision enriched the methodological foundations of the field; to Professor **Zoran Dragišić**, whose steadfast dedication, professional experience, and scholarly guidance provided essential structure and stability to the development of SSJ; and to Professor **John Nomikos**, whose long-standing leadership in intelligence studies, international collaboration, and strategic vision has significantly reinforced the evolution of Security Science and strengthened the global reach of the Security Science Journal. Their collective work, wisdom, and encouragement have shaped not only this definition, but also the emergence of Security Science as a distinct and necessary scientific discipline. The Security Science Journal exists today because they believed in the importance of establishing a scientific foundation for understanding the security condition of the modern state. Their contributions will remain permanently woven into the identity of Security Science and will continue to guide generations of scholars who follow.

Special dedication to Professor Dr. Alex P. Schmid

This dedication honors Professor Dr. Alex P. Schmid, one of the world's most distinguished scholars in the field of terrorism studies, whose intellectual influence and professional integrity have profoundly enriched the development of the Institute for National and International Security (INIS) and the Security Science Journal. As an esteemed member of INIS, Professor Schmid has offered not only his exceptional academic expertise but also sincere support, encouragement, and trust in the vision that guides our work. His pioneering contributions to the academic understanding of terrorism,

radicalization, and political violence have shaped entire generations of researchers. For INIS and SSJ, his engagement represents a unique source of strength and legitimacy, reinforcing our mission to establish Security Science as an independent and globally recognized discipline. Through his guidance, we have advanced our intellectual foundations with clarity, rigor, and a deeper sense of purpose. We extend our profound gratitude for his generosity, his mentorship, and his unwavering commitment to elevating the standards of security research. His support stands as an enduring part of our institutional identity and a guiding light for all who contribute to the growth and international recognition of Security Science.

Special dedication to Dr. Richard R. Valcourt

This dedication is offered in honor of Dr. Richard R. Valcourt, a distinguished scholar, respected editor, and one of the most influential voices in the global study of intelligence and counterintelligence. His lifetime of academic leadership, particularly through his stewardship of the *International Journal of Intelligence and CounterIntelligence*, has shaped the intellectual landscape of modern intelligence studies and set the standard for rigorous scholarship in the field. For the Institute for National and International Security (INIS) and the Security Science Journal, Dr. Valcourt's support has been significant. His recognition of our efforts, his encouragement at critical moments, and his shared belief in the necessity of establishing Security Science as a coherent and independent discipline have strengthened our mission and elevated our work. His presence within the INIS community symbolizes not only academic excellence but also integrity, mentorship, and a genuine commitment to advancing knowledge in the service of global security. We express our heartfelt appreciation for his outstanding contributions, his wisdom, and his unwavering dedication to academic rigor. His name and legacy stand as a source of inspiration, guiding both the development of Security Science and the evolution of the Security Science Journal. His influence will continue to resonate in the work of future scholars who follow the path he helped illuminate.

Special dedication to the Professor. dr Jan Goldman

This dedication is made in honor of Dr. Jan Goldman, a leading scholar in intelligence studies, whose intellectual depth, ethical insight, and long-standing commitment to academic excellence have greatly enriched the development of the Institute for National and International Security (INIS) and the Security Science Journal. As one of

the foremost global authorities on intelligence analysis, intelligence ethics, and the role of intelligence in democratic societies, Dr. Goldman has shaped modern understanding of how intelligence work must be conducted with rigor, responsibility, and respect for fundamental values. For INIS and SSJ, his engagement represents an invaluable contribution. His scholarly expertise, openness to collaboration, and sincere encouragement have strengthened our belief in the need to establish Security Science as a fully recognized and coherent academic discipline. Through his support, our mission gained both intellectual credibility and a deeper philosophical grounding, particularly in understanding how intelligence fits within the broader security condition of the State. We extend our most profound appreciation for his guidance, generosity, and enduring commitment to fostering scholarship that upholds scientific integrity and the public good. Dr. Goldman's influence will continue to inspire future generations of researchers and practitioners whose work will build upon the foundations he helped shape.

Special dedication to the Professor. Dr Juliusz Piwowarsky

A special expression of gratitude is extended to **Prof. Dr. Juliusz Piwowarski**, whose scholarly excellence, partnership, and long-standing commitment to the development of the field of Security Science represent a foundational pillar in the international recognition of this discipline. As co-author of the book *From Security Science to Security Culture*, his academic contribution significantly shaped the conceptual evolution of Security Science and enabled its transformation into an operational, measurable, and internationally relevant scientific framework. His intellectual guidance, collegial support, and unwavering academic integrity continue to inspire the present work and all future research dedicated to strengthening the protection of societies, states, and the dignity of human life.

References - Proposed Literature

Trifunović, D., & Kazansky, R. (2021). *Conflict theory – One of the theoretical foundations of security science.* International Strategic Studies Association. ISBN 978-1-892998-22-4.

Trifunovic, D. (2024). The New Craft of Intelligence: Information Operations and Cyber Security. In: Besenyő, J., Khanyile, M.B., Vogel, D. (eds) Terrorism and Counter-Terrorism in Modern Sub-Saharan Africa. African Histories and Modernities. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-56673-8_9

Dragnea, Mihai; Fitsanakis, Joseph; Trifunovic, Darko; Nomikos, John; Stamevski, Vasko; and Cupcea, Adriana, "Aspects of Islamic Radicalization in the Balkans After the Fall of Communism" (2023). *CCU Faculty Books*. 37.
https://digitalcommons.coastal.edu/faculty-books/37

Piwowarski, J., & Trifunović, D. (2023). *From security science to security culture.* RIEAS – Research Institute for European and American Studies; INIS – Institute for National and International Security.

Trifunovic, D., & Dragišić, Z. (2022). The Security Intelligence System of the Republic of Serbia. International Journal of Intelligence and CounterIntelligence, 35(2), 353–373. https://doi.org/10.1080/08850607.2021.2022429

Trifunović, D. (2014). Security studies-synthesis between academy and practice. Contemporary Military Challenges, Slovenian Ministry of Defence. https://dk.mors.si/info/images/SVI/PDF/2014_2/trifunovic.pdf

Trifunović, D**.** (2025). *Intelligence and counterterrorism. National Security and the Future, 26*(1). https://doi.org/10.37458/nstf.26.1.7

Baldwin, D. A. (1997). The concept of security. Review of International Studies

Booth, K. (2007). Theory of world security. Cambridge University Press.

Kolodziej, E. A. (2005). *Security and international relations*. Cambridge University Press.

Collins, A**.** (Ed.). (2007). *Contemporary security studies*. Oxford University Press.