Baginskyi Andrii, and Mary Lai O. Salvaña. 2026.
"Self-Organised Criticality in Asymmetric Defence: Russia–Ukraine War." *Obrana a strategie* 26, no. 1: 65–86.
https://doi.org/10.3849/1802-7199.26.2026.01.65-86. Published online: June 2026

ORIGINAL ARTICLE

Self-Organised Criticality in Asymmetric Defence: Russia–Ukraine War

Andrii Baginskyi[1], Mary Lai O. Salvaña[2]

Abstract

This study applies self-organised criticality (SOC) theory to analyze organizational vulnerability, resilience, and failure dynamics in the context of the Russia–Ukraine war. The proposed SOC-based framework introduces a quantitative metric—the power-law exponent (α)—to assess the likelihood of systemic failure under sustained stress. Results indicate that highly centralized military structures exhibit greater susceptibility to cascading failures, while distributed and adaptive organizational architectures demonstrate enhanced resilience. The analysis further shows that wartime adaptation reinforces decentralized structures and that both actors strategically synchronize military operations with diplomatic timelines to amplify political effects. By linking complex systems theory with empirical conflict dynamics, the study demonstrates how SOC-informed models can improve asymmetric defence strategies and enable smaller actors to generate disproportionate strategic outcomes. The findings provide implications for NATO force design, defence planning, and resilience-oriented military transformation.

Keywords

Self-organised criticality; asymmetric defence; Russia–Ukraine war; organizational resilience; cascading failures; complex systems; military strategy.

Acknowledgements

Special thanks go to Professor Gregory L. Tangonan (Ateneo Innovation Center and Ateneo de Manila University, Philippines) for his valuable insights on self-organised criticality, complex systems, and asymmetric warfare.

[1] Department of Sociology, The National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine, ORCID iD: 0000-0001-5633-4614, e-mail: andrei.baginsky@gmail.com

[2] Department of Statistics, University of Connecticut, 215 Glenbrook Rd., Storrs, Connecticut, 06269, USA, ORCID iD: 0000-0003-4868-7713, e-mail: marylai.salvana@uconn.edu

AI Disclosure

The authors acknowledge the use of the following generative AI tools to assist in the preparation of this manuscript: OpenAI ChatGPT. These tools were used solely for language editing and structural suggestions, under the complete control and responsibility of the authors. All AI-assisted content was critically reviewed and revised by the authors, who accept full responsibility for the accuracy and integrity of the final version.

Introduction

The Russian invasion of Ukraine, beginning in February 2022, has provided unprecedented empirical evidence of a counterintuitive phenomenon: a numerically and materially superior military force can experience cascading operational failures when confronted by a smaller adversary employing precisely targeted disruptions. On the eve of Russian aggression in 2022, many experts were sceptical about Ukraine's ability to survive as a state against a fully militarised adversary. It soon turned out that the assessments of even the most authoritative researchers were wrong. Now in its fourth year of high-intensity conflict, Ukraine has demonstrated a capacity for state resilience that has become a significant factor in global security architecture, one that other international actors seek to understand and that positions Ukraine as an element of international stability. This capacity has multiple sources: the political leadership's ability to mobilise international support, a level of patriotism across the armed forces and civilian population exceptional for a European country, and a sustained capacity for resourceful adaptation, on the battlefield and in civilian governance alike.

Russia entered the war with overwhelming material advantages: larger manpower reserves, greater stocks of armour and artillery, a sizable air force, and the industrial capacity to sustain prolonged operations (International Institute for Strategic Studies 2022, 192; Carlough and Harris 2025). Since 2022, these advantages have been reinforced by external support, including sustained energy revenues from China, Iranian-supplied strike drones, and North Korean artillery ammunition (Bowen 2026, 2). By conventional measures of military power, Russia should be able to convert these resources into battlefield outcomes at a manageable cost.

Instead, the opposite has occurred. By December 2025, Russian forces had suffered nearly 1.2 million casualties, including an estimated 275,000–325,000 battlefield fatalities, more deaths in three years than in all Soviet and Russian wars combined since World War II (Jones and McCabe 2026, 3-4, 11). Daily casualty rates exceeded 1,500 in late 2024 (Allison 2024; RFE/RL's Ukrainian Service 2024), while equipment losses have run between 2:1 and 5:1 against Ukraine (Jones and McCabe 2025, 2, 10), including the destruction of more tanks than Russia's entire prewar active-duty inventory (Bowen 2026, 2). As NATO Secretary General Rutte noted, Russia now loses in a single month what the Soviet Union lost in ten years in Afghanistan (NATO 2026). These are not the losses of a force winning efficiently.

Attrition models cannot account for this pattern (Taylor 1974). Although Russia enjoys superior firepower, manpower, and external support, it bleeds at historically unprecedented rates. The common explanation, that Moscow deliberately tolerates high casualties as a strategy of attrition, describes what Russia accepts, not what generates the losses. A force with superior resources should be able to advance at lower cost, not higher. The puzzle is not whether Russia accepts casualties, but why its operations continually produce them.

Despite the apparent chaos of warfare, with its fog, friction, and countless variables that Clausewitz (1976, 101-102) warned defy prediction, a remarkable regularity emerges when we examine conflicts at scale. Wars, like earthquakes and avalanches, exhibit power-law distributions: many small skirmishes, fewer major battles, and rare but catastrophic campaigns that reshape entire theatres,

all following the same underlying pattern. This regularity is not a coincidence but a signature of Self-Organised Criticality (SOC): it reveals that war systems operate near criticality, where small actions and catastrophic events follow the same underlying dynamics. Cederman (2001, 135) documented this pattern across centuries of interstate wars. Dobias (2009, 92) found the same power-law pattern in insurgencies, analysing coalitions in Iraq and Afghanistan. Different conflicts, different scales, different actors, yet the same power-law signature emerges.

SOC, first proposed by Bak et al. (1987), describes systems that naturally evolve toward a critical state where minor perturbations can trigger cascading events across all scales. The theory emerged from the canonical sandpile model illustrated in Figure 1. In the initial phase (Figure 1a), grains are added one at a time to a flat surface; each grain simply lands and stays where it falls. As the pile grows (Figure 1b), it approaches a critical slope at which the entire structure becomes vulnerable; every grain now rests against its neighbours under shared tension. At this critical state (Figure 1c), adding a single grain can trigger an avalanche, not because that grain is special, but because the system has accumulated enough internal stress that any small push can release it. Most grains cause only local shifts, but occasionally one grain brings down the whole pile. This dynamic has been observed across domains from earthquakes to financial crashes, and SOC theory has been applied to analyse and prevent natural and man-made disasters (Salvaña et al. 2026), offering a framework for assessing cascading risks that can inform strategic decisions on crisis prevention and organisational resilience.

(a) (b) (c)

Figure 1: The Sandpile Model of Self-Organised Criticality

Note: (a) Grain accumulation phase. (b) Approach to critical slope. (c) An avalanche triggered by a single grain addition.

(Source: Bak et al. 1988, 372)

Military organisations exhibit analogous dynamics. Like the sandpile in Figure 1, modern military forces evolve toward critical states through the ordinary pressures of operation. Efficiency optimisation eliminates redundancy: why maintain two supply depots when one will do? Resource constraints concentrate capabilities: a single maintenance facility serves an entire brigade. Operational tempo accumulates stress across the system as equipment degrades, supplies deplete, and personnel fatigue. Each optimisation is rational in isolation, but collectively they push the organisation toward the critical slope (Figure 1b) where every element depends tightly on others. In the critical state, a precision strike against a logistics hub does not merely destroy trucks. It simultaneously cuts fuel supply, ammunition distribution, and maintenance support across multiple combat formations. A cyberattack against

communications does not simply take down radios; it severs the information flows enabling fire support coordination, intelligence fusion, and command authority. Like the single grain that triggers an avalanche (Figure 1c), these targeted perturbations can propagate failures far beyond the immediate point of impact.

Recognising proximity to criticality is essential for crisis management. Dobias (2009) demonstrated this by showing that although both Iraq and Afghanistan followed SOC dynamics, violence manifested differently in each case. Iraq had reached criticality, like the sandpile at the critical slope in Figure 1b, where one grain can trigger an avalanche. A single violent incident could set off a chain of further incidents (Figure 1c), escalating into spirals that proved difficult to contain. Afghanistan remained subcritical, like a sandpile still below the critical slope, as in Figure 1a, where a single grain simply lands and stays. A violent incident remained isolated, naturally dampening rather than cascading. The same underlying dynamics but different system states require different strategic responses. In a subcritical state, disruptions can be contained, and the situation stabilised. In a critical state, even small events can spiral beyond control, demanding far greater caution.

SOC also creates opportunities for asymmetric strategy. Freedman (2015) defines asymmetric conflict as the strategy of the weaker party: avoid the adversary's strengths, protract the conflict, and erode political will. These strategies are ancient (David versus Goliath, guerrillas versus occupiers), but they gain new potency when understood through the lens of SOC. The asymmetric defender's task is to recognise that the adversary, like all systems under pressure, drifts toward criticality, creating vulnerabilities where precise perturbations can trigger a systemic cascade rather than localised damage. The defender need not match the adversary's resources; instead, the defender must identify where the adversary has concentrated dependencies and apply force at precisely those points. A single well-placed strike against a system at criticality (Figure 1b) can accomplish what a thousand strikes against a subcritical system (Figure 1a) cannot. Yet the defender must also recognise that their own organisation is subject to the same dynamics. Both attacker and defender are SOC systems: both accumulate stress, both drift toward criticality, both face systemic collapse. An effective asymmetric strategy requires exploiting the adversary's criticality while preventing one's own.

To execute such a strategy, planners require models that capture SOC dynamics. Existing approaches (wargaming, scenario analysis, network vulnerability assessment) treat military organisations as static systems. They identify critical nodes, simulate specific attacks, and measure outcomes. But they do not model the system as self-organising to criticality. They fail to recognise that stress accumulates in components over time, that the system drifts toward criticality through its own ordinary operations, and that the same strike can produce catastrophic collapse or localised damage depending on where the system sits in that drift. Current tools answer tactical and operational questions: Which nodes are critical? What happens if we strike target X? Can this plan succeed? The SOC model answers a more fundamental question: how vulnerable is this system? More importantly, it produces a single metric (α) that quantifies vulnerability to cascading failures. This metric can be compared across force designs, doctrines, and scenarios, enabling planners to assess not just whether a plan will work but also whether the system can absorb the friction it will generate.

This reframes the planning problem. Rather than asking "What happens if we strike target X?", a question whose answer depends on tactical conditions that cannot be fully known, planners ask "What is this system's α, and how do changes to structure or parameters shift it?" Organisational restructuring, doctrinal reform, foreign aid, and attack strategies all become interventions that move α. The model enables planners to systematically compare interventions: which changes produce the largest shift toward resilience (for friendly forces) or vulnerability (for adversary forces)?

This article makes five contributions. First, it introduces an SOC model for military organisations. Second, it applies this model to compare Russian and Ukrainian force architectures, revealing that centralised structures are substantially more vulnerable to cascading collapse than distributed ones under identical stress conditions. Third, it demonstrates that adaptation during wartime produces measurable gains in organisational resilience even as external pressure intensifies. Fourth, it identifies a mechanism by which both sides amplify military outcomes into political effects by timing operations to the diplomatic calendar. Fifth, it connects the SOC framework to conflict resolution theory, showing how the dynamics of criticality interact with the conditions for negotiated settlement. The SOC framework provides an answer to the casualty puzzle posed above: Russia's centralised command architecture generates systemic fragility that material superiority cannot offset, while Ukraine's modular structure, wartime adaptation, and alliance support sustain subcritical resilience under sustained pressure.

The Self-Organised Criticality Model for Military Organisations

This section presents the SOC model for military organisations. The model has two parts: (1) components that define the system—nodes, edges, stress, threshold, and transfer rule; and (2) an algorithm that simulates how stress accumulates, how nodes fail, and how failures propagate. Each component maps to factors that defence planners can observe, measure, or influence. This mapping is what makes the model actionable, i.e., changes to real-world force structure translate into changes in the model parameters, and the resulting shift in α quantifies the effect.

Components

Five components define the system:

1. Nodes are potential failure points, e.g., command posts, logistics hubs, combat units, communication centres, or any element whose disruption propagates consequences. The modelling question: if this element fails, does it stress others in ways that could cause them to fail as well? If yes, it is a node.

2. Edges are failure propagation pathways. An edge from X to Y means X's failure stresses Y. Edges represent dependency, not support. If a logistics hub serves three battalions, edges run from the logistics hub to the battalions. A node with many outgoing edges is dangerous: its failure propagates widely. Centralised architecture concentrates edges around hubs; distributed architecture spreads them uniformly.

3. Stress is pressure applied to the system. Random stress (uniform probability across nodes) models general attrition—operational tempo, environmental conditions, and distributed low-level attacks. Targeted stress (probability proportional to node degree) models precision strikes on high-value targets. Analysts can vary intensity (how much stress per attack) and frequency (how often attacks occur).

4. Threshold is the capacity to absorb stress. A node fails when accumulated stress exceeds its threshold. Threshold models hardening, stockpile depth, equipment redundancy, personnel reserves, and foreign aid. When allied nations provide ammunition or equipment, they raise threshold values.

5. Transfer Rule indicates the fraction of stress passed to neighbours when a node fails. High transfer means tight coupling—one failure heavily burdens neighbours. Low transfer means loose coupling—neighbours continue operating. Transfer models doctrine: centralised command with rigid coordination implies high transfer; mission-type orders with autonomous action imply low transfer.

Table 1 summarises these components and their military interpretations.

Table 1: SOC Model Components

Component	*Military Interpretation*
Nodes	Potential failure points: command posts, logistics hubs, combat units, communication centres
Edges	Failure propagation pathways: an edge from X to Y means X's failure stresses Y
Stress	Pressure applied to the system: attacks, operational demands
Threshold	Capacity to absorb stress before failing
Transfer Rule	Fraction of stress passed to connected nodes when failure occurs

(Source: authors)

Algorithm

Given the components, the following algorithm simulates cascade dynamics by tracing how a single strike ripples through a force as a chain of unit failures:

1. Add stress to a node (a strike on a unit).

2. If any node's accumulated stress exceeds its threshold, it fails and transfers a fraction of that stress to connected nodes, any of which may then fail in turn.

3. Repeat step 2 until no node exceeds the threshold (the cascade has settled).

4. Record the cascade size or the number of nodes that failed.

5. Return to step 1.

The algorithm produces a cascade size for each run. That is, how many nodes failed from a single strike. After thousands of runs, we examine the distribution of cascade sizes. SOC theory predicts these distributions follow a power law: $P(s) \propto s^{-\alpha}$, where P(s) is the probability density of a cascade of size s. The exponent α characterises systemic vulnerability by capturing how often a single strike spreads beyond its target:

- Low α: large cascades are common. The system is vulnerable. Strikes routinely propagate, so a small number of disruptions can knock out a disproportionate share of the system.

- High α: large cascades are rare. The system is resilient. Most strikes produce only localised damage and rarely trigger systemic collapse.

Crucially, the SOC model does not predict what will happen in any specific engagement. It answers a different question: given this structure, doctrine, and resources, how vulnerable is this system to collapse? Planners can model different configurations and compare α's. For your own force: how does distributing logistics across multiple hubs change α compared to consolidating them? How does adopting mission-type orders shift α compared to centralised command? For the adversary: given what you observe about their structure, where are the likely vulnerabilities—and which class of strikes will have the greatest impact?

Scope and Limitations

The SOC model isolates the structural component of organisational vulnerability. Human factors such as morale, leadership quality, battlefield experience, junior-officer initiative, discipline, and commanders' ability to react under pressure lie outside their scope, as do operational factors such as terrain, weather, engineering depth, logistical reach, and the interaction of specific weapon systems.

The SOC analysis conducted in this study is therefore a complement to conventional operational and unit-level assessments, not a replacement for them. The structural advantage identified for Ukraine is one of several factors that jointly explain its resilience. The simulation's conclusions are held under the modelled architecture and stated parameters; the empirical battlefield record is consistent with these claims but is not derived from them.

Case Study: Why Is Ukraine Still Standing?

The SOC model offers a framework for answering a question that has puzzled military analysts since February 2022: why has Ukraine—smaller, less equipped, facing a nuclear-armed superpower—not collapsed? The model provides three explanations.

Explanation 1: Organisational Structure

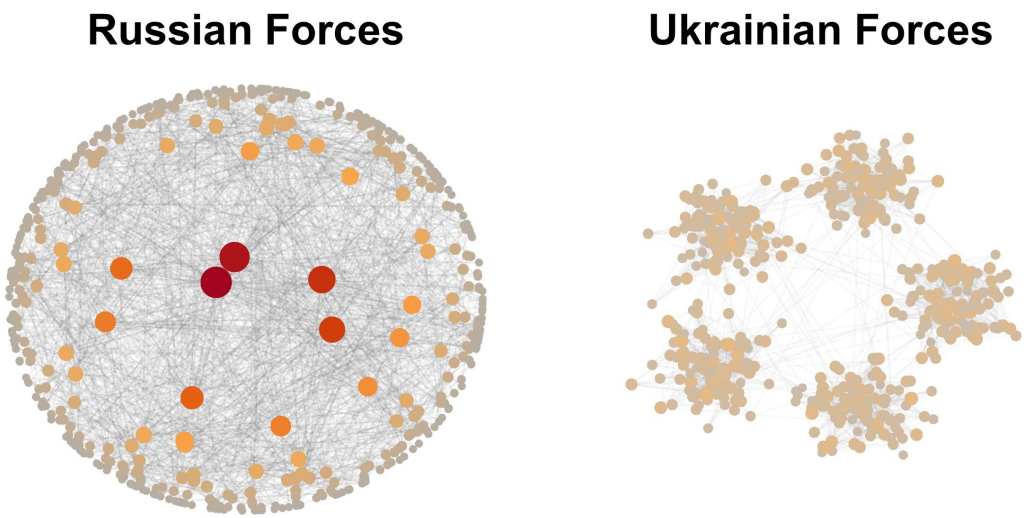

Figure 2: Comparison of Russian and Ukrainian Military Organisational Structures

Note: Both networks use 500 nodes to enable direct comparison; node colour intensity reflects the degree (number of connections)

(Source: authors)

We construct SOC models of both forces using network topologies that capture the structural characteristics documented in doctrinal sources. For the Russian Battalion Tactical Group (BTG), we employ a hub-dominated network structure approximated by a scale-free topology. Doctrinal analyses describe the BTG as a battalion-centred, modular formation in which combined-arms capabilities are aggregated around a single headquarters, with tank, artillery, air defence, engineer, and logistics elements attached from the parent brigade or regiment (Mitrović and Bojanić 2021; Grau and Bartles 2016, 2022). Logistics rely on "the support platoon organic to the battalion on which the BTG is based," creating a sustainment bottleneck that can support operations for only "1–3 days" before requiring resupply from higher echelons (Grau and Bartles 2022). We model this centralised, attachment-based architecture as a scale-free network. Scale-free networks, generated through preferential attachment, produce a small number of highly connected hubs—representing command posts, logistics nodes, and artillery coordination centres—surrounded by many sparsely connected manoeuvre elements. In Figure 2 (left panel), these hubs appear as large, dark red nodes concentrated near the network centre.

We represent the Ukrainian mechanised brigade organisation using a modular network topology. Hooker and Parfonov (2025) describe the Ukrainian brigade as the primary unit of action: "The brigade is the unit of action in the Ukrainian Ground Forces… Brigades are self-sufficient with organic combat, combat support, and combat service support units". Ukrainian brigades "typically have up to four artillery battalions" and include organic air defence, engineers, maintenance, logistics, reconnaissance, and electronic warfare elements within the brigade structure. Command and control above the brigade level is "ad hoc in the form of operational tactical groups," indicating lateral coordination rather than rigid hierarchical dependence. We model this distributed and self-contained architecture

using a modular network topology: dense intra-brigade connections represent organic integration, while sparse inter-brigade links represent ad hoc coordination across formations. In Figure 2 (right panel), nodes appear similar in size and colour, reflecting the absence of dominant hubs, and are organised into five distinct clusters representing semi-autonomous brigades connected through limited coordination ties.

These topology choices are anchored in established network-science results. Albert, Jeong, and Barabási (2000) showed that scale-free networks are robust to random failure but extremely fragile under targeted removal of high-degree nodes, matching the vulnerability profile of a hub-dominated command system. Dong et al. (2018) and Shai et al. (2015) showed that networks with community structure dampen propagation across module boundaries and remain operational where homogeneous networks collapse, matching the resilience profile of a self-sufficient brigade architecture. The two topologies, therefore, correspond to two known cascade regimes: hub fragility under targeted attack and modular containment of disruption.

We emphasise that the BTG and the Ukrainian mechanised brigade serve as archetypes of the two doctrinal poles, not as representative averages of all formations deployed by either side. The Russian inventory includes motorised rifle brigades, tank brigades, naval infantry, airborne units, and the post-2024 reconstituted regiments, each with its own variations on the BTG model; the Ukrainian Ground Forces likewise field mechanised, motorised, tank, air-assault, and territorial defence brigades that differ in equipment, training, and the degree to which mission command is actually practised. Our model represents the modal mechanised formation on each side as documented in the cited doctrinal literature, and the resulting alpha differential should be read as the structural component of vulnerability rather than as a prediction of unit-level battlefield performance.

Russian centralisation, moreover, is not purely a doctrinal preference. It is reinforced by structural constraints on mid-level command, including the well-documented absence of a robust professionalised non-commissioned officer corps, the limited junior-officer mission-command tradition, and the operational tendency to forward-deploy general officers to manage tactical decisions that more decentralised armies delegate downward (Grau and Bartles 2016; Kofman and Lee 2023; McEnany and Roper 2024). The high transfer parameter assumed for the Russian model is therefore consistent with both the formal architecture and the cadre limitations that make low-coupling alternatives operationally infeasible.

To isolate the effect of topological structure, we hold all other parameters constant: the threshold, transfer rule, and initial stress distribution are identical in both models; only the topology differs. We then simulate 100,000 strikes on each network under two attack strategies. Under random attack, each node has an equal probability of being struck, representing undirected fires or attrition warfare. Under targeted attack, strike probability is proportional to node degree, representing intelligence-driven targeting of high-value nodes such as command posts, logistics hubs, and communication centres. Table 2 presents the model configuration.

Table 2: SOC Model Configuration for Attack Strategies

Attack Strategy	*Random*	*Targeted*
Stress	+1 to random node	+1 weighted by degree
Threshold	6	6
Transfer Rule	0.4	0.4

(Source: authors)

Figure 3 displays the cascade size distributions under both attack strategies. The contrast is stark. Under random attack, Ukraine exhibits a steep power-law slope (α = 2.70) with a maximum cascade size of 49 nodes, while Russia exhibits a shallow slope (α = 1.15) with a maximum cascade size of 1386 nodes—28x larger. This means that when strikes land randomly across the Ukrainian network, most cascades remain small and localised stress dissipates within the module that absorbed the strike. The modular structure acts like a firebreak. In contrast, random strikes on the Russian network frequently propagate into large cascades because even peripheral nodes connect through hubs. When a random strike eventually destabilises a hub's neighbour, the cascade propagates through the hub to the entire network.

Under targeted attack, Ukraine's α decreases to 2.54 with maximum cascade size reaching 59 nodes—modularity limits propagation as no single node dominates. Conversely, Russia's falls to 1.06, with cascades soaring to 1,785 nodes; striking dependency-heavy hubs (e.g., BTG commanders or logistics) triggers catastrophic failure. Consequently, each strike on the Russian network produces 30 times more cascade damage than a Ukrainian equivalent. This thirty-fold figure is a simulation result under stated parameters, illustrating the inherent vulnerability of hub-dominated architectures rather than an operational forecast.

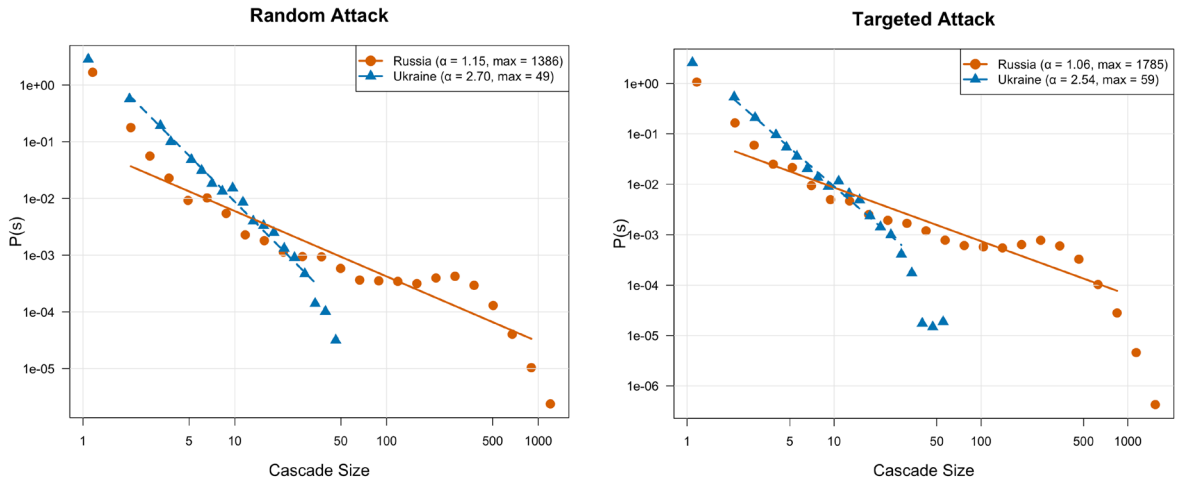

Figure 3: Cascade Size Distributions in Log-log Scale

(Source: authors)

The preceding SOC models demonstrate that distributing capabilities across semi-autonomous modules produces substantially greater resilience to both random attrition and targeted strikes. By contrast, concentrating capabilities in hubs may optimise performance under stable conditions but create catastrophic vulnerability when those hubs are threatened. The implications for targeting are as follows: against a centrally coordinated adversary, intelligence-driven strikes on high-degree nodes yield disproportionate returns. Against a modular adversary, no single strike produces a decisive effect.

Explanation 2: Wartime Adaptation

Ukraine has also become more resilient over the course of the war, adapting its force structure, command arrangements, and integrating commercial technologies at scale in response to battlefield pressures (Kofman and Lee 2023; Bondar 2025; Parfonov 2025). Since February 2022, Ukraine has accelerated its adoption of mission command, with an “increasing emphasis on decentralised command and initiative at lower ranks” and with battlefield lessons “rapidly fed back into training curricula” (Ryan 2025). McEnany and Roper (2024) similarly observe that "with a more decentralised command structure, the Ukrainian military has excelled at bottom-up tactical adaptation."

The SOC model can be used to assess how changes in resilience affect cascade dynamics through the transfer parameter—the fraction of stress passed to neighbouring nodes when a unit fails. High transfer implies tight coupling: when one unit fails, neighbouring units experience significant stress and may fail as well. Low transfer means loose coupling: failures remain localised. We model this shift as a decrease in transfer from 0.4 (pre-invasion) to 0.25 (wartime). The network structure remains constant, i.e., the same modular topology as in Explanation 1. Table 3 presents the parameter values.

Table 3: SOC Model Specification for Ukraine’s Resilience Evolution

	Pre-Invasion	*Wartime*
Stress	+1 to random node	+1 to random node
Threshold	6	6
Transfer Rule	0.4	0.25

(Source: authors)

Figure 4 displays the results. As transfer decreases from 0.4 to 0.25, α increases from 3.64 to 4.88, and maximum cascade size falls from 29 to 18 nodes—a 38% reduction in damage per strike. Crucially, this improvement emerges without any change to the underlying network. When units are tightly coupled, a single node failure sends stress rippling outward, triggering the large cascades that characterise brittle organisations. As coupling loosens—as units develop the capacity to absorb local shocks rather than passing them on—failures remain contained rather than propagate. This loosening of coupling presupposes the human conditions that make mission command operationally viable: trained junior officers and non-commissioned officers, a culture of initiative at lower ranks, lateral coordination habits across adjacent units, and battlefield-driven feedback loops. The modelled shift in α is therefore a joint consequence of doctrinal change and these human factors.

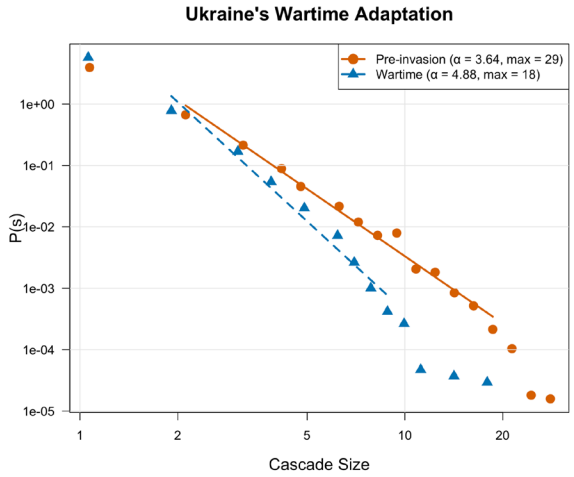

Figure 4: Cascade Size Distributions in Log-log scale

(Source: authors)

Understanding why this adaptation matters requires recognising what modern states are. Mann (1993) argues that the state is polymorphic: it crystallises as a centre, but as a multiple centre whose form depends on the number of political networks it must coordinate, expressed in the diversity of functions and tasks it faces. Social power, in his framework, divides into despotic power—exercised through hierarchical command—and infrastructural power—exercised through networks that penetrate and coordinate society. Modern states seek to expand infrastructural power by embedding themselves within overlapping political, military, economic, and ideological networks. Ukraine's wartime shift toward mission command can thus be interpreted, in Mann's terms, as a movement from despotic toward infrastructural power within its military network—replacing rigid hierarchical dependency with distributed coordination. Russia's BTG structure reflects the opposite tendency: the concentration of despotic power in hub nodes that enable tight control but amplify systemic vulnerability when disrupted. In Mann's framework, then, resilience is not simply a matter of how much power a state commands, but how that power is organised.

Conventional tools for assessing state resilience do not capture this distinction. For example, the Fragile States Index (Fragile States Index 2024) measures incoming pressure—refugees, infrastructure damage, economic disruption, territorial loss—which Ukraine experiences at substantially higher rates than Russia. Such measures capture exposure to stress but not how that stress propagates through organisational structures. On the contrary, the SOC model distinguishes between how hard a system is hit (stress rate) and whether it can absorb the hit (cascade dynamics). Ukraine's high FSI reflects external pressure; its high α reflects internal resilience. We demonstrate by applying differential stress rates to the same network topologies in Explanation 1. Ukraine receives higher stress per iteration (reflecting invasion, displacement, and infrastructure destruction), while Russia receives lower stress (reflecting its position as the aggressor state facing sanctions but not territorial devastation). Table 4 summarises the parameter specification.

Table 4: SOC Model Specification for Differential External Pressure

	Ukraine (High Pressure)	*Russia (Low Pressure)*
Stress	+3 to random node	+1 to random node
Threshold	6	6
Transfer Rule	0.4	0.4

(Source: authors)

Figure 5 clarifies the distinction between conventional fragility metrics and the SOC definition of systemic vulnerability. The left panel displays cumulative external pressure over time, the type of exposure captured by indices such as the Fragile States Index. Ukraine accumulates stress at a substantially higher rate, reflecting invasion, territorial loss, mass displacement, and infrastructure destruction. By this measure alone, Ukraine appears more fragile. The right panel shows cascade dynamics—how each system responds to that pressure. Despite receiving higher stress, Ukraine ($\alpha = 2.84$) exhibits steeper power-law slopes and smaller maximum cascades than Russia ($\alpha = 1.15$). The modular structure contains cascades even under elevated pressure. The reconciliation is straightforward: FSI measures how hard you are being hit; SOC's α measures whether you can take the hit. Ukraine is hit hard, but absorbs it. Russia is hit less hard but cannot absorb it. Traditional fragility indices conflate these two distinct phenomena, leading to misleading assessments in conflict settings.

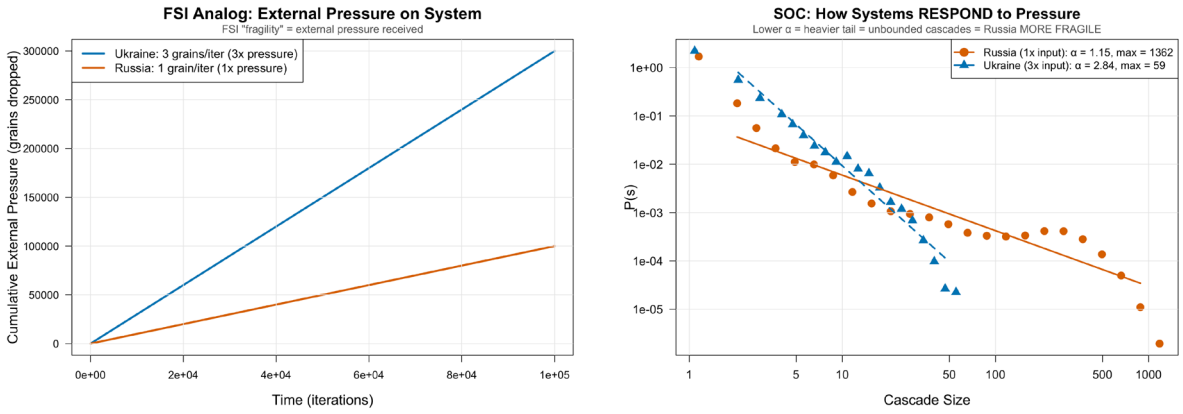

Figure 5: External Pressure Versus Cascade Dynamics.

Note: The left panel shows cumulative stress—what traditional fragility indices measure. The right panel shows how systems respond to that stress.

(Source: authors)

Explanation 3: Strategic Timing and Availability Cascades

Explanations 1 and 2 establish that Russia's centralised architecture is structurally fragile while Ukraine's modular organisation is resilient—and that this resilience has deepened through wartime adaptation. But the war is not fought on the battlefield alone. Military operations also generate political effects: they shape the perceptions of decision-makers in allied capitals who control military aid, sanctions, and diplomatic leverage. Both sides appear to recognise this, and the data suggests that

both deliberately escalate attacks around international meetings, e.g., NATO summits, EU Council sessions, peace conferences, to maximise political impact at moments when the world is watching.

Decision-makers assemble at these gatherings to evaluate the conflict, allocate resources, and set policy, and their judgments are shaped by the information environment in the days immediately preceding these gatherings. A battlefield event that arrives at the right moment does not merely report a military outcome; it provides vivid evidence that anchors deliberation. Tversky and Kahneman (1973) established that decision-making under uncertainty is driven by the availability of recent examples rather than by systematic evaluation of historical outcomes. Kuran and Sunstein (1999) formalised this insight as the availability cascade: a self-reinforcing cycle in which a dramatic event increases media coverage, which in turn increases salience among decision-makers, which generates policy responses, and those responses further validate the original narrative. The triggering event need not be strategically decisive—it need only be vivid, timely, and interpretable within an existing narrative. Well-timed interventions just before political decisions or funding negotiations can disproportionately strengthen an already-forming belief, even if the event's real impact is modest. Strategically timed media coverage amplifies this effect, ensuring the event saturates the information environment before deliberation begins.

Figure 6 presents attack counts for Russia (Panel A) and Ukraine (Panel B) during the six days preceding and the day(s) of major international meetings held between February 2022 and December 2024. Russian-side attacks rose from 908 six days before to 1,189 on the eve of the meetings, then surged to 3,778 on meeting day(s)—a 4.2-fold increase relative to day -6. Ukrainian-side attacks follow a similar ratcheting pattern, rising from 21 to 35 in the final countdown before spiking to 119 on meeting day(s)—a 5.7-fold increase. Rather than remaining flat, both sides exhibit a progressive escalation in the days immediately preceding meetings, culminating in a sharp surge when international attention peaks. Were attacks independent of the diplomatic calendar, meeting-day totals would be statistically indistinguishable from the preceding days. Instead, both sides appear to concentrate on kinetic activity precisely when global visibility is highest. We emphasise that this evidence is consistent with the availability-cascade mechanism described above, but does not by itself establish causation; alternative explanations, including operational tempo cycles independent of the diplomatic calendar, cannot be ruled out from these counts alone.

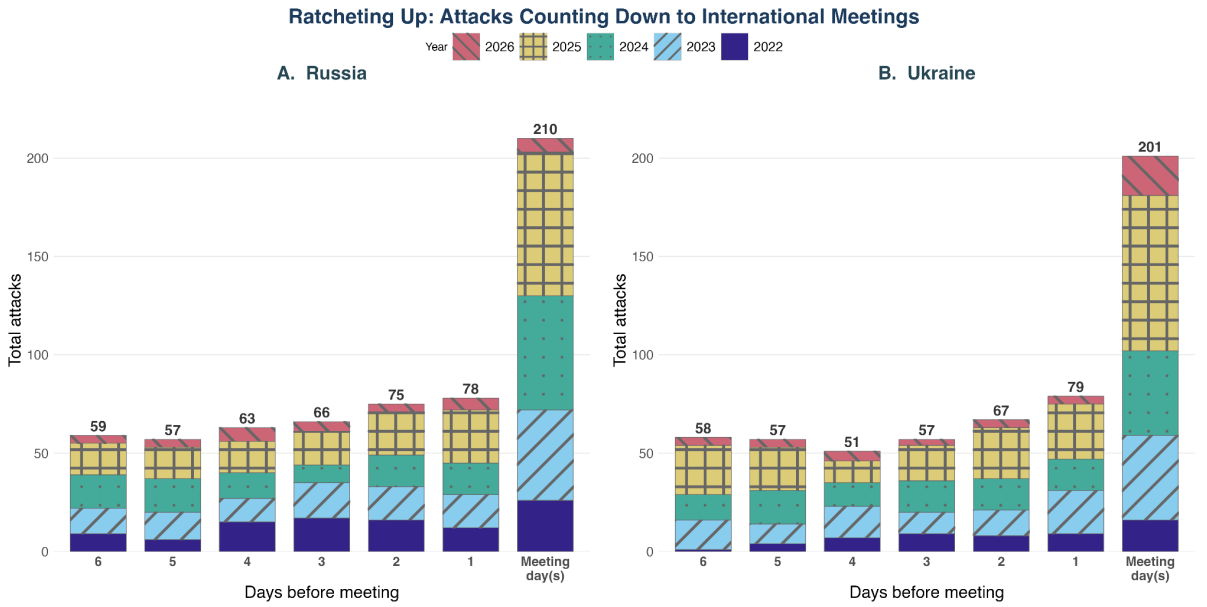

Figure 6: Strategic Escalation Around the Diplomatic Calendar

Note: Meetings include NATO summits, EU Council meetings, G7/G20 gatherings, Ukraine Recovery Conferences, peace talks, and the UN General Assembly

Note: Daily attack counts are reconstructed from the Uppsala Conflict Data Program (UCDP) Georeferenced Event Dataset (GED) version 25.1 (Sundberg & Melander 2013; Davies et al. 2025). Russian-side attacks are events with conflict_name = "Russia - Ukraine" occurring in Ukraine, plus state-on-civilian events by the Government of Russia in Ukraine. Ukrainian-side attacks are events in the same conflict occurring in Russia. International meetings are verified through official summit communiques and institutional calendars.

(Source: authors)

For Ukraine, a well-timed strike on a Russian command post, ammunition depot, or naval vessel just before a NATO summit provides decision-makers with evidence that Ukraine is an effective partner worth supporting. Framing makes aid approvals, sanctions extensions, and security commitments more likely. The resulting support—weapons, ammunition, intelligence, and financial assistance —strengthens Ukraine's military capacity, enabling further operations that reinforce the perception of Ukrainian success. The availability cascade becomes self-reinforcing: belief generates action, action generates evidence, and evidence strengthens belief.

Russia employs the same strategy. Dramatic strikes on Ukrainian infrastructure before international meetings signal that Russia retains escalatory capacity and that the war's costs will continue to mount. This framing aims to amplify war fatigue in allied capitals and generate pressure to condition aid on diplomatic concessions. Attacks timed to coincide with peace talks further signal resolve, positioning Russia as a party that cannot be coerced. The availability cascade operates in the opposite direction: vivid evidence of destructive capacity primes decision-makers to perceive continued support as costly.

Strategic timing is especially effective against centralised adversaries because two amplifying mechanisms operate in sequence. First, as Explanation 1 demonstrated, structural fragility converts small perturbations into disproportionately large operational failures—a single strike on a hub node cascades through Russia's centralised architecture far beyond the point of impact. Second, when that

operational failure coincides with an international summit, the availability cascade converts a military outcome into a disproportionate policy response: decision-makers outweigh the vivid, recent evidence when deliberating next steps. Timing is the bridge between the two: it ensures that the amplified military effect arrives precisely when it can trigger the amplified political effect.

Looking Forward: Criticality and Mutually Hurting Stalemate

The preceding analysis has shown that Russian and Ukrainian military organisations are SOC systems with fundamentally different cascade dynamics. Russia's centralised architecture produces low α values, meaning large cascades are common and the system is structurally fragile. Ukraine's modular architecture produces high α values, meaning cascades remain localised, and the system is resilient. Both sides strategically time perturbations to maximise political effect through availability cascades. These findings have immediate implications for how we assess the trajectory of this war — and for the broader question of when and whether it ends.

Zartman (2008b) proposed the concept of the ripeness of conflict — the idea that the willingness of the parties to cease fighting is closely tied to the exhaustion of the means to continue fighting. Sustained confrontation imposes escalating economic costs on both sides, compelling them to seek alternatives. Simultaneously, the continuation of fighting carries mounting risks, and it is this convergence of costs and risks that produces ripeness — a condition that often elicits intervention by a third party. Central to this framework is the concept of a "mutually hurting stalemate" (MHS), which denotes a situation in which both parties seek to avert the catastrophe of further confrontation. As Zartman writes, "The concept is based on the notion that when the parties find themselves locked in a conflict from which they cannot escalate to victory, and this deadlock is painful to both of them (although not necessarily in equal degree or for the same reasons), they seek an alternative policy or way out. The catastrophe provides a deadline or a lesson indicating that pain can be sharply increased if nothing is done about it now; catastrophe is a useful extension of MHS, but is neither necessary to its definition nor to its existence. If the notion of mutual blockage is too static to be realistic, the concept may be stated dynamically as a moment when the upper hand slips and the lower hand rises, both parties moving toward equality, with both movements carrying pain for the parties." (Zartman 2008b, 1). The passage through MHS and toward an "Exit" leads the parties to negotiations and a "mutually enticing opportunity" for resolution. Zartman later clarified that MHS can occur at any stage of a conflict and is not confined to the highest level of escalation; the subjective perception of a possible catastrophe becomes a significant factor (Zartman 2008a, 232–234).

Moreover, influential international actors can accelerate the parties' movement toward resolution. The term "mediation with muscles" refers to pragmatic political, economic, and diplomatic pressure applied by a powerful third party to the belligerents. This leverage is especially potent when the armed struggle depends substantially on allied resources. As Bramsen, Svensson, and Wallensteen (2025) argue in their analysis of Trump's approach to peace diplomacy, contemporary "deal-making" strategies rely heavily on visible leverage and transactional pressure to compel movement toward negotiation. In the Russia-Ukraine war, such pressure intensified in 2024 on the eve of and during the second term of US President Donald Trump, whose stated ambition included international peacemaking across multiple armed conflicts. In the Russia-Ukraine context, dual pressure on both

parties has taken the form of temporary restrictions on financing aid to Ukraine alongside the imposition of further sanctions on Russia (see, for example: Kelly 2024; Hird et al. 2005; McCabe 2025). For Ukraine, this led to disruptions in the supply of certain weapons systems, partially offset by European assistance through the PURL mechanism. For Russia, sanctions have constrained budget financing, reducing the stability of the broader economic system. This policy narrows both parties' capacity to sustain combat operations — driving both systems closer to criticality after 2024.

Conclusion

This article is, to our knowledge, the first to apply the sandpile model of self-organised criticality as an analytical framework for assessing military organisational vulnerability in an active interstate war. The results yield several critical lessons.

First, the model reveals substantial structural advantages for Ukraine. The α differential between the two forces is not marginal. Russia's centralised architecture is more vulnerable to cascading failure than Ukraine's distributed organisation under identical stress conditions, and Ukraine's wartime adaptation toward mission command has widened this gap further. These are not advantages that depend on a specific weapons system, a particular battle, or the continuation of any single external support arrangement. They are properties of organisational architecture itself. Moreover, these structural advantages sit alongside other factors that jointly explain Ukrainian resilience, including Western material and intelligence support, leadership and training, and population mobilisation. The SOC model isolates the structural component that conventional attrition analyses miss.

Second, both systems will remain critically engaged. The SOC framework provides no basis for predicting the outcome of this war. In systems at criticality, the same perturbation can produce a trivial local effect or a catastrophic system-wide cascade, and there is no way to determine in advance which it will be. Assessments that project specific timelines for Russian collapse or Ukrainian exhaustion lack a reliable foundation. The model suggests that Russia's structure is more fragile and Ukraine's more resilient, and that this asymmetry shows no sign of reversing.

Third, the analysis must extend beyond the battlefield to the strategic interests of the parties' international supporters. Russia depends on China for financial, material, and technological support to sustain its war effort. For China, the calculus is shifting. Sustained support for an increasingly costly and structurally fragile Russian military effort must be weighed against the value of stable economic and diplomatic relations with the European Union, relations that continued association with Russia's war progressively undermines. As the α differential makes clear, China is investing in the more fragile system.

Fourth, the diplomatic landscape reflects these structural realities. Russia's preferred path to resolution (a peace arrangement brokered by the United States without substantive involvement from the EU and NATO) would yield significant concessions at minimal cost. But European and NATO capitals have observed what the SOC model formalises: that Russia is weakened, structurally fragile, and bleeding at rates its organisational architecture cannot efficiently manage. There is little prospect that Ukraine's structural advantages will diminish. On the contrary, the escalating international condemnation of documented war crimes introduces an additional amplifying mechanism that

operates alongside the military and political cascades analysed in this article. The demand for accountability (reparations for destruction, the return of children unlawfully transferred from occupied territories, and the prosecution of commanders and personnel responsible for atrocities) adds layers of political and legal stress to the Russian system that extend well beyond the battlefield. These demands do not dissipate with a ceasefire; they accumulate, compounding the cascading pressures that Russia's centralised architecture is least equipped to absorb.

Finally, this study points toward a broader research agenda. The model introduced here addresses military organisational structure, but the SOC framework is not limited to the battlefield. Economic systems, political institutions, supply chains, and alliance architectures are all complex adaptive systems subject to criticality. Extending the model to capture these dimensions and applying it across other active and historical conflicts represents a natural and promising direction for future research. Ukraine's resistance has demonstrated that a smaller force, organised for resilience, can withstand a larger adversary. That lesson extends far beyond this war. The SOC model developed here provides the analytical foundation to act on it.

References

Albert, Réka, Hawoong Jeong, and Albert-László Barabási. 2000. “Error and Attack Tolerance of Complex Networks.” Nature 406 (6794): 378–382. https://doi.org/10.1038/35019019.

Allison, George. 2024. “Russian casualties reach record highs in Ukraine“. *UK Defence Journal*, December 6, 2024. https://tinyurl.com/3hsvezfy.

Bak, Per, Chao Tang, and Kurt Wiesenfeld. 1987. “Self-Organised Criticality: An Explanation of 1/f Noise.” Physical Review Letters 59 (4): 381–384.

Bak, Per, Chao Tang, and Kurt Wiesenfeld. 1988. “Self-Organised Criticality.” Physical review A: General physics 38(1): 364–374. https://doi.org/10.1103/PhysRevA.38.364.

Bondar, Kateryna. 2025. How Ukraine Rebuilt Its Military Acquisition System Around Commercial Technology. CSIS Report. Washington, DC: Center for Strategic and International Studies, January 2025. https://tinyurl.com/5eey9fan.

Bramsen, Isabel, Isak Svensson, and Peter Wallensteen. 2025. “Making Peace Great Again? The Challenges and Potentials of Trump’s Approach to Peace Diplomacy.” Commentary, The Global Observatory, March 25, 2025. https://tinyurl.com/4aabjuh2.

Cederman, Lars-Erik. 2003. “Modelling the Size of Wars: From Billiard Balls to Sandpiles.” *American Political Science Review* 97 (1): 135–150. https://www.jstor.org/stable/3118226.

Clausewitz, Carl von. 1976. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press.

Carlough, Molly, and Benjamin Harris. 2025. “Comparing the Size and Capabilities of the Russian and Ukrainian Militaries.” Policy explainer, *Council on Foreign Relations*, June 3, 2025. https://tinyurl.com/ypj55uf2.

Congressional Research Service. 2026. Russian Military Performance and Outlook, by Andrew S. Bowen. CRS Report IF12606. Washington, DC: Library of Congress. https://tinyurl.com/yz3vnjpu.

Davies, Shawn, Therése Pettersson, Margareta Sollenberg, and Magnus Öberg. 2025. “Organised Violence 1989–2024, and the Challenges of Identifying Civilian Victims.” *Journal of Peace Research* 62 (4): 1223–1240. https://doi.org/10.1177/00223433251345636.

Dobias, Peter. 2009. “Self-Organised Criticality in Asymmetric Warfare.” *Fractals* 17 (1): 91–97. https://doi.org/10.1142/S0218348X0900417X.

Dong, Gaogao, Jingfang Fan, Louis M. Shekhtman, Saray Shai, Ruijin Du, Lixin Tian, Xiaosong Chen, H. Eugene Stanley, and Shlomo Havlin. 2018. “Resilience of Networks with Community Structure Behaves as If under an External Field.” Proceedings of the National Academy of Sciences 115 (27): 6911–6915. https://doi.org/10.1073/pnas.1801588115.

Fragile States Index. 2024. *Fragile States Index 2024*. Washington, DC: The Fund for Peace. https://fragilestatesindex.org/.

Freedman, Lawrence. 2015. *Strategy: A History*. New York: Oxford University Press.

Grau, Lester W., and Charles K. Bartles. 2016. *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces*. Fort Leavenworth, KS: Foreign Military Studies Office, U.S. Army. https://tinyurl.com/3m8njd9m.

Grau, Lester W., and Charles K. Bartles. 2022. “Getting to Know the Russian Battalion Tactical Group.” *Royal United Services Institute (RUSI)*, April 14, 2022. https://tinyurl.com/yuba95kz.

Hird, Karolina, Grace Mappes, Kateryna Stepanenko, Christina Harward, Davit Gasparyan, Daria Novikov, Frederick W. Kagan, and Nate Trotter. 2025. “Russian Offensive Campaign Assessment, March 4, 2025.” Daily assessment, Institute for the Study of War. https://tinyurl.com/mrysdvyv.

Hooker, Richard D., Jr., and Hlib Parfonov. 2025. *Order of Battle of the Ukrainian Armed Forces*. Special Report. Policy Brief. Washington, DC: Jamestown Foundation. https://tinyurl.com/35tx74ww.

International Institute for Strategic Studies. 2022. *The Military Balance 2022*. London: Routledge. https://tinyurl.com/59u3as44.

Jones, Seth G., and McCabe, Riley. 2025. *Russia’s Battlefield Woes in Ukraine*. CSIS Briefs. Washington, DC: Center for Strategic and International Studies, June 2025. https://tinyurl.com/2vyfrdpm.

Jones, Seth G., and Riley McCabe. 2026. *Russia’s Grinding War in Ukraine: Massive Losses and Tiny Gains for a Declining Power*. CSIS Briefs. Washington, DC: Center for Strategic and International Studies, January 2026. https://tinyurl.com/yjsh8ep8.

Kelly, Laura. 2024. “Johnson Rejects Biden Request for $24 Billion on New Ukraine Aid.” *The Hill*, April 12, 2024. https://tinyurl.com/22t9ydb8.

Kofman, Michael, and Rob Lee. 2023. “Perseverance and Adaptation: Ukraine’s Counteroffensive at Three Months.” *War on the Rocks*, September 4, 2023. https://tinyurl.com/yarwfu3w.

Kuran, Timur, and Cass R. Sunstein. 1999. “Availability Cascades and Risk Regulation.” *Stanford Law Review* 51 (4): 683–768. https://doi.org/10.2307/1229439.

Mann, Michael. 1993. The Sources of Social Power, Volume 2: The Rise of Classes and Nation-States, 1760-1914. Cambridge: Cambridge University Press.

McCabe, Riley. 2025. “Aid Cuts Make Peace Negotiations in Ukraine Less Likely.” Center for Strategic and International Studies, June 16, 2025. https://tinyurl.com/5a7v8ta6.

McEnany, Charles and Roper, Daniel S. 2024. “The Russo-Ukrainian War: Protracted Warfare Implications for the U.S. Army.” *AUSA Spotlight* 24-2, October 1, 2024. Association of the United States Army. https://tinyurl.com/4x3hh5z4.

Mitrović, Miroslav, and Bojanić, Dragan. 2021. “Battalion Tactical Groups of the Russian Armed Forces in the Altered Physiognomy of Modern Conflicts.” *Vojno delo* 73 (2): 44–59.

North Atlantic Treaty Organization. 2026. “Remarks by NATO Secretary General at the World Economic Forum, Davos, 21 January 2026.” https://tinyurl.com/mw84t5bv.

Parfonov, Hlib. 2025. “Ukraine’s Military Transitioning to Corps-Based Command Structure.” Jamestown Foundation, November 24, 2025. https://tinyurl.com/pjfkammh.

RFE/RL’s Ukrainian Service. 2024. “Russia Reportedly Suffered Record 1,500 Casualties Daily in October”, November 10, 2024, https://tinyurl.com/yms88pk4.

Rutte, Mark. 2026. “Remarks by NATO Secretary General at the World Economic Forum, Davos.” Speech, North Atlantic Treaty Organization, 21 January 2026. https://tinyurl.com/mw84t5bv.

Ryan, Mick. 2025. “Military Training Lessons from Ukraine.” Commentary, The Interpreter (Lowy Institute), October 29, 2025. https://tinyurl.com/3xjyuwsr.

Salvaña, Mary Lai O., Bolingot, Harold Jay M. and Tangonan, Gregory L. 2026. “A Self-Organised Criticality Model of Extreme Events and Cascading Disasters of Hub-and-Spoke Air Traffic

Networks." *International Journal of Disaster Risk Reduction* 133: 1-13. https://doi.org/10.1016/j.ijdrr.2026.106009.

Shai, Saray, Dror Y. Kenett, Yoed N. Kenett, Miriam Faust, Simon Dobson, and Shlomo Havlin. 2015. "Critical Tipping Point Distinguishing Two Types of Transitions in Modular Network Structures." Physical Review E 92 (6): 062805. https://doi.org/10.1103/PhysRevE.92.062805.

Sundberg, Ralph, and Erik Melander. 2013. "Introducing the UCDP Georeferenced Event Dataset." Journal of Peace Research 50 (4): 523–532. https://doi.org/10.1177/0022343313484347.

Taylor, James G. 1974. "Lanchester-Type Models of Warfare and Optimal Control." *Naval Research Logistics Quarterly* 21 (1): 79–106. https://tinyurl.com/3ck3mc8h.

Tversky, Amos, and Kahneman, Daniel. 1973. "Availability: A Heuristic for Judging Frequency and Probability." *Cognitive Psychology* 5 (2): 207–232. https://doi.org/10.1016/0010-0285(73)90033-9.

Zartman, I. William. 2008a. "The Timing of Peace Initiatives: Hurting Stalemates and Ripe Moments." In Peacemaking in International Conflict: Methods and Techniques, edited by I. William Zartman and J. Lewis Rasmussen, 225–250. Washington, DC: United States Institute of Peace Press.

Zartman, I. William. 2008b. Negotiation and Conflict Management: Essays on Theory and Practice. New York: Routledge.