Original scientific paper

UDK 355.358.014:355.01 DOI 110.7251/DEFEN2559093K COBISS.RS-ID 142735873

ANALYSIS OF THE APPLICABILITY OF CLAUSEWITZIAN FRICTION THEORY IN MODERN HYBRID WARFARE

Slaven Knežević, MA[1]

Abstract: This article explores Clausewitz›s understanding of friction in military theory through the lens of contemporary asymmetric and hybrid conflicts, demonstrating how this concept has transformed from primarily a physical and tactical phenomenon into a multidimensional construct encompassing informational, cognitive, organizational, and strategic aspects. The research methodology combines historical analysis of Clausewitz›s original concept with empirical findings from contemporary conflicts and a multidisciplinary approach that integrates military, sociological, psychological, and technological perspectives. The article›s objective is to develop a new theoretical paradigm that can adequately encompass the complexity of friction in the digital age through identification, categorization, and analysis of new sources and manifestations of friction characteristic of the contemporary operational space. The findings provide a significant contribution to military theory and practice through redefining the classical concept of friction in a way that can inform more effective doctrine, training, and organization of military forces for navigating through the complexity of contemporary conflicts.

Keywords: *Clausewitz, friction, hybrid warfare, asymmetric conflicts, information domain, cyber operations*

1 PhD student at the Faculty of Political Sciences, University of Banja Luka. Correspondence: slaven.knezevic998@gmail.com

1. CONCEPTUALIZATION OF FRICTION IN CLAUSEWITZIAN MILITARY THEORY

Carl von Clausewitz,[2] a Prussian general and one of the most significant military theorists of all time, in his magnum opus "On War" (*Vom Kriege*) published posthumously in 1832, introduced the concept of "friction" (*Friktion*)[3] which remains fundamental to understanding the dynamics of armed conflicts even today, nearly two centuries later. The conceptualization of friction in Clausewitzian military theory represents one of his most original contributions to strategic thought and requires detailed consideration of the historical context in which it emerged, as well as analysis of the fundamental principles upon which it rests.

Clausewitz's understanding of war was not the product of purely theoretical considerations, but was deeply rooted in his personal experience during the Napoleonic Wars. As an officer in the Prussian army, Clausewitz witnessed the defeat at Jena and Auerstedt in 1806, participated in the Rus-

2 Carl von Clausewitz (*Carl Philipp Gottfried von Clausewitz*) was born on June 1, 1780, in Burg near Magdeburg, and died on November 16, 1831, in Breslau (now *Wrocław*) of cholera. As a Prussian general and military theorist, Clausewitz served in the Prussian-Russian campaigns against Napoleon (1812-1815), was chief of staff of the Prussian Military Academy, and director of the *Kriegsakademie* in Berlin from 1818 to 1830. His magnum opus "On War" (*Vom Kriege*) remained unfinished due to his premature death, and was posthumously published by his wife Marie von Clausewitz (*Marie von Clausewitz*) in 1832, who edited the manuscripts he had worked on during the last twelve years of his life. Although Clausewitz was unable to complete the envisioned revision of his work, "On War" has been recognized as one of the most influential works of military theory in history, becoming the foundation of strategic thinking in many military academies around the world.

3 In the original German text of Clausewitz's work *Vom Kriege*, the author uses the term *Friktion* for a concept that translates into Serbian as "trenje" (friction). Clausewitz deliberately borrows this term from mechanics, creating a powerful metaphor that depicts the forces that oppose the smooth conduct of military operations. A nuance that is sometimes lost in translation is that *Friktion* in German carries a stronger connotation of mechanical resistance and physical interaction than the word "trenje" often conveys in our language. Regarding the frequently cited phrase "fog of war", it is interesting that Clausewitz never literally used the term *Nebel des Krieges* (which would be a direct translation), but rather spoke of "uncertainty" (*Ungewissheit*) and a phenomenon similar to "twilight" or "half-light" (*Halblicht*). The concept of "fog of war" was developed through interpretations and adaptations of Clausewitzian thought, becoming a powerful metaphor for uncertainty and incompleteness of information in wartime conditions.

sian campaign against Napoleon, and was present in the Waterloo campaign of 1815. Such experiences provided him with a unique perspective on the gap between military plans and their realization on the battlefield. As Paret notes: „Clausewitz's experience of warfare against Napoleonic France shaped his theoretical thought in a way that cannot be separated from his analysis of friction in war" (Paret, 1985:142). It was precisely in this gap between theory and practice, between plan and execution, that Clausewitz identified the phenomenon he called "friction". In attempting to explain why military operations rarely unfold according to plan, Clausewitz coined one of his most famous analogies: „Everything in war is very simple, but the simplest things become extremely difficult. Difficulties accumulate and create a kind of friction that is hard to imagine for those who have not experienced war" (Clausewitz, 1976:119). This metaphor of friction, borrowed from mechanics, served as a perfect illustration of forces that oppose the smooth conduct of military operations. Just as friction in mechanics slows down movement, so friction in war complicates the implementation of military plans.

Clausewitz's conceptualization of friction was not merely descriptive, but also analytical. He identified various sources of friction, among which the unreliability of information, physical efforts and limitations, unpredictability, fear and uncertainty particularly stand out. According to Clausewitz: „The reports that are received in war are mostly contradictory, even more are false, and the greatest part are uncertain... In short, most reports are false, and the fear of men increases lies and untruths" (Clausewitz, 1976:117). Such observation about the "fog of war" (*Nebel des Krieges*) became one of the key aspects of his understanding of friction. In considering Clausewitz's theory of friction, it is important to view the historical context in which it emerged. The period after the French Revolution marked a fundamental transformation in the way of warfare, where mass armies of nation-states replaced the smaller, professional armies of the previous period. As Howard (1983) emphasizes: „Clausewitz's understanding of friction partly arose from his observation of how traditional armies faced new challenges of mass mobilization and logistics brought by the Napoleonic way of warfare" (Howard, 1983:78). Indeed, with the increase in army size and operational complexity, the friction that commanders had to deal with also increased.

The fundamental principles of Clausewitz's theory of friction can be better understood through his tripartite division of war. Clausewitz conceptualized war through three levels: rational (linked to political objectives), irrational (linked to chance and probability), and non-rational (linked to emotions and passion). Friction is primarily located in the irrational sphere of war, where chance, unpredictability, and probability play a key role. According to Summers' interpretation: „Clausewitz's brilliance lies in understanding that war is not governed only by rational calculation, but also by elements that cannot be easily quantified - friction and chance are among the most important" (Summers, 1992:54). One of the greatest contributions of Clausewitz's theory is the recognition that friction is an inevitable characteristic of war, not an anomaly that can be eliminated through better planning. As Clausewitz himself emphasizes: "Friction is the only concept that generally corresponds to what distinguishes real war from war on paper" (Clausewitz, 1976:121). The distinction between "ideal" and "real" war has profound implications for military theory and practice. As Echevarria (2007) points out: „Clausewitz's insistence on friction as a fundamental characteristic of war represented a direct challenge to the Enlightenment belief that war could be reduced to rational formulas and geometric principles" (Echevarria, 2007:112). It is important to note that Clausewitz did not consider friction only as an obstacle to be overcome, but also as a phenomenon that could be exploited against the enemy. The ability to function despite friction - or to create friction for the opponent - became a key element of military skill. In this context, Clausewitz introduces the concept of "military genius" as a leader who possesses the intuition and character needed to navigate through the friction of war. According to Clausewitz: „Genius in war is nothing other than an exceptional ability to remain composed in an atmosphere of danger and uncertainty, from which comes the greater part of friction" (Clausewitz, 1976:124).

Clausewitz's theory of friction can also be viewed in the context of his broader theory of "absolute" and "real" war. While absolute war is a theoretical construct that implies escalation of violence to the extreme limits, real war is limited by numerous factors - and friction is one of the most significant. As van Creveld notes: „Clausewitz's distinction between absolute and real war is actually an acknowledgment of the in-

fluence of friction in limiting the theoretical possibilities of conflict escalation" (Creveld, 1991:98). The distinction was crucial for avoiding purely abstract theories that would have no practical application. One of the most interesting characteristics of Clausewitz's theory of friction is its dialectical nature. Namely, friction is not only a product of material factors such as weather, terrain, or logistics, but also of the human factor - both one's own forces and the enemy. What is particularly significant in Clausewitz's analysis is the recognition of the interactive nature of friction -- enemy actions create friction, but the very presence of the enemy creates psychological friction through fear and uncertainty. As Watts (2004) notes: „Clausewitz's greatest achievement was recognizing that friction is not just the result of physical circumstances, but also of complex interaction between opposing wills" (Watts, 2004:76).

The network of conditionalities created by friction leads to Clausewitz's concept of „centers of gravity" (*Schwerpunkt*), which represents the point where enemy power is concentrated, but also the point of greatest vulnerability. As Strange emphasizes: „Clausewitz's theory of centers of gravity directly derives from his analysis of friction -- identification of centers of gravity enables commanders to direct their efforts to critical points where created friction could have decisive influence" (Strange, 1996:103). The presented approach emphasizes economy of force and precise targeting of efforts, instead of simple accumulation of resources. Clausewitz's understanding of friction also contributed to his concept of "culminating point of victory" - the moment when offensive force reaches maximum efficiency before friction begins to dominate and reduce its effectiveness. According to Clausewitz: „In every military operation, once the culminating point is passed, friction and resistance become so great that further advance becomes counterproductive" (Clausewitz, 1976:198). Such observation has significant implications for operational planning and articulation of limited objectives.

The implications of Clausewitz's theory of friction for military practice were far-reaching: it encouraged the development of the concept of *Auftragstaktik* (mission command)[4] in the Prussian army, later

4 Clausewitz's theory of friction had a profound impact on the development of the German

the German *Wehrmacht*, where subordinate officers received greater autonomy so they could adapt plans to the friction they encountered in the field. As Keegan emphasizes: „The Prussian-German acceptance of Clausewitz's concept of friction led to decentralization of command that enabled greater flexibility at the tactical level - a direct response to the uncertainty created by friction in war" (Keegan, 1993:167). Clausewitz's conceptualization of friction in military theory represents one of the most significant contributions to strategic thought. His recognition of the gap between theory and practice, between ideal plan and actual execution, fundamentally changed the way war is thought about. As Gray emphasizes: „Perhaps no other aspect of Clausewitz's theory is as relevant to contemporary understanding of war as his concept of friction - it represents a bridge between abstract theories and actual challenges of command" (Gray, 1999:143). Clausewitz's theory of friction remains vitally relevant even in the contemporary age of technology and information, reminding us that war, in its essence, is a human endeavor marked by uncertainty, complexity, and friction.

---

concept of *Auftragstaktik*(mission-type command), which became the foundation of Prussian and later German military doctrine. Recognizing the inevitability of friction and "fog of war" on the battlefield, Prussian military reformers under the leadership of Helmuth von Moltke the Elder developed a command system that emphasized decentralization of decision-making and initiative among subordinate officers. Instead of detailed orders prescribing every aspect of execution, *Auftragstaktik* emphasizes clearly defining intent (the so-called *Commander's Intent*) and the desired end state, leaving subordinates free to decide for themselves how to accomplish the assigned mission. This approach is a direct adaptation to Clausewitz's observation that centralized command becomes less effective as friction increases, since plans rarely survive first contact with the enemy. Through two German military academies (*Kriegsakademie*), Clausewitzian thought on friction was integrated into officer training, emphasizing the need for adaptability, independence, and rapid decision-making at all levels. The successes of the Prussian army against Austria (1866) and France (1870-71) demonstrated the effectiveness of this approach, cementing the influence of Clausewitz's theory on German military doctrine. The modern German military (*Bundeswehr*) still applies this concept under the name *Führen mit Auftrag* (leading through mission), while many other military forces, including the US and NATO, have adopted similar approaches as an adaptation to the friction of modern warfare. Through the doctrine of *Mission Command*, the US Armed Forces explicitly acknowledge their intellectual debt to Clausewitz's understanding of friction and uncertainty, demonstrating the lasting influence of his ideas on contemporary military thinking.

2. HYBRID WARFARE AS A COMPLEX OPERATIONAL SPACE

Contemporary conflicts[5] increasingly take on the characteristics of hybrid warfare, a phenomenon that combines conventional military operations with unconventional tactics, cyber attacks, information operations, economic pressures, and other means of power projection. The evolution in warfare methodology has significantly transformed the nature of conflicts, creating a more complex operational space that generates new sources and manifestations of "friction" in the Clausewitzian sense. As Hoffman emphasizes: „Hybrid warfare incorporates different models of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts and criminal behavior, creating a multimodal operational space of unprecedented complexity„ (Hoffman, 2007:14). Such complexity creates fertile ground for the emergence of new forms

5 The Russian-Ukrainian conflict (Knežević, 2025) represents an exceptional demonstration of Clausewitz's concept of friction in a contemporary context, showing how this theoretical principle evolves and acquires new dimensions. The traditional sources of friction that Clausewitz identified - unreliability of information, physical limitations, and unpredictability - manifest in this conflict, but in transformed forms that reflect the complexity of modern warfare. Informational friction manifests through massive disinformation campaigns that create a "digital fog of war" that makes it difficult to distinguish reality from propaganda, both for military leaders and civilian populations. Physical friction is visible through the logistical challenges faced by Russian forces in the early phases of the Special Military Operation, demonstrating how even technologically advanced armies succumb to classical limitations of terrain, time, and endurance. Operational friction arises *through the discord between doctrine and actual circumstances on the battlefield*, which was evident when Russian forces applied tactics designed for rapid conventional victories in a prolonged conflict that requires a different approach. Organizational friction manifests through rigid hierarchical structures that hinder adaptation to changing circumstances, which was particularly visible in the first months of the war. Strategic friction arises through the discord between political objectives and military means, where expected rapid victory gives way to prolonged attritional conflict with unclear prospects for decisive success. Technological friction is visible through the limitations of sophisticated weapons systems in complex operational environments, including challenges posed by simpler and cheaper systems like drones. Cognitive friction manifests through erroneous assumptions about the motivation and endurance of the adversary, which has led to significant strategic miscalculations on both sides. Diplomatic friction arises through complex international relations and interactions that limit the options available to the warring parties, particularly in the context of nuclear deterrence and economic sanctions. Legitimacy friction demonstrates how the perception of justice and justification of the conflict affects support, mobilization, and endurance, creating a unique dynamic that transcends mere material calculation.

of friction that significantly differ from those Clausewitz described in his work "On War".

Hybrid warfare presents a challenge to traditional understanding of friction primarily because of its intrinsic multidimensionality. Unlike conventional conflicts where front lines are relatively clear, hybrid conflicts occur simultaneously through multiple domains - physical, informational, cognitive, cyber, and others - with each domain possessing its own unique characteristics that generate specific forms of friction. According to McCulloh and Johnson: „Hybrid warfare deliberately blurs the boundaries between different domains of conflict, creating a situation where friction appears not only within individual domains, but also at their overlaps and interfaces" (McCulloh & Johnson, 2013:32). This overlap of different operational domains significantly complicates the problem of friction, as it requires synchronization of activities that are subject to different dynamics and limitations. In the context of hybrid warfare, the information sphere becomes a particularly significant source of friction. The massive proliferation of information technologies and social media has created an environment in which information moves at incredible speed, creating what Cronin calls an "information tsunami" that significantly complicates distinguishing facts from disinformation. As Cronin emphasizes: „In hybrid conflict, information overload and intentional manipulation of information create a new kind of 'fog of war' that is denser and more persistent than the one commanders faced in Clausewitz's time" (Cronin, 2020:87). Digital "fog of war" presents a fundamental challenge for decision-makers, as it undermines the ability to form an accurate picture of the situation that is necessary for effective command.

The cyber domain of hybrid warfare also represents a rich source of new forms of friction. Traditionally, friction in warfare was limited by the physical laws of the material world - terrain, weather, logistics, and human limitations. However, cyberspace possesses its own laws and dynamics that create new and unpredictable forms of friction. As Libicki notes: „Cyber friction is not simply an extension of physical friction into the digital sphere, but a fundamentally new phenomenon arising from the unique characteristics of cyberspace - its inhomogeneity, asymmetry,

instability, and unpredictability" (Libicki, 2012:178-179). For example, latency in network communications, software bugs, system compatibility, and cyber attacks represent new forms of friction that have no direct analogies in the physical domain, but can have equally significant or even more important impact on the outcome of operations.[6]

The asymmetric nature of hybrid warfare additionally contributes to creating new forms of friction. In hybrid conflicts, state and non-state actors often possess drastically different capabilities, motivations, and operational approaches, creating asymmetric interactions that generate friction in unexpected ways. As Kilcullen emphasizes: „Asymmetry in hybrid conflict is not just a matter of disproportion in military power, but fundamental differences in operational logic and strategic thinking, creating 'conceptual friction' that is often harder to overcome than

6 The *NotPetya* attack from 2017 represents an exceptional example of "cascading friction" in the digital domain, where malware initially targeted at Ukrainian companies caused global consequences through unexpected chains of interdependence, resulting in over $10 billion in damages to multinational companies such as *Maersk*, *FedEx*, and *Merck*. The Russian attack on Ukraine's electrical grid in 2015 and 2016 demonstrates „operational asymmetry friction", where attackers exploited the disparity between high-tech components of critical infrastructure and the limited *cyber*-security capabilities of operators, successfully cutting power to hundreds of thousands of citizens. Operation *Olympic Games* (Stuxnet) against Iran's nuclear program illustrates "epistemological uncertainty friction", where Iranian engineers were faced for months with inexplicable centrifuge failures, inability to reliably determine the cause, and uncertainty about the authenticity of data displayed by their control systems. The *SolarWinds* attack discovered in 2020 shows "cumulative complexity friction", where a sophisticated supply chain-compromised software component enabled access to systems of over 18,000 organizations, including numerous US government agencies, demonstrating how technological interdependence creates new vectors of friction. DDoS attacks against Estonian digital infrastructure in 2007 illustrate "temporal asymmetry friction", where relatively simple attacks caused disproportionately long-lasting consequences due to society's dependence on digital services, creating friction that manifested through economic and social effects long after the attacks themselves ceased. The leak campaign against the Democratic National Committee during the 2016 US presidential election shows "information asymmetry friction", where strategically timed release of compromised data created disproportionate effects on the information environment and voter decision-making processes. The *WannaCry ransomware* attack from 2017, which hit Britain›s healthcare system (NHS), demonstrates "technical debt friction", where outdated but critical systems created vulnerabilities that enabled malware spread through key infrastructure, resulting in the cancellation of thousands of medical procedures. These examples clearly illustrate how cyber attacks create new forms and manifestations of friction that transcend Clausewitz's original understanding, but remain faithful to his fundamental concept of factors that create a gap between plan and realization.

purely physical friction" (Kilcullen, 2013:56). Such "conceptual friction" arises when actors operate according to different rules and logics, making it difficult to predict their actions and adequately respond to them. Ambiguity and intentional indeterminacy represent another characteristic source of friction in hybrid warfare. Unlike conventional conflicts where identification of the enemy and their intentions is relatively clear, hybrid warfare is characterized by deliberate obfuscation of responsibility and denial of involvement. Gerasimov, a Russian general whose ideas are often associated with the concept of *Gerasimov Doctrine*, emphasizes: „The boundaries between war and peace are becoming increasingly blurred. Wars are no longer declared, and when they begin, they do not follow the pattern we are accustomed to" (Gerasimov, 2013:24). This ambiguity creates significant friction in decision-making processes, as decision-makers must act under conditions of prolonged uncertainty regarding the identity, intentions, and objectives of the opponent.

Hybrid warfare is also characterized by a high degree of nonlinearity, which represents a significant source of new friction. Nonlinearity implies that small actions can have disproportionately large effects, that cause-and-effect relationships are not always obvious, and that systems can show emergent behavior that cannot be predicted based on their individual components. As Bousquet emphasizes: „The nonlinearity of hybrid conflicts creates a fundamentally different kind of friction from that which Clausewitz described - friction that arises not only from physical obstacles or human limitations, but from the inherent unpredictability of complex adaptive systems" (Bousquet, 2009:203). Nonlinearity is particularly pronounced in the information sphere, where memes or viral content can rapidly escalate and have strategic impact that is disproportionate to their initial significance. In hybrid warfare, friction increasingly manifests through the cognitive dimension. Hybrid operations often target perceptions, attitudes, and beliefs of targeted populations, creating what some theorists call *cognitive friction*. According to Lawrence Freedman: „The primary goal of many hybrid campaigns is not physical destruction, but cognitive disintegration - creating confusion, uncertainty, and decision paralysis through manipulation of perceptions" (Freedman,

2017:242). The cognitive aspect of friction is particularly important in the context of democratic societies, where public opinion and perception of legitimacy have significant influence on strategic decisions. The temporal dimension of friction also takes on new forms in hybrid warfare. While Clausewitz was primarily focused on short-term friction that manifests during active combat operations, hybrid warfare often includes long-term low-intensity campaigns that create what we might call *chronic friction*. As Freedman notes: „Hybrid campaigns are often designed to cause long-term exhaustion of the opponent through persistent but tolerable friction that over time erodes the will and ability to resist" (Freedman, 2017:73). The temporal dimension of friction represents a particular challenge for democratic societies that often have limited political will for long-term low-intensity conflicts.

One of the most interesting characteristics of hybrid warfare is the ability of actors to deliberately create and exploit friction. While Clausewitz saw friction primarily as a natural phenomenon arising from the inherent characteristics of war, in hybrid warfare friction becomes an operational objective - something that is deliberately provoked to disrupt the functionality of opposing systems. According to McKenzie: „Creating systemic friction in opposing decision-making processes, operational cycles, and strategic calculations has become an explicit goal of hybrid operations, especially those conducted by actors aware of their inferiority in conventional military power" (McKenzie, 2016:112). The instrumentalization of friction represents a significant evolution from Clausewitz's original understanding of this concept. The integration of civilian and military means in hybrid warfare also creates new sources of friction through complex command chains and complex administrative structures.[7] Gray

7 Multinational corporations and private military companies (PMCs) introduce a new dimension of friction in great power relations through the creation of "hybrid actors" that operate in the gray zone between state and non-state action. Corporations such as technology giants control critical digital infrastructure that transcends national borders, creating *sovereignty friction* where the state no longer has complete control over key elements of its national power. Private military companies such as Russia›s *Wagner* or America›s former *Blackwater* (now *Academi*) enable states to project military power with *deniability friction*, maintaining strategic ambiguity about their involvement in conflicts. These entities often act as intermediaries in conflicts between great powers, enabling escalatory actions without formally cross-

observes: "Hybrid warfare requires coordination between traditionally separated government agencies, military components, private companies, and other actors, creating organizational friction that can be as significant as operational friction in the field" (Gray, 2017:98). The administrative dimension of friction is particularly problematic in societies with strict separation between civilian and military structures, where institutional culture and legal frameworks can complicate effective coordination and integrated response.

Technological proliferation in the context of hybrid warfare has a dual impact on friction. On one hand, advanced technologies can reduce certain traditional sources of friction - satellite systems reduce uncertainty regarding terrain, advanced communication systems enable faster information transfer, and automated systems can eliminate human errors. However, on the other hand, technology creates new forms of dependencies and vulnerabilities that generate new forms of friction. As Singer emphasizes: „Technological sophistication creates an illusion of reduced friction, but actually only transforms its nature - from direct physical obstacles to complex cascading failures in interconnected technological systems" (Singer, 2009:234). The transformation of the nature of friction through technology represents one of the most significant challenges for military planners and commanders in the hybrid operational environment. Legal and normative aspects also represent a significant source of new friction in hybrid warfare. Actors conducting hybrid operations often deliberately operate in "gray zones" of international law, choosing tactics that are sufficiently ambivalent to complicate clear legal qualification and adequate response. According to Whither (2016): „Hybrid actors exploit conceptual and legal gaps between war and peace, military and civilian activities, creating 'legal friction' that complicates formulating a coherent and legitimate response" (Whither, 2016:67). Such *legal friction* is particularly problematic for liberal

ing thresholds that would provoke direct confrontation, thereby creating *escalation control friction*. As Singer (2008) observes, these non-state actors create asymmetric relationships of responsibility and transparency, where their activities produce strategic effects but without the traditional mechanisms of oversight and control that exist with state actors, further increasing uncertainty and complexity in the geopolitical environment.

democracies that are bound by the rule of law and often have rigorous restrictions regarding the use of force in situations that are not clearly qualified as armed conflict.

The psychological dimension of friction in hybrid warfare manifests through what Waltz calls *anxiety of uncertainty*. According to his view: „Hybrid threats generate a special kind of psychological friction through their ambivalence and multiplicity - the feeling that threat can come from any direction, in any form, at any moment, creating psychological exhaustion and anxiety that degrades decision-making effectiveness" (Waltz, 2018:156). The psychological dimension of friction can have profound implications for strategic planning and operational execution, as it affects cognitive processes that are at the basis of decision-making at all levels. Hybrid warfare as a complex operational space creates numerous new sources and manifestations of friction that significantly exceed the framework established by Clausewitz. Multidimensionality, information saturation, cyber specificities, asymmetry, ambiguity, nonlinearity, cognitive dimension, temporal extension, deliberate instrumentalization, organizational complexity, technological transformations, legal ambivalences, and psychological factors - all contribute to creating a new topography of friction that requires fundamental reconsideration of traditional approaches to military planning and execution of operations. As Hammes emphasizes: „Understanding new forms of friction in hybrid warfare is not just an academic question, but an imperative for effective strategic thinking in the 21st century - without such understanding, military planners and decision-makers risk applying inadequate conceptual models to contemporary challenges" (Hammes, 2016:312). The transformation of the nature of friction represents one of the most significant challenges facing military organizations in the process of adapting to the realities of the contemporary security environment, requiring not only technical and organizational innovations, but also fundamental reconsideration of the conceptual foundations of strategic thinking.

3. METHODOLOGICAL FRAMEWORK FOR ANALYZING FRICTION IN THE INFORMATION AND CYBER DOMAIN OF CONTEMPORARY CONFLICTS

The analysis of the friction phenomenon[8] in contemporary conflicts requires the development of a robust methodological framework that can adequately encompass all the complexities of the information and cyber domain. Clausewitz's original conceptualization of friction emerged in the context of the industrial era and physical battlefield, where sources of friction were primarily of material nature - weather, terrain, logistics, fatigue, and fear. However, the information age has brought fundamentally new dimensions of conflict that require reconsideration and enhancement of the traditional methodological apparatus. As Arquilla notes: „The digital revolution has not only transformed weapons and warfare tactics, but has created completely new domains of conflict and associated forms of friction that require new analytical approaches and methods" (Arquilla, 2012:27). The development of an adequate methodological framework for analyzing friction in the information and cyber domain therefore represents not only academic interest, but also practical necessity for understanding the dynamics of contemporary conflicts.

The information and cyber domains possess unique characteristics that significantly complicate the development of a coherent methodol-

8 The empirical analysis presented in this article relies on several complementary data sources that enable triangulation of findings and increase their reliability. Primary quantitative data on asymmetric conflict outcomes were drawn from the *Correlates of War* (COW) database covering interstate and intrastate conflicts from 1816 to 2021, and from the UCDP/PRIO *Armed Conflict Dataset* which provides more detailed data on low-intensity conflicts. For analysis of specific manifestations of friction in hybrid conflicts, data from the *Global Terrorism Database* (GTD) and the ACLED (*Armed Conflict Location & Event Data*) project were used, enabling geographically precise analysis of incidents and tactics. Qualitative data on organizational, cognitive, and strategic dimensions of friction were collected from published memoirs of military commanders, official post-operational reports, and compiled interviews with veterans of asymmetric conflicts. For the cyber domain, reports from private cybersecurity companies (*Mandiant, CrowdStrike, ESET*) were analyzed, along with academic case studies of documented cyber attacks and unclassified reports from government agencies such as US-CERT and EU CERT. All empirical data were categorized according to a developed analytical framework that enables systematic coding of different manifestations of friction across multiple domains, thereby creating a foundation for comparative analysis and pattern identification.

ogy for friction analysis. Unlike the physical domain where the laws of physics are constant and predictable, digital space is characterized by extreme instability, inhomogeneity, and constant evolution. As Libicki observes: „Cyberspace is not a natural phenomenon with unchanging laws, but a human creation that is constantly changing - this fluidity presents a fundamental methodological challenge for any analysis of friction in that domain" (Libicki, 2016:43). Additionally, the multidimensionality of the information and cyber domain creates the problem of conceptualizing the space itself in which friction manifests - whether it is physical infrastructure, logical layer of networks, semantic content, or cognitive effects on human operators and targeted populations. One of the fundamental methodological challenges in analyzing friction in the information and cyber domain is defining and operationalizing the very concept of friction in this context. While Clausewitz defined friction as „that which distinguishes real war from war on paper," in the digital domain the boundaries between "real" and "paper" (i.e., theoretical) become much more blurred. Singer and Friedman offer the following definition of digital friction: „Cyber friction represents the totality of factors that degrade, slow down, or otherwise impede the ideal performance of digital systems and decision-making processes based on information from those systems" (Singer & Friedman, 2014:132). The definition, although useful as a starting point, requires further elaboration through the development of concrete indicators and metrics that would enable systematic measurement and comparison of friction in different contexts. In developing a methodological framework for analyzing friction in the information and cyber domain, it is necessary to take into account the multidisciplinary nature of this phenomenon. As Gartzke emphasizes: „Adequate analysis of cyber conflicts requires methodologies that integrate insights from computer science, cybernetics, systems theory, cognitive psychology, organizational theory, and traditional military-strategic thought" (Gartzke, 2013:67). Multidisciplinarity represents a significant methodological challenge, but also an opportunity for developing integrated analytical approaches that overcome the limitations of traditional, disciplinarily fragmented methodologies.

Systematic analysis of friction in the information and cyber domain requires the development of a typology that would enable classification

of different forms of friction. Based on extensive analysis of contemporary cyber conflicts, Valeriano and Maness propose the following typology of cyber friction: „technological friction (arising from imperfections and incompatibilities of technological systems), human-cognitive friction (arising from human interaction with technology), organizational friction (arising from institutional structures and processes), and strategic friction (arising from interaction of different actors in cyberspace)" (Valeriano & Maness, 2018:109). Such typology represents a useful analytical tool, but requires further refinement through the development of specific indicators for each category of friction. Quantification of friction in the information and cyber domain presents a special methodological challenge. Unlike certain aspects of physical friction that can be directly measured (e.g., time needed to move troops), digital friction often has qualitative dimensions that are difficult to precisely quantify. Kello proposes a multidimensional approach to measuring cyber friction through a combination of technical metrics (such as system response time, error rate, network throughput), organizational indicators (decision time, coordination effectiveness), and psychological parameters (cognitive load, stress, perceptual distortions). „Quantification of cyber friction", claims Kello, „requires a combination of objective metrics and qualitative assessments that together can provide holistic insight into the actual impact of friction on operational effectiveness" (Kello, 2017:211).

The temporal dimension represents another significant aspect of the methodological framework for analyzing friction in the information and cyber domain. Unlike traditional friction that manifests primarily synchronously during active operations, digital friction often has a diachronic dimension - effects can accumulate over longer periods or manifest with significant time delays. As Lindsay observes: „The temporal dimension of cyber friction requires methodological approaches that can encompass both immediate effects and their evolution through time, including cascading effects and emergent phenomena that can manifest days or even months after the initial event" (Lindsay, 2015:78). Temporal complexity requires longitudinal studies and developmental models that can track the evolution of friction through different phases of cyber conflict. Epistemological challenges additionally complicate the development of a method-

ological framework for analyzing friction in the information and cyber domain. The problem of attribution - reliable determination of the source of certain cyber activity - represents a fundamental limitation for empirical analysis. Buchanan emphasizes: „Attribution insecurity creates epistemological friction that complicates precise analysis of cyber conflict dynamics - even when we have detailed technical data about an incident, we often cannot determine with certainty who is responsible, with what intention, and with what strategic goal" (Buchanan, 2020:143). Epistemological uncertainty has direct implications for methodological design - it requires approaches that can operate under conditions of high uncertainty and incorporate probabilistic assessments instead of deterministic conclusions. The development of effective methodology for analyzing friction in the information and cyber domain is additionally complicated by the problem of access to relevant data. The most sophisticated cyber incidents often remain classified, and states and organizations rarely share detailed information about their vulnerabilities and operational limitations. Rid and Buchanan emphasize this problem: „Cyber conflict analysts face a fundamental methodological challenge - the most relevant data for understanding friction dynamics are often unavailable due to operational secrecy, while publicly available data are often incomplete or misleading" (Rid & Buchanan, 2015:32). Such limitation requires the development of innovative methodological approaches that can generate significant insights even from incomplete data, including techniques such as triangulation of different sources, extrapolation from available data, and development of theoretically informed models that can fill empirical gaps.

For complex analysis of friction in the information and cyber domain, it is necessary to combine different methodological approaches. Quantitative methods such as network analysis, statistical modeling, and simulations can provide insight into structural aspects of friction, while qualitative methods such as case studies, in-depth interviews, and ethnography can illuminate contextual and interpretive dimensions. Smith advocates *methodological pluralism* in this area: „Understanding friction in the digital age requires a combination of computational, mathematical, social-scientific, and humanistic methodologies - each illuminates differ-

ent aspects of this multidimensional phenomenon" (Smith, 2018:218). An integrative approach enables the development of holistic understanding of friction that transcends the limitations of individual methodological traditions. The operationalization of Clausewitz's concept of "fog of war" (*Nebel des Krieges*) in the context of the information and cyber domain presents a special methodological challenge. Traditionally understood as uncertainty arising from incomplete, inaccurate, or outdated information on the battlefield, "fog of war" in the digital age takes on new dimensions. Perlroth describes this phenomenon as "digital fog" that arises not only from lack of information, but also from their abundance: „The paradox of the digital age is that increased quantity and speed of information often creates greater, not lesser uncertainty - analytical systems and human operators become overloaded, making it difficult to distinguish signal from noise" (Perlroth, 2021:289). The methodological framework for friction analysis must therefore include techniques for assessing information overload and its effects on decision-making processes.

For adequate analysis of friction in the information and cyber domain, it is necessary to develop a methodology that can encompass the human factor, especially cognitive and psychological dimensions. Kahneman, Sibony, and Sunstein (2021) emphasize the importance of understanding cognitive biases in cyber friction analysis: „Digital friction is not only a technical phenomenon, but also cognitive - the way the human mind processes uncertainty, risk, and complexity in the digital environment creates unique forms of friction that often have greater operational impact than purely technical limitations" (Kahneman, Sibony & Sunstein, 2021:176). Methodologically, this requires integration of experimental approaches from cognitive psychology, including tests for assessing cognitive load, attention, risk perception, and decision-making under pressure. The methodological framework for analyzing friction in the information and cyber domain must also address the problem of emergence - the appearance of behavior at the system level that cannot be predicted based on the characteristics of individual components. As Jervis emphasizes: „Complex cyber-physical systems are characterized by nonlinear interactions that can generate emergent friction - forms of operational limitations that cannot be anticipated even with complete un-

derstanding of individual system components" (Jervis, 2017:112). Methodologically, analysis of emergent friction requires approaches based on complexity theory, including agent-based modeling, system dynamics, and chaos theory, which can encompass nonlinear interactions and self-organizing system behavior. The development of effective methodology for analyzing friction in the information and cyber domain is additionally complicated by the problem of *interdomain interactions*. Friction rarely manifests exclusively in one domain - more often it involves complex interactions between cyber, informational, cognitive, social, and physical dimensions. As Demchak (2018) emphasizes: „A methodological approach that treats cyber friction as an isolated phenomenon will inevitably miss key interdomain effects that often have decisive influence on operational outcomes" (Demchak, 2018:89). This requires the development of integrated analytical frameworks that can track cascading effects through different domains and identify critical points where friction in one domain amplifies or transforms friction in others.

One of the most significant methodological innovations in cyber friction analysis is the application of *resilience theory*. Unlike the traditional approach that focuses primarily on identifying and preventing friction, the resilience perspective emphasizes the system's ability to absorb friction and maintain functionality despite operational limitations. Linkov and Trump define resilience in the cyber context as „the ability of systems to anticipate, absorb, adapt to, and recover from events that produce friction, while preserving critical functionalities" (Linkov & Trump, 2019:54). Methodologically, this requires the development of metrics for measuring system resilience to different forms of friction, including indicators such as robustness, redundancy, adaptability, and recovery speed. The integration of qualitative and quantitative methods represents a key aspect of the methodological framework for analyzing friction in the information and cyber domain. Quantitative metrics such as system response time, error rates, or traffic density can provide objective indicators of technical friction, but cannot adequately encompass subjective and contextual dimensions such as perceived uncertainty, organizational culture, or strategic context. As Gompert notes: „The real strength of methodology for analyzing cyber friction comes from integrating quan-

titative metrics that can precisely measure technical dimensions with qualitative approaches that can illuminate human, organizational, and strategic factors" (Gompert, 2016:133). Integration of different methodological approaches enables the development of holistic understanding of friction that transcends the limitations of individual metrics or analytical frameworks. For effective analysis of friction in the information and cyber domain, it is necessary to develop a methodology that can encompass different levels of analysis - from the technical level of individual systems, through tactical and operational levels, to strategic and policy levels. Betz and Stevens (2013) emphasize the importance of this multi-level approach: „Understanding cyber friction requires integrated analysis that connects the micro-level of technical incidents with the macro-level of strategic implications, identifying how friction transforms and amplifies through different levels" (Betz & Stevens, 2013:147). Methodologically, this requires the development of approaches that can connect technical incidents with their operational effects and strategic implications, instead of treating these levels as separate analytical domains (Knežević, 2025).

Comparative analysis represents another important element of the methodological framework for understanding friction in the information and cyber domain. Through systematic comparison of different cases of cyber incidents and information operations, researchers can identify patterns and factors that consistently influence friction manifestation. Sanger emphasizes the value of the comparative approach: „Only through systematic comparison of different cyber conflicts can we begin to distinguish idiosyncratic factors from fundamental principles that govern friction dynamics in the digital domain" (Sanger, 2018:231). Methodologically, this requires the development of standardized protocols for documentation and case analysis that enable meaningful comparison despite significant variations in context, actors, and technologies. The development of scenarios and simulations represents a valuable methodological tool for analyzing friction in the information and cyber domain, especially given ethical and practical limitations of experimenting with critical systems in the real world. Wu and Kott emphasize: „Simulations and exercises enable researchers to experiment with different forms of friction in a controlled environment, identify critical vulnerability points,

and test different mitigation strategies without risk to operational systems" (Wu & Kott, 2019:178). Methodologically, this requires the development of realistic scenarios and simulation environments that can adequately replicate relevant characteristics of the real world (Knežević, 2024), including technical, organizational, and human factors.

An important aspect of the methodological framework for analyzing friction in the information and cyber domain is also the development of metrics for assessing the effectiveness and costs of different friction mitigation strategies. As Clark and Hazelwood emphasize: „For informed decision-making about investments in cyber capabilities, decision-makers need methodology that can not only identify different forms of friction, but also quantify the probable impact and costs of different approaches to addressing them" (Clark & Hazelwood, 2017:92). This requires the development of *cost-benefit*analytical frameworks adapted to the specificities of the cyber domain, including metrics for assessing direct implementation costs, indirect complexity costs, and probable benefits in terms of reduced friction or increased resilience. The systems approach perspective offers a particularly valuable methodological framework for analyzing friction in the information and cyber domain. Instead of focusing on individual incidents or specific technologies, the systems approach views information and cyber systems as complex, adaptive socio-technical entities. Perrow emphasizes the importance of this approach: „Friction in complex systems often arises from unexpected interactions between components that individually function according to specifications - these emergent interactions can only be understood through a holistic, systems approach that transcends analysis of individual components" (Perrow, 2011:209). Methodologically, the systems approach includes techniques of system mapping, identification of critical interdependencies, and analysis of potential cascading effects that can amplify initial friction.

Analysis of friction in the information and cyber domain must also take into account the sociopolitical context in which operations take place. Different regulatory regimes, cultural norms, economic factors, and geopolitical relations significantly influence the manifestation and impact of friction. As Deibert observes: „A methodological framework

that ignores the broader sociopolitical context of cyber operations will inevitably miss important factors that shape friction dynamics, from regulatory constraints and legal barriers to cultural differences in risk perception and organizational practices" (Deibert, 2020:175), and this requires an interdisciplinary approach that integrates insights from political science, international relations, sociology, and anthropology with technical analyses of information and cyber systems. The development of robust epistemological foundations represents another important aspect of the methodological framework for analyzing friction in the information and cyber domain. Cyberspace is characterized by fundamental epistemological uncertainty - even seemingly simple questions such as "who carried out the attack?" or "what were the real intentions?" often remain without definitive answers. As Shires emphasizes: „Epistemological uncertainty is not just a practical limitation of cyber friction analysis, but also an essential element of friction itself - uncertainty regarding actor identity, their intentions and capabilities directly contributes to decision-making processes and operational execution" (Shires, 2021:132). Methodologically, this requires explicit addressing of epistemological limitations through application of analytical frameworks that can operate under conditions of high uncertainty, including Bayesian reasoning,[9] *fuzzy logic*, and sensitivity analysis.

For complete analysis of friction in the information and cyber domain, it is necessary to develop a methodological approach that can encompass the interaction between cyber and physical domains. With the proliferation of the Internet of Things (IoT) and cyber-physical systems, the boundary between digital and physical becomes increasingly porous, creating new forms of interdomain friction. Schneier describes this phenomenon: „As our physical systems become increasingly connected and dependent on digital components, friction in the

9 Bayesian reasoning is an inference approach based on Bayes' theorem that formally updates beliefs based on new evidence. The formula $P(A|B) = [P(B|A) \times P(A)] / P(B)$ calculates the posterior probability of a hypothesis after receiving new information. It is particularly useful in high-uncertainty situations such as the cyber domain because it explicitly quantifies initial knowledge (so-called *prior probabilities*) and their updating. In friction analysis, it enables decision-making based on incomplete information. It integrates subjective assessments into a mathematically rigorous framework, ideal for attack attribution problems and risk assessment.

cyber domain increasingly directly and immediately affects the physical world, creating new types of risks and vulnerabilities that transcend traditional domain boundaries" (Schneier, 2018:87). Methodologically, this requires the development of integrated approaches that can track friction propagation between cyber and physical domains, identifying critical conversion points where digital friction has direct physical implications. The ethical dimension must also be explicitly addressed in the methodological framework for analyzing friction in the information and cyber domain. Research on cyber conflicts raises significant ethical questions related to privacy, security, and the potential *dual-use* nature of developed knowledge. Singer and Cole warn: „Methodology that ignores the ethical implications of cyber research risks not only normative violations, but also undermines the long-term value and credibility of the research itself" (Singer & Cole, 2020:219). This requires the development of ethical protocols for data collection and analysis, especially when dealing with sensitive information, and adequate protection of source identities and technical details that could be misused.

The development of a robust methodological framework for analyzing friction in the information and cyber domain of contemporary conflicts represents a complex but necessary undertaking. Such a framework must transcend the limitations of traditional approaches developed for analyzing friction in the physical domain, address the unique characteristics of digital space, integrate different disciplinary perspectives, and develop metrics that can encompass the multidimensional nature of digital friction. As Cunningham and Massee emphasize: „Only through the development of an integrated and flexible methodological framework that can encompass technical, cognitive, organizational, and strategic dimensions of friction can we begin to understand the real dynamics of contemporary information and cyber conflicts" (Cunningham & Massee, 2022:243). Such a framework is not only an academic tool, but also a practical necessity for military planners, security analysts, and decision-makers who daily face the challenges of navigating through the complex and often insufficiently understood information and cyber space of contemporary conflicts.

4. REDEFINING CLAUSEWITZ'S CONCEPT OF FRICTION THROUGH THE PRISM OF ASYMMETRIC OPERATIONS: EMPIRICAL FINDINGS AND A NEW THEORETICAL PARADIGM

Clausewitz conceptualized friction in his seminal work "On War" as a fundamental factor that distinguishes *war on paper*from *real war*. His understanding that „everything in war is very simple, but the simplest things become extremely difficult" established a theoretical foundation that has shaped military strategic thinking for more than two centuries. However, the contemporary era of asymmetric conflicts, characterized by dramatic imbalances in military power, technological capabilities, organizational structure, and strategic objectives between conflicting parties, demands a thorough reexamination and redefinition of this concept. While Clausewitz developed his theory of friction primarily in the context of conventional interstate conflicts of the industrial era, asymmetric conflicts of the post-industrial, globalized world manifest forms of friction that transcend his original conceptualizations — both in their nature and strategic implications. Such evolution requires the development of a new theoretical paradigm that can adequately encompass the empirical realities of contemporary asymmetric conflicts and provide a coherent analytical framework for understanding friction in that context.

The very nature of asymmetric conflict fundamentally changes the dynamics of friction. The traditional understanding of friction was primarily focused on material factors — weather conditions, terrain, logistical constraints, fatigue, fear, and uncertainty. However, as Arreguin-Toft points out: „Asymmetric strategies not only seek to exploit traditional sources of friction but actively create new forms of friction through strategic manipulation of perceptions, time, and space — turning weakness into strength and the opponent's strength into weakness" (Arreguin-Toft, 2005:41). This perspective emphasizes how weaker actors in asymmetric conflicts consciously develop strategies that maximize friction for technologically and materially superior opponents, often using precisely the advantages that arise from their structural inferiority — flexibility, dispersion, and deep integration into the local social context.

Empirical research on asymmetric conflicts of recent decades provides rich material for redefining the concept of friction. Analyzing historical data on asymmetric conflicts from 1800 to 2005, Lyall and Wilson discovered a striking trend: „The percentage of victories by materially superior actors in asymmetric conflicts has continuously declined over time — from about 80% in the 19th century to less than 40% after 1945 — which implies that increasing technological and material superiority can paradoxically generate new forms of strategic and operational friction" (Lyall & Wilson, 2009:82).[10] This empirical finding directly challenges conventional assumptions about the inverse correlation between material superiority and exposure to friction, suggesting that technological sophistication can, in certain contexts, increase rather than reduce exposure to friction.

One of the key mechanisms explaining this paradox is what Simpson calls "operational rigidity friction" —the tendency of technologically superior forces to develop complex, standardized operational procedures that, while optimized for conventional conflicts, create additional friction when applied in unconventional, asymmetric conflicts. As Simpson notes: „Highly developed military organizations develop operational rigidity as a byproduct of institutional learning and standardization — procedures optimized for victory in one type of conflict can become a source of friction in another" (Simpson, 2018:124). Operational rigidity represents a form of "self-induced friction" that arises from internal structural characteristics of military organizations, rather than from external factors that Clausewitz primarily identified.

The temporal dimension of friction in asymmetric conflicts also represents a significant departure from Clausewitz's conceptualization. While Clausewitz was primarily focused on friction that manifests in

10 Statistical analysis conducted by Lyall and Wilson (2009) shows that the percentage of victories by materially superior actors in asymmetric conflicts has constantly declined over time: from approximately 80% in the period 1800-1850, to 65% in the period 1900-1950, and to only 40% after 1950. In more recent research, Arreguín-Toft (2013) analyzed 196 asymmetric conflicts between 1800 and 2003, discovering that weaker actors won in 28.5% of cases during the 19th century, 34.7% during the first half of the 20th century, and in as many as 55% of cases from 1950 to 2003. The data clearly illustrate a paradoxical trend where increased technological superiority correlates with declining probability of victory in asymmetric conflicts.

real-time during active operations, asymmetric actors often consciously manipulate the temporal dimension of conflict as a strategic weapon. As Mack emphasizes in his classical analysis of asymmetric conflicts: „An actor who cannot win in space often tries to win in time — prolonging the conflict and increasing economic, political, and psychological costs for the opponent to the point where the price of continuing the conflict exceeds the potential benefits of victory" (Mack, 1975:175). Strategic manipulation of time creates a form of "strategic endurance friction" that accumulates over long periods and has a cumulative effect on the technologically superior side's ability to maintain operational tempo and political will to continue the conflict.

The cognitive dimension of friction in asymmetric conflicts represents another area requiring conceptual redefinition of Clausewitz's model. Analyzing the experiences of Western military forces in asymmetric conflicts after the Cold War, Kilcullen identifies what he calls *cognitive friction of cultural distinction* — cognitive dissonance and operational challenges that arise when military forces trained for conventional warfare face opponents whose mode of warfare stems from fundamentally different cultural, social, and historical contexts. „Cognitive friction in asymmetric conflicts"[11], argues Kilcullen, „does not only arise from

11 The concept of *cognitive friction of cultural distinction* represents a special type of operational friction that arises when military forces face an adversary whose way of warfare, motivations, values, and operational logic stem from a fundamentally different cultural, social, and historical context. Kilcullen (2013) defines this type of friction as cognitive dissonance and operational challenges that manifest when military forces trained and organized according to one cultural model of warfare attempt to understand, predict, and effectively act against an adversary that functions according to entirely different cultural patterns. This type of friction manifests through several key mechanisms:

1. Impeded understanding of adversary motivations (which hinders behavioral prediction);
2. Misinterpretation of signals and intentions (due to different communication codes);
3. Inadequate assessment of the value of objectives and resources (what is valuable in one cultural context may be irrelevant in another);
4. Inappropriate application of strategies and tactics developed for culturally similar adversaries.

Unlike the traditional understanding of friction that focuses on physical obstacles or incomplete information, *cognitive friction of cultural distinction* emphasizes how even complete information can be misinterpreted when filtered through inappropriate cultural frameworks. This phenomenon is particularly visible in Western military interventions in culturally distant contexts such as Afghanistan, Iraq, or other areas where concepts such as authority, loyalty,

the uncertainty that Clausewitz described, but from fundamental misunderstanding of the sociocultural context of the conflict, which makes it difficult to interpret opponent behavior through conventional analytical frameworks and doctrine" (Kilcullen, 2013:93). Cognitive friction has direct operational implications, as it complicates anticipation of enemy actions, interpretation of intelligence data, and creation of effective counter-strategies while respecting international law.

The organizational structure of asymmetric actors also generates new forms of friction that transcend Clausewitz's conceptualizations. Sageman, analyzing terrorist networks, identifies *organizational dissonance friction* — challenges that hierarchically organized military and security structures face when confronting networked, decentralized opponents. *Network-organized opponents*, notes Sageman, „create operational friction for hierarchical structures through their ability to absorb losses without degradation of overall capabilities, rapidly adapt tactics without central command, and exploit slow decision-making processes characteristic of bureaucratic

time, success, or honor may have significantly different meanings and manifestations from those to which Western military structures are accustomed and for which they are trained.

[1] The concept of *organizational dissonance friction* refers to operational challenges and friction that arise when opposing sides in a conflict are characterized by fundamentally different organizational structures, decision-making processes, and operational logics. In the context of asymmetric conflicts, this type of friction occurs when hierarchically structured, highly formalized military organizations (typical of conventional forces) confront network-organized, decentralized, and adaptable adversaries (characteristic of insurgent, terrorist, or other unconventional groups). Sageman (2008) explains that network-organized adversaries create significant friction for hierarchical structures through several mechanisms:

1. Ability to absorb losses without degradation of overall operational capabilities (due to decentralization and redundancy);
2. Possibility of rapid tactical adaptation without central command (through horizontal communication and localized autonomy);
3. Exploitation of slow decision-making processes characteristic of bureaucratic military organizations (playing on the tempo of operations).

Organizational dissonance creates challenges for conventional forces that must balance between the need for centralized coordination (for consistency and efficiency) and requirements for decentralized executive capability (for adaptability and speed of response) in conflict with an adversary that operates according to a fundamentally different organizational logic. This type of friction has direct operational implications because standard operating procedures, command chains, and control mechanisms that are efficient against symmetrically organized adversaries become sources of operational limitations when applied against an asymmetrically organized enemy.

military organizations" (Sageman, 2008:142). Organizational dissonance creates a fundamental challenge for conventional military forces that must balance between the need for central coordination and requirements for decentralized, adaptive executive capability in the field.

The informational dimension of friction in asymmetric conflicts represents a significant evolution from Clausewitz's understanding of the *fog of war*. While Clausewitz primarily considered uncertainty arising from lack of information or its unreliability, contemporary asymmetric conflicts often involve what Betz calls *information overload friction*. As he explains: „Paradoxically, technological superiority that enables collection of enormous amounts of data can create new friction through information overload, fragmentation of attention, and difficulty in distinguishing signal from noise — a situation where decision-makers have access to more information than ever before but face greater challenges in their effective interpretation and integration" (Betz, 2015:65). This informational friction is particularly relevant in the context of asymmetric conflicts where opponents are often dispersed among civilian populations, dramatically increasing the complexity of identifying and targeting legitimate military objectives.

The political dimension of friction in asymmetric conflicts also requires conceptual expansion of Clausewitz's theory. Analyzing U.S. experiences in asymmetric conflicts, Biddle (2006) identifies what he calls *strategic divergence friction* — operational challenges that arise when there is divergence between political objectives and military means for their achievement. „In asymmetric conflicts", notes Biddle, „there is often fundamental tension between political constraints (need to minimize collateral casualties, respect humanitarian law, maintain domestic and international support) and military imperatives (need for constant pressure on the opponent, maintaining operational tempo, isolating insurgents from civilian population)—this tension creates friction that manifests through restrictive rules of engagement, complex operation approval procedures, and lengthy decision-making processes" (Biddle, 2006:212). Strategic friction has a direct impact on operational effectiveness, as it limits the ability of military forces to apply their full technological and material superiority against asymmetric opponents.

Empirical analysis of specific asymmetric conflicts provides additional insights into new forms of friction requiring conceptual redefinition. Studying the dynamics of American intervention in Iraq, Hashim identifies *legitimacy deficit friction* — operational challenges that arise when foreign military forces operate in a society where they lack perception of legitimacy among the local population. „Legitimacy deficit", notes Hashim, „creates friction through erosion of reliable intelligence information, enabling the opponent to manipulate local perceptions, and creating security challenges that require disproportionate allocation of resources for basic security and force protection" (Hashim, 2006:133). Such legitimacy deficit friction is particularly relevant in the context of external actor interventions in local conflicts, where asymmetry of legitimacy is often as significant as asymmetry of material power.

Advances in military technology, paradoxically, can also generate new forms of friction in asymmetric conflicts. Analyzing the use of advanced technologies in counterinsurgency operations, Chin (2019) identifies "technological dependency friction" — operational challenges that arise when military forces become overly reliant on technological solutions in complex social conflicts. „Technological dependency", argues Chin, „can create friction through atrophy of fundamental military skills, creation of false sense of security and superiority, and encouragement of operational approaches that prefer technology-intensive methods even when socially-intensive methods might be more effective" (Chin, 2019:191). This type of friction is particularly relevant in counterinsurgency operations, where technological superiority can create an illusion of understanding the terrain and opponent that does not correspond to the complex sociopolitical realities of the conflict.

The juridical dimension of friction in asymmetric conflicts also represents a significant aspect requiring conceptual expansion of Clausewitz's theory. As Dunlap (2008) emphasizes in his analysis of the *lawfare* concept (use of law as a weapon in asymmetric conflicts): „Asymmetric actors increasingly use legal constraints as a strategic weapon against technologically superior opponents, creating 'juridical friction' through exploitation of limitations that international humanitarian law and domestic legislation impose on conventional military forces" (Dun-

lap, 2008:88). Juridical friction has direct operational impact, as it imposes complex target verification procedures, limits the use of certain weapons and tactics, and creates asymmetric constraints that often favor parties that do not adhere to the same legal standards.

Analysis of specific operational challenges in asymmetric conflicts further illustrates new forms of friction requiring redefinition of Clausewitz's theory. Studying the dynamics of urban asymmetric conflicts, Evans identifies *urban terrain friction* — unique operational challenges that arise when conventional military forces face asymmetric opponents in densely populated urban areas. „Urban terrain", argues Evans, „imposes specific forms of friction through dramatically reduced visibility ranges, impaired communication, limited mobility, need for precise fire in the presence of civilians, and complex three-dimensional nature of combat space that favors knowledge of local environment over technological superiority„ (Evans, 2016:56). This type of operational friction becomes increasingly significant in the context of global urbanization, where asymmetric opponents consciously choose urban areas as preferred terrain for confrontation with technologically superior opponents.

Empirical analysis of the psychological dimension of asymmetric conflicts also provides insights into new forms of friction that transcend Clausewitz's conceptualizations. Through extensive interviews with veterans of asymmetric conflicts, Grossman and Christensen identify *moral dissonance friction* — psychological challenges that arise when soldiers trained for conventional conflicts face opponents who do not follow conventional norms of warfare. „Moral dissonance", the authors note, „creates operational friction through psychological stress, uncertainty in identifying legitimate targets, and tension between mission imperatives and concerns for civilian casualties — factors that can significantly degrade combat effectiveness through increased caution, hesitation, and psychological exhaustion" (Grossman & Christensen, 2007:174). This type of friction has direct implications for training, doctrine, and support for soldiers engaged in asymmetric conflicts, where conventional preparation models may be inadequate for addressing the unique psychological challenges these conflicts present.

Strategic analysis of superior force failures in asymmetric conflicts further illuminates new forms of friction requiring redefinition of

Clausewitz's theory. In his comprehensive study, Record identifies *strategic asymmetry of interests friction* — the fundamental challenge faced by external forces intervening in local conflicts where their stake is less critical than that of local actors. „Asymmetry of interests", argues Record, „creates friction through disparity in willingness to accept casualties, costs, and time needed to achieve objectives — external actors, even when possessing dramatic material superiority, face unique strategic friction arising from limited political capital for prolonged, expensive conflicts with unclear prospects for decisive victory" (Record, 2007:122). This type of strategic friction has direct implications for planning, execution, and evaluation of military interventions in asymmetric conflicts, where conventional success metrics and traditional progress indicators may be inadequate.

Empirical analysis of organizational learning in asymmetric conflicts also provides significant insights relevant to redefining the concept of friction. Studying military organization adaptations during prolonged asymmetric conflicts, Nagl identifies *institutional conservatism friction* — the tendency of established military organizations to resist fundamental adaptations even when faced with evident failure of existing approaches. „Institutional conservatism", notes Nagl, „creates friction through resistance to innovations perceived as deviations from organizational tradition and identity, preference for incremental modifications over fundamental reforms, and tendency to attribute failures to inadequate implementation of existing doctrine rather than fundamental shortcomings of the doctrine itself" (Nagl, 2005:215). This type of organizational friction is particularly relevant in the context of conventional military force adaptation for asymmetric conflicts, where traditional organizational structures, training systems, and doctrinal approaches may be fundamentally inadequate for new operational reality.

Redefining Clausewitz's concept of friction through the prism of asymmetric operations requires development of a new theoretical paradigm that can adequately encompass these empirical realities. Such a paradigm must transcend the limitations of traditional understanding of friction as primarily a material and tactical phenomenon, and incorporate a more complex understanding of strategic, organizational, cognitive,

cultural, and political dimensions of friction in asymmetric conflicts, taking into account the spirit of war history. As Gray emphasizes: „Clausewitz's fundamental intuition about the centrality of friction in warfare remains valid, but his specific understanding of friction manifestations and sources must be expanded and redefined to encompass the realities of post-industrial, globalized security environment characterized by proliferation of asymmetric actors, tactics, and strategies" (Gray, 2012:198).

The new theoretical paradigm of friction in asymmetric conflicts must be multidimensional, integrating different forms of friction into a coherent analytical framework that can encompass their mutual interactions and cumulative effects. Such a paradigm should distinguish at least five distinctive dimensions of friction in asymmetric conflicts: 1) operational friction (tactical and logistical challenges in the field), 2) organizational friction (structural constraints and adaptive capacity), 3) cognitive friction (challenges of perception, interpretation, and decision-making), 4) political friction (constraints imposed by political imperatives of legitimacy and support), and 5) strategic friction (tension between objectives and means, short-term imperatives and long-term interests). Integration of these different dimensions enables understanding of friction not only as unwanted resistance to be minimized, but also as a strategic factor that can be actively manipulated — either through reducing one's own friction or through amplifying opponent friction.

Empirical findings from asymmetric conflicts also emphasize the need for understanding friction as a relative, rather than absolute phenomenon. Traditional understanding of friction often implicitly assumes that it uniformly affects all actors in conflict, varying only in intensity. However, as Nagl emphasizes: „Different actors, with different organizational cultures, structures, and strategic imperatives, experience fundamentally different forms of friction even in the same operational environment — what represents critical friction for one actor may be marginal or even irrelevant for another" (Nagl, 2005:220). The relative nature of friction has significant strategic implications, as it suggests that success in asymmetric conflicts may depend more on the ability to adapt to inevitable friction than on the illusory quest for its elimination through technological or material superiority.

The new theoretical paradigm of friction in asymmetric conflicts must also address the interaction between different types of friction and their cumulative effect. As Hammes (2004) emphasizes in his analysis of "fourth generation warfare": „Effective asymmetric strategies aim to create cascading friction—where initial tactical friction generates operational complications, which then create organizational dysfunctions, which ultimately undermine strategic coherence and political sustainability" (Hammes, 2004:245). Understanding the cascading nature of friction has significant implications for analysis and planning, as it emphasizes the need for a holistic approach that can adequately encompass complex interdependencies between different levels and dimensions of friction.

Redefining the concept of friction through the prism of asymmetric operations also has significant implications for military doctrine, training, and organization. Traditional approaches, based on Clausewitz's understanding of friction, often emphasize standardization of procedures, hierarchical control, and technological solutions as primary mechanisms for reducing friction. However, empirical analysis of asymmetric conflicts suggests that these approaches may be inadequate or even counterproductive in contexts requiring high degrees of adaptability, decentralized initiative, and contextual understanding. As Kilcullen (2013) emphasizes: „Effective confrontation with asymmetric opponents requires organizational culture and structures that accept the inevitability of friction, develop capacity for rapid adaptation, and cultivate the ability to operate effectively amid uncertainty rather than the illusory quest for its elimination" (Kilcullen, 2013:241). This perspective emphasizes the need for fundamental reexamination of dominant assumptions about optimal design of military organizations and processes of training and doctrinal adaptation, especially amid the evolution of international law.

Redefining Clausewitz's concept of friction through the prism of asymmetric operations represents not only an academic but also a practical imperative for understanding the dynamics of contemporary conflicts. Empirical findings from asymmetric conflicts clearly demonstrate the need for a new theoretical paradigm that can adequately encompass the complexity and multidimensionality of friction manifested in these conflicts. Such a paradigm must transcend the limitations of tradition-

al understanding of friction focused primarily on material and tactical factors, and incorporate more sophisticated understanding of organizational, cognitive, cultural, political, and strategic dimensions of friction. Through integration of these different perspectives and empirical findings, it is possible to develop a coherent analytical framework that can inform more effective theory and practice in the context of asymmetric conflicts that will likely continue to dominate the security environment in the decades to come.

5. CONCLUSION

Clausewitz's theory of friction remains one of the most significant contributions to understanding the nature of war and military operations, but as we have seen through our analysis, the contemporary context of warfare requires its significant redefinition and expansion. From the historical context and fundamental principles that Clausewitz established, through the complex operational space of hybrid warfare, methodological challenges of analysis in the information and cyber domain, to empirical findings from asymmetric operations—each dimension of our research has contributed to a holistic understanding of the evolution of the concept of friction in modern warfare. The key conclusion that runs through all aspects of our research is that friction has evolved from primarily a material and tactical phenomenon to a multidimensional concept encompassing organizational, cognitive, informational, legal, political, and strategic components. Contemporary conflicts characterized by multidimensionality, nonlinearity, and asymmetry create new forms of friction that require new analytical approaches and adaptations of traditional military organizations and doctrines.

Hybrid warfare has presented a challenge to conventional understanding of friction through blurring boundaries between different domains of conflict and deliberate instrumentalization of friction as a strategic weapon. Information saturation, cyber specificities, ambiguity, asymmetry, and manipulation of perceptions create new sources and manifestations of friction that Clausewitz could not have anticipated in his time. Methodological challenges of friction analysis in information and cyber

domains require a multidisciplinary approach that integrates technical, social, and cognitive perspectives. Epistemological uncertainty, the attribution problem, the relative nature of friction, and complex inter-domain interactions create the need for developing new metrics, analytical frameworks, and research approaches that can adequately encompass these phenomena.

Asymmetric conflicts have particularly illuminated the paradoxical nature of contemporary friction, where technological and material superiority can paradoxically create new forms of strategic, operational, and organizational friction. Operational rigidity, cultural dissonance, political constraints, and asymmetry of interests represent factors that can significantly reduce the effectiveness of materially superior parties in asymmetric conflict.

The new paradigm of understanding friction that we propose through this research emphasizes the need for a holistic approach that views friction not only as an obstacle to be minimized, but also as a strategic factor that can be actively managed. Such a paradigm recognizes the relative nature of friction, its multidimensionality, and cascading effects that manifest through different levels of conflict. For military organizations, the implications are significant—success in contemporary conflicts increasingly depends on the ability to effectively adapt to inevitable friction, develop organizational resilience, and cultivate operational flexibility. Organizations that remain trapped in traditional understanding of friction risk developing doctrine, structure, and capabilities that are inadequate for the realities of contemporary conflicts. Redefining Clausewitz's concept of friction through the prism of contemporary conflicts represents not only an academic but also a practical imperative for military organizations that want to remain relevant in the complex, multidimensional, and nonlinear security environment of the 21st century.

6. LITERATURE

1. Arquilla, J. (2012). *Cyberwar is Coming!: The Future of Conflict in the Digital Age*. RAND Corporation.
2. Arreguin-Toft, I. (2005). *How the Weak Win Wars: A Theory of Asymmetric Conflict*. Cambridge University Press.
3. Betz, D. J. (2015). *Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power*. Oxford University Press.
4. Betz, D. J. & Stevens, T. (2013). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Routledge.
5. Biddle, S. (2006). *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton University Press.
6. Bousquet, A. (2009). *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. Columbia University Press.
7. Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.
8. Chin, W. (2019). *Britain and the War on Terror: Policy, Strategy and Operations*. Routledge.
9. Clark, D. & Hazelwood, S. (2017). *Translating Strategy into Action: The Role of Professional Military Education in the Future of Warfare*. Center for Strategic and International Studies.
10. Clausewitz, C. v. (1976). *On War* (Translation: M. Howard and P. Paret). Princeton University Press.
11. Cronin, A. K. (2020). *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford University Press.
12. Cunningham, F. & Massee, P. (2022). *Digital Friction: Methods and Metrics for Cyber Conflict Analysis*. Georgetown University Press.
13. Deibert, R. J. (2020). *Reset: Reclaiming the Internet for Civil Society*. House of Anansi Press.
14. Demchak, C. C. (2018). *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. University of Georgia Press.
15. Dunlap, C. J. (2008). Lawfare Today: A Perspective. *Yale Journal of International Affairs*, 3(1), 146-154.

16. Echevarria, A. J. (2007). *Clausewitz and Contemporary War*. Oxford University Press.
17. Evans, M. (2016). *Future War in Cities: Urbanization's Challenge to Strategic Studies in the 21st Century*. International Institute for Strategic Studies.
18. Freedman, L. (2017). *The Future of War: A History*. Public Affairs.
19. Fridman, O. (2018). *Russian "Hybrid Warfare": Resurgence and Politicization*. Oxford University Press.
20. Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38(2), 41-73.
21. Gerasimov, V. (2013). The Value of Science is in Prediction: New Challenges Require Rethinking Forms and Methods of Conducting Combat Operations. *Military-Industrial Courier*, 8(476), 23-29.
22. Gompert, D. C. (2016). *Cyber Power and National Security*. National Defense University Press.
23. Gray, C. S. (1999). *Modern Strategy*. Oxford University Press.
24. Gray, C. S. (2012). *Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional*. Strategic Studies Institute.
25. Gray, C. S. (2015). *The Future of Strategy*. Polity Press.
26. Grossman, D. & Christensen, L. W. (2007). *On Combat: The Psychology and Physiology of Deadly Conflict in War and in Peace*. Warrior Science Publications.
27. Hammes, T. X. (2004). *The Sling and the Stone: On War in the 21st Century*. Zenith Press.
28. Hammes, T. X. (2016). *Deglobalization and International Security*. Potomac Books.
29. Hashim, A. S. (2006). *Insurgency and Counter-Insurgency in Iraq*. Cornell University Press.
30. Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
31. Howard, M. (1983). *Clausewitz*. Oxford University Press.
32. Jervis, R. (2017). *System Effects: Complexity in Political and Social Life* (2nd ed.). Princeton University Press.

33. Kahneman, D., Sibony, O., & Sunstein, C. R. (2021). *Noise: A Flaw in Human Judgment*. Little, Brown Spark.

34. Keegan, J. (1993). *A History of Warfare*. Vintage Books.

35. Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

36. Kilcullen, D. (2013). *Out of the Mountains: The Coming Age of the Urban Guerrilla*. Oxford University Press.

37. Knežević, S. (2024). *Prauzrok: nacrt za uvod u morfologiju kosmologije, evolucije i teogonije* [Primordial Cause: Draft for an Introduction to the Morphology of Cosmology, Evolution and Theogony]. Belgrade: Metaphysica.

38. Knežević, S. & Martinović, T. (2024). Development international law after World War II. *Defendologija* 54-2024, 125-145.

39. Knežević, S. (2025). *Imperijalna prenapregnutost Sjedinjenih Američkih Država i Specijalna vojna operacija u Ukrajini* [Imperial Overstretch of the United States and the Special Military Operation in Ukraine]. Banja Luka: Evropski defendologija centar.

40. Libicki, M. C. (2012). *Crisis and Escalation in Cyberspace*. RAND Corporation.

41. Libicki, M. C. (2016). *Cyberspace in Peace and War*. Naval Institute Press.

42. Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security*, 39(3), 7-47.

43. Linkov, I. & Trump, B. D. (2019). *The Science and Practice of Resilience*. Springer International Publishing.

44. Lyall, J. & Wilson, I. (2009). Rage Against the Machines: Explaining Outcomes in Counterinsurgency Wars. *International Organization*, 63(1), 67-106.

45. Mack, A. (1975). Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict. *World Politics*, 27(2), 175-200.

46. McCulloh, T. & Johnson, R. (2013). *Hybrid Warfare*. Joint Special Operations University Press.

47. McKenzie, S. (2016). *Hybrid Threats and Asymmetric Warfare: What to Learn from 2011–2014*. Swedish Defence University.

48. Nagl, J. A. (2005). *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*. University of Chicago Press.

49. Paret, P. (1985). *Clausewitz and the State*. Princeton University Press.

50. Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury Publishing.

51. Perrow, C. (2011). *Normal Accidents: Living with High-Risk Technologies* (Updated ed.). Princeton University Press.

52. Record, J. (2007). *Beating Goliath: Why Insurgencies Win*. Potomac Books.

53. Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1-2), 4-37.

54. Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. University of Pennsylvania Press.

55. Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Crown Publishing Group.

56. Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. W. W. Norton & Company.

57. Shires, J. (2021). *The Politics of Cybersecurity in the Middle East*. Hurst Publishers.

58. Simpson, E. (2018). *War From the Ground Up: Twenty-First Century Combat as Politics*. Oxford University Press.

59. Singer, P. W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Penguin Press.

60. Singer, P. W. & Cole, A. (2020). *Burn-In: A Novel of the Real Robotic Revolution*. Houghton Mifflin Harcourt.

61. Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

62. Smit, S. (2018). *Information Friction: Digital Media in Conflict Zones*. Columbia University Press.

63. Strange, J. (1996). *Centers of Gravity & Critical Vulnerabilities*. Marine Corps War College.

64. Summers, H. G. (1992). *On Strategy: A Critical Analysis of the Vietnam War*. Presidio Press.

65. Valeriano, B. & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.
66. van Creveld, M. (1991). *The Transformation of War*. Free Press.
67. Waltz, E. (2018). *Information Warfare: Principles and Operations*. Artech House.
68. Watts, B. D. (2004). *Clausewitzian Friction and Future War*. National Defense University Press.
69. Whither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal*, 15(2), 61-72.
70. Wu, Z. & Kott, A. (2019). *Adversarial Deep Learning for Cyber Security*. Springer International Publishing.

Paper received: 16. 12. 2024
Paper accepted: 10. 4. 2025