British Journal of Political Science (2026), **37**, 1–19

CAMBRIDGE UNIVERSITY PRESS

ARTICLE TYPE

Strategic Interdependence: How Combatants Manage Collective Institutions During War

Nadiya Kostyuk,[*,1] Jon Lindsay,[2] Eunji Emily Kim,[3] Aniket Anand,[4] Zachary Bischof,[5] Amanda Meng,[5] and Alberto Dainotti[2]

[1]Assistant Professor, Carnegie Mellon Institute for Strategy and Technology, Carnegie Mellon University
[2]Associate Professor, Georgia Institute of Technology
[3]PhD Candidate, Georgia Institute of Technology
[4]PhD Student, University of Chicago
[5]Researcher, Georgia Institute of Technology
[*]Corresponding author. Email: nkostyuk@andrew.cmu.edu

Abstract

This article challenges the view that war and interdependence are inherently incompatible by examining how combatants manage collective institutions during conflict. Using the Internet as a case of such an institution, we show that belligerents selectively preserve or disrupt mutual access based on battlefield conditions. Disruption is more likely during mobile offensives, which offer greater operational freedom, while static or constrained operations incentivize maintaining interdependence for coordination, intelligence, or deception. Drawing on geolocated data from Internet outages in the Russia–Ukraine war (2022–2023) and qualitative evidence from this conflict and the Armenia–Azerbaijan conflicts (2020, 2023), we find that the disruption likelihood declines as battlefield constraints increase. These findings reveal how interdependence can serve as a tactical asset rather than merely a casualty of war. This has important implications for understanding the relationship between institutions and conflict, as wartime strategies shape not only battlefield outcomes but also prospects for post-war peacebuilding.

Keywords: collective institutions; conflict; cooperation, interdependence; military strategy; battlefield conditions

1. Introduction

Since Russia's full-scale invasion in February 2022, both Russia and Ukraine have at times disrupted and at other times preserved the Internet—a collective institution based on shared infrastructure and protocols vital for information access and coordination. The observed fluctuations in how belligerents treat the Internet challenge the common assumption that combatants are more likely to destroy than to deliberately safeguard mutual interdependence during war. While Russia carried out more than twenty documented Internet outages in 2022 alone, it more often preserved Internet access in order to exploit cyberspace for intelligence gathering and disinformation (AF Brantly and N Brantly 2024).

This case highlights an increasingly urgent yet underexplored question in international relations (IR): *How do combatants navigate interdependence during wartime?* Much existing scholarship views interdependence and conflict as fundamentally incompatible, highlighting how shared institutions (e.g., trade agreements, humanitarian aid routes, the Internet) foster peace and how war disrupts institutional cooperation (Crescenzi 2003; North et al 2009; Oneal and Russett 2001). However, recent research suggests that the relationship between collective institutions and conflict is not always negative (Carnegie 2021; Goddard 2018). Institutions may not only survive war but also be deliberately maintained or strategically manipulated in ways that support military aims. Building on this scholarship, we argue that institutions can become operational tools of warfare, selectively

disrupted or preserved by combatants depending on the tactical demands and constraints they face on the battlefield.

We explain this variation by theorizing how different wartime strategies—maneuver, attrition, and punishment—shape the incentives and constraints combatants face in deciding whether to maintain or disrupt shared institutions. Specifically, we argue that battlefield dynamics influence the feasibility and desirability of institutional disruption. Attackers engaged in maneuver warfare are more likely to disrupt common institutions to gain surprise and disorient defenders. Defenders against such maneuver operations, by contrast, face greater constraints and are more reliant on institutional continuity for coordination. In attrition warfare, the relative stability of frontlines encourages selective use of shared institutions by all combatants, while punishment campaigns in enemy-held areas pose unique challenges that often incentivize preserving connectivity.

We test our theory using the ongoing war in Ukraine—a conflict of immense geopolitical significance. Importantly, it presents a hard case for our theory due to potential data biases stemming from underreported cyber operations and unintended disruptions during intense attrition warfare. Finding support for our theory in this scenario only strengthens its reliability.

This article makes several contributions. Theoretically, it challenges prevailing views, which tend to posit either a negative or positive relationship between collective institutions and warfare by focusing on that relationship at *the onset and termination of a conflict*. In contrast, we shift the focus to the fluctuating patterns of interdependence *during wartime*, showing how institutions are actively managed in response to shifting battlefield conditions. The Ukraine war provides rich temporal and geographic variation in battlefield dynamics, allowing us to develop a nuanced, locality-based measure of military strategy—advancing prior research that often assumes a single dominant strategy per war (Stam 1998) or battle (Biddle 2004). By grounding our analysis in the conduct of war rather than its causes or outcomes, this study advances both the study of wartime strategy and broader IR debates on institutional resilience under conditions of armed conflict.

Methodologically, we advance empirical research on the micro-dynamics of conflict by introducing a new measure of battlefield strategy and a novel approach to capturing Internet disruptions during war. Collaborating with computer science co-authors, we develop tools that detect geolocated, daily Internet outages—moving beyond prior approaches focused on broad, prolonged national shutdowns. Drawing on quantitative analysis of these disruptions, as well as qualitative evidence from Ukraine and the 2020 and 2023 Armenia–Azerbaijan conflicts, we find robust support for our theoretical claims, demonstrating that the strategic targeting and management of Internet connectivity is not unique to Ukraine but reflects a broader pattern across contemporary conflicts (Access Now 2021, 2024).

2. Institutions and Conflict

Institutions are generally defined as the "rules of the game" that structure human interactions (North 1990; Ostrom 1990). By establishing shared expectations and reducing uncertainty, institutions promote coordination and increase interdependence among actors (Morrow 2014). This interdependence has traditionally been seen as incompatible with war. Classic IR scholarship associates strong institutions with peace and conflict resolution, and it views war as a breakdown of cooperative order (Waltz 1979). Accordingly, much research has focused on how institutional strength reduces the likelihood of war (Oneal and Russett 2001) or how war undermines institutional durability.

However, recent scholarship has begun to complicate this binary. Scholars now show that institutional interdependence can be exploited during conflict rather than merely undermined. Institutions can serve as platforms for covert competition, intelligence collection, and strategic manipulation (Carnegie 2021; Farrell and Newman 2019). Actors may weaponize institutional ties to shape asymmetric dependencies or project influence through seemingly cooperative mechanisms (Goddard and Nexon 2016; Lindsay 2025). These insights suggest that institutions may not only

persist but actually play functional roles during conflict, especially when actors find strategic advantage in maintaining them.

Building on this work, our approach shifts the focus from whether institutions prevent or survive war to how they are actively used as tools during wartime operations. We develop a theory of institutional status that is grounded in the strategic demands of different military campaigns. While much of the literature treats the relationship between conflict and institutions as either structurally negative or positive, we emphasize that institutional interdependence is not static but varies across time and space in response to shifting battlefield conditions. That is, depending on an actor's battlefield position and strategic constraints at a given moment, the actor may maintain institutions like the Internet in order to use or exploit them—for communication, intelligence, or influence—or the actor may disrupt those institutions in order to deny those same advantages to an opponent.

By focusing on the micro-dynamics of warfighting—particularly how combatants manage interdependent institutions like the Internet—we contribute to a growing body of research that moves beyond war onset and termination to examine the tactical logic of conflict behavior. In doing so, we show that institutional interdependence can be a flexible asset shaped by wartime strategy, with implications not only for how conflicts are fought but also for how peace is rebuilt—depending on whether and how institutions are preserved or damaged during war.

3. A Theory of Institutional Status in Wartime

Our theory of institutional status centers on two strategic options: actors can either maintain or disrupt collective institutions. We broadly define *disruption* as a deliberate decision by combatants to interrupt collective institutions during conflict. We contrast disruption with *maintenance*, the deliberate decision to preserve institutions. Among the many collective institutions that can operate during wartime—such as trade networks and humanitarian aid organizations—we have chosen to focus on the Internet. This choice reflects both its empirical traceability and its theoretical value as a paradigmatic case of institutional interdependence under fire.

While commonly understood as infrastructure, the Internet also functions as a collective institution because it is governed by shared rules, protocols, and technical standards that enable coordination and communication at scale. These non-material elements—such as the Transmission Control Protocol/Internet Protocol, Border Gateway Protocol, and Domain Name System—bind disparate systems together, making the Internet a system of human-devised constraints that structure interaction. In this sense, the Internet is a sociotechnical institution, blending material components (like fiber-optic cables and servers) with normative and rule-based components (like routing protocols and access policies).[1]

An institutional interpretation of the Internet (DeNardis 2014) also diverges from the common view of cyberspace as a geographic 'domain' like air, sea, or outer space (Branch 2021). In physical domains like airspace, denying access to a rival makes the domain easier to exploit. In contrast, restricting others' Internet access simultaneously limits one's own; conversely, maintaining open access allows everyone to benefit.[2] This characteristic highlights a common feature of collective institutions: institutional disruption negates benefits for all parties while institutional maintenance preserves institutional benefits and opens avenues for exploitation to all.

This dual nature of institutional interdependence—offering both opportunity and vulnerability—raises a broader strategic question: *How do combatants decide when to preserve or disrupt access to collective institutions in wartime?* To answer this question, we first define these two options and then

[1]Following North (1990), institutions can impose both material constraints (e.g., architectural barriers) and normative constraints (e.g., legal or social rules). In practice, technologies like the Internet blend both. For example, a firewall is a physical and logical constraint that enforces normative content restrictions. See also Lindsay (2017) and Jepperson (1991).

[2]Even when militaries use private networks to secure their communications, they still rely on shared core protocols and infrastructure. Moreover, most modern militaries depend heavily on civilian information and communication technologies, including the public Internet (e.g., Russian forces in Ukraine have used Google maps for navigation).

show how variation in operational constraints—shaped by time and space depending on the military strategy employed—influences these choices.

3.1 Institutional Disruption versus Institutional Maintenance

Strategic *disruption* of collective institutions in wartime can take many forms. For example, toward the end of World War I, German forces intentionally disrupted logistics routes and relief supply chains—previously used to facilitate trade and food aid in occupied areas—to gain territorial advantage. Where the institution's primary utility is to enable communication, as with the Internet, *disruption* becomes a strategy to incapacitate an enemy's communication, thereby disrupting military command and control. The military logic is straightforward: a force unable to communicate is more vulnerable to defeat. This logic underpins both historical cases—like Britain severing Germany's telegraph cables in 1914 —and modern-day disruptions to Ukraine's digital infrastructure.

Yet combatants do not always choose disruption. Institutional *maintenance* can offer significant strategic advantages, particularly through *exploitation*—which we define broadly as subversion of a collective institution's normal function to gain a competitive edge. During World War I, for example, both sides used trade and humanitarian-organizational channels to smuggle military supplies disguised as civilian aid. In the Internet context, exploitation often involves cyber operations for intelligence gathering or dissemination of (dis)information.

This trade-off between disruption and maintenance reflects a core tension of institutional interdependence: shared systems enhance both capability and vulnerability. As shown in Table 1, disruption and maintenance strategies impose distinct costs and benefits, forcing combatants to weigh the military pros and cons of each.

Table 1. Institutional disruption versus institutional maintenance

Strategy	Pros	Cons
Disruption	Eliminates institutional benefits for the target	Also eliminates institutional benefits for the attacker
Maintenance	Preserves institutional benefits for the attacker	The attacker retains institutional benefits; increases risk of counterintelligence exposure

3.2 Institutional Status and Battlefield Constraints

Classic IR theory often treats war as an anarchic environment where institutions collapse (Waltz 1979). However, we argue that institutions can persist in war—not as relics of peacetime, but as actively contested tools, shaped by strategic incentives. This perspective builds on research that views institutionalization and anarchy as dynamic rather than binary conditions (Lake 2009; Mcconaughey et al 2018). In this sense, we also argue that war is not monolithic: constraints on combatants fluctuate over time and shape their decisions to either disrupt or maintain collective institutions.

Prior research identifies several sources of constraints—geography, logistics, audience costs (Carr and Tanczer 2018), deterrence (Gannon et al 2024), alliances, and peacekeeping operations (Lanoszka 2022)—but overlooks the influence of combat dynamics themselves. Wars are episodic, often alternating between fluid movements and static, sustained engagements. These shifts affect the degree of battlefield control a combatant enjoys—and, with it, their freedom of action. We focus on three core military strategies—maneuver, attrition, and punishment—each associated with distinct combat dynamics (Pape 1996; Stam 1998). Our central claim is that *operational freedom drives institutional disruption, while constraint favors institutional maintenance.*

While our theory models combatant organizations as unitary actors, we recognize that deviations from high command strategy can occur at the tactical level due to principal-agent problems.

Nevertheless, modern military technologies—such as real-time communication, GPS coordination, and surveillance systems—can reduce information asymmetries and enhance command-and-control capacity, even in fluid battlefield environments. Moreover, contemporary doctrines often emphasize "mission command," granting local autonomy within the bounds of a shared strategic intent. As a result, decentralized or autonomous actions frequently remain aligned with broader institutional goals. Our focus, therefore, remains on explaining aggregate patterns in targeting behavior rather than assuming perfect hierarchical control.

3.2.1 Maneuver Strategy: High Freedom, High Disruption Incentives

Maneuver warfare is a military strategy that emphasizes speed, mobility, and flexibility to gain operational advantage by disrupting the enemy's decision-making. It focuses on exploiting weaknesses in the opponent's disposition while maintaining control over one's own forces and freedom of action.

Even though mobility is a typical feature of both offensive and defensive combatants in maneuver warfare, the two sides differ markedly in their levels of control and freedom—and, therefore, in their level of constraints—during maneuver. *Offensive* combatants initiate maneuver when they are least constrained by combat dynamics—i.e., when they have greatest control over the battlefield, with the freedom to decide when and where to strike. Therefore, offensive maneuver warfare is proactive and aggressive, focusing on rapid, decisive movements to seize initiative and exploit enemy weaknesses. It prioritizes secrecy and surprise to break through defenses and sow destabilizing confusion within enemy ranks.

The dynamic nature of maneuver warfare makes institutional disruption attractive to offensive combatants for several reasons. When attempting to force openings and create chaos within enemy ranks, it makes sense for offensive combatants to disrupt collective institutions, such as communication networks or logistical systems, to create opportunities for surprise and significantly hinder the enemy's ability to coordinate and respond effectively, thereby amplifying the offensive actor's advantage. Additionally, communication disruption heightens confusion within enemy ranks and within the civilian population that supports them, increasing the psychological shock of maneuver. Disruption operations are also often easier to plan than intelligence exploitation, as they focus on blocking communications rather than managing an ongoing intrusion. This simplicity is particularly valuable in the context of maneuver warfare, given the complexity of the combined-arms approach that often characterizes this strategy.

Unlike offensive conduct in maneuver warfare, which is proactive, *defensive* conduct in maneuver is largely reactive, focused on responding to the initiatives of offensive forces by absorbing enemy attacks while maintaining flexibility for counterattacks. Defensive combatants use tactics like fortifying positions and delaying actions, with a primary goal of preserving the status quo. As a result, defensive combatants are most constrained during maneuver warfare, as it is the combat dynamic in which they have the least control over the battlefield. In this context, defensive forces are less likely than offensive forces to disrupt collective institutions during maneuver warfare for the following reasons.

First, maintenance of collective institutions can be crucial for sustaining defensive operations, managing resources, and coordinating responses. For example, the Internet serves as a vital communication tool, enabling defenders to organize, share information, and maintain a degree of operational coherence despite pressure from offensive actions. While defenders might not have many opportunities to exploit shared institutions (e.g., to use the Internet for intelligence collection or influence operations), preserving them provides stability and resilience, enabling defenders to remain operational despite constant offensive threats.

Second, while disruption operations are often simpler to execute than institutional exploitation, they may nevertheless require more logistical effort than defensive combatants can afford to expend during fast-moving maneuver warfare, diverting precious resources and attention from more urgent counterresponses to offensive operations. Additionally, because far-less-constrained offensive

combatants are more likely to target shared institutions when they initiate maneuver, they may preemptively undermine defenders' ability to do so.

This underscores the role of strategic interaction in shaping combatants' decisions to disrupt institutions. Actors must consider not only their own operational constraints but also how their adversary might respond to, or preempt, such actions. Disruption is most attractive when combatants expect their efforts will catch the enemy off-guard or strike at a moment of heightened vulnerability. For offensive combatants, this moment often comes early in a maneuver campaign, when speed and surprise are paramount. For defensive combatants, however, maneuver warfare tends to be less conducive to disruption. Their primary focus is preserving control and countering enemy advances—tasks that demand coordination, logistical stability, and—often—the very institutional infrastructure that disruption would undermine.

> **Hypothesis 1A (Offensive vs. Defensive Maneuver):** *During maneuver warfare, offensive combatants are more/less likely than defensive combatants to disrupt/maintain institutions (Internet connectivity).*

3.2.2 Attrition Strategy: Mutual Constraints, Strategic Maintenance

Attrition warfare occupies a middle ground between the extreme freedom of offensive maneuver and extreme constraints of defensive maneuver, imposing a relatively high degree of constraints on both sides. This relative equalizing of battlefield control makes it more difficult to distinguish between offensive and defensive operations in attrition warfare. We therefore do not make this distinction in our hypotheses regarding attrition warfare when comparing it to offensive and defensive maneuvering.[3]

While maneuver prioritizes mobility, attrition is marked by relative stasis, in that it is conducted by combatants entrenched along a well-defined geographical front, whose mutual goal is to gradually wear down the enemy's strength and exhaust enemy resources through sustained attacks. In this sense, attrition is a relatively stable combat dynamic, even as it is also a costly one in terms of lives and resources. Over time, predictable patterns emerge: Front lines become more defined and static, defenses strengthen, and supply lines are established to allow forces to regroup and resupply in safer rear areas. Unlike maneuver warfare, where tactical decision-making is decentralized to allow frontline commanders to adapt quickly, attrition warfare often involves more centralized command and control, with logistics and civil infrastructure developing along the front. This predictability can make the tempo of battle so routine that the risks of war may be taken for granted by soldiers, politicians, and civilians, alike.

While the mutual constraints of attrition warfare limit combatants' flexibility, its predictability enables sustained operations, making maintenance of collective institutions both more feasible and more desirable than disruption. In an attrition-based stalemate, where both sides seek ways to break the deadlock, stable institutions become crucial because they provide opportunities for exploitation. Specifically, combatants can leverage Internet connectivity for cyber or influence operations. Maintaining normal connectivity can lull the enemy into a false sense of security, setting the stage for intelligence-gathering via cyber-espionage operations to identify weaknesses, plan future offensives, and provide early warning of enemy attacks. Internet-based propaganda and disinformation that target civilian and military forces, or even international audiences, can undermine the enemy's morale, weaken internal cohesion, and boost support for friendly forces.

[3] We do not examine the distinction between offensive and defensive constraint levels in attrition warfare, because scholars generally agree that it is challenging to differentiate between offensive and defensive operations in this combat dynamic. While Stam (1998) does differentiate between a state's offensive and defensive doctrines in attrition warfare, the angle of doctrine places the author's focus on identifying the dominant strategy across an entire conflict rather than examining the evolving dynamics within a single conflict. Stam (1998) also relies on expert opinions that assess strategies (i.e., attrition offensive versus attrition defensive) after a conflict ends. In contrast, we aim to study the conflict as it unfolds.

At the same time, the value of functioning institutions in attrition warfare is mutual. For instance, both sides benefit from access to communication and information infrastructure, which is crucial for gathering intelligence that may enable a transition to maneuver operations. Thus, even though each side is aware that the other may exploit these institutions, the strategic benefits of preserving access often outweigh the risks. Rather than deny themselves access by disrupting institutions, combatants in attrition are often willing to accept some degree of vulnerability in exchange for continued exploitation. In this context, the cost of institutional disruption—cutting off one's own access to valuable intelligence and operational coordination—can exceed the benefits of disrupting the enemy's access.

This trade-off contrasts with conditions under maneuver warfare. Attrition warfare is more constrained than offensive maneuvering. The greater freedom offensive combatants have in maneuver warfare, we argue, encourages them to disrupt rather than exploit institutions, given the tactical advantage of maintaining mobility and surprise (*Hypothesis 1B*). In contrast, attrition warfare is less constrained than defensive maneuvering. Despite the stability of the front, combatants in attrition warfare can take more initiative in their actions than can defensive combatants in maneuver warfare, who are largely reactive. This relative freedom, we argue, explains why combatants in attrition warfare are more likely to disrupt collective institutions, such as Internet connectivity, than are defensive combatants in maneuver warfare (*Hypothesis 1C*).

> **Hypothesis 1B (Attrition vs. Offensive Maneuver):** *Combatants are less/more likely to disrupt/maintain institutions (Internet connectivity) when engaged in attrition combat than when conducting offensive maneuver campaigns.*

> **Hypothesis 1C (Attrition vs. Defensive Maneuver):** *Combatants are more/less likely to disrupt/maintain institutions (Internet connectivity) when engaged in attrition combat than when conducting defensive maneuver campaigns.*

3.2.3 Punishment Strategy: Spatial Constraints, Institutional Exploitation

Punishment strategy targets enemy civilians—typically through airstrikes, long-range attacks, or economic blockades. While punishment strategies are traditionally defined by their focus on coercing civilian populations (Pape 1996), we emphasize the location where they take place. The fact that these operations are typically waged in enemy-held areas, away from active frontlines, imposes constraints that shape the institutional choices available to combatants, making institutional exploitation both more attractive and more feasible than disruption.

When combatants lack direct control over terrain, as they do in enemy-controlled territories, they must rely on intelligence gathering, signaling, and indirect influence. In such environments, maintaining access to collective institutions like the Internet becomes strategically useful. Rather than disrupting institutions, therefore, combatants conducting punishment campaigns are more likely to exploit them—for example, to monitor civilian sentiment, spread disinformation, or coordinate remote strikes.

In contrast, when combatants wage attacks on contested territories, they enjoy greater operational freedom. Here, disruption of shared institutions becomes more attractive, as it can degrade enemy coordination, create confusion, and amplify the advantages of initiative and surprise. In contrast, institutions located deeper in enemy-controlled territories may be more heavily defended, making successful disruption more difficult or costly and, as a result, reducing incentives for attackers to disrupt institutions there. It might also be the case that institutions in enemy-controlled areas are already integrated into the enemy's command structure and thus less accessible to frontline combatants. In contrast, shared institutional infrastructure in contested zones often remains exposed and actively used by both sides, making it a more immediate and vulnerable target. Therefore, we argue that combatants are more likely to disrupt institutions such as Internet connectivity in

contested territories, where maneuver and attrition take place, than in enemy-controlled areas, where punishment strategies do.

> **Hypothesis 2 (Punishment):** *Combatants are more/less likely to disrupt/maintain institutions (Internet connectivity) in contested territories—where maneuver and attrition typically occur—than in territories under enemy control, where punishment strategies are more common.*

4. Why We Focus on the War in Ukraine

To test our theory, we focus on Russia's 2022 invasion of Ukraine for three primary reasons. First, as the largest land war since World War II, the case's significance is immense. Second, the Ukraine war is a hard case for our theory due to potential attenuation biases in our data. Internet outages during the conflict could result from either cyber-operations or military actions. If they stem from cyber-operations, the resilience of Ukrainian Internet infrastructure,[4] combined with Western support before and during this war (Kostyuk and A Brantly 2022), could bias our data toward underreporting Russian-sponsored cyber-operations aimed at causing outages. On the other hand, if Internet outages result from military actions, the intensity of brute-force attrition warfare could cause more disruptions, even if the forces did not intend to target the Internet. This would lead to an overrepresentation of actor-attributed outages during attrition warfare compared to offensive maneuver warfare. Finally, by employing cutting-edge techniques from the Internet measurement community, we collect near real-time, micro-level, geolocated data on regional Internet outages. We discuss this unique data, which had not previously been utilized in IR research, in the section below (see Section 5.1).

5. Research Design

Our temporal unit of analysis is a *day*. Our analysis starts on February 24, 2022 (Russia invades Ukraine) and ends on December 31, 2023, covering 676 days of war. Our spatial unit of analysis is a *province* ('oblast') given that this is the smallest spatial unit of the Internet Outage Detection and Analysis (IODA) data. For the main analysis, we cover twenty-four oblasts and the capital city of Kyiv. In all, we have 16,900 oblast-day observations in our data.

Our analysis combines both quantitative and qualitative components. The quantitative analysis examines Russia's use of Internet outages during the war in Ukraine, as the number of such incidents allows for robust statistical testing. Although Ukraine also used Internet outages to disrupt enemy communications, these occurrences were too few for meaningful quantitative analysis.[5] Given the scarcity of Ukraine-attributed outages, we rely on descriptive evidence and anecdotal evidence to demonstrate that Ukrainian actions align with our theoretical expectations (see Online Appendix Section 3). While we use the same data sources to identify our dependent and independent variables for both the Ukrainian and Russian sides, the remainder of the research design and findings section focuses on Russian actions.

5.1 Dependent Variable

Our dependent variable `Rus Internet Outage` is a dummy indicating whether the Russian state—represented by either the government or military—is responsible for disruptions in Internet connectivity on a specific day in a given oblast.

[4]For instance, Ukraine has twenty-five Internet Exchange Points on its borders and many cross connections within them, which improves resilience by enabling the network to route around local outages.

[5]This is unsurprising: Ukraine seeks to reclaim Russia-occupied or contested territories in southern Ukraine, and imposing outages within Russia would likely be viewed as escalatory. Moreover, consistent with our theory, such actions are less frequent in opponent-controlled territories.

To create this variable, we used the following three data sources. Members of our team have pioneered Internet Outage Detection and Analysis (IODA) methods, which employ cutting-edge Internet measurement techniques to monitor digital traffic patterns and identify macroscopic Internet outages (Internet Intelligence Lab 2022). IODA uses four different data sources that employ distinct and complementary methodologies for monitoring Internet connectivity: Border Gateway Protocol announcements, active probing, network telescope data, and Google product traffic (available only at the country level). For this analysis, we focus mainly on IODA's active probing signal, with availability tuned to the oblast level; this displays a more consistent pattern of normal connectivity compared to the sometimes-erratic telescope data and is best able to reflect power outages. Every 10 minutes, the IODA system adaptively probes approximately 3.5 M /24 network blocks worldwide. When /24 network blocks stop responding to IODA's probes, this indicates possible disconnection from the Internet.

To identify Internet outages, we used a daily sum of drops in Internet connectivity for each oblast using both a mean-shift change detection and standard deviation change detection. The mean-shift change detection algorithm identifies longer-duration drops in connectivity due to mean-shift changes in active probing. To identify mean-shift changes, we first divided the time series into 15 segments, with one three-week segment and 14 four-week segments. We applied mean-shift change point detection separately for each of the 15 segments. The results of the mean-shift change were hand inspected to ensure detection of the most apparent mean-shift changes. We employ standard deviation change detection to identify shorter but sharp drops in active probing that may not cause a mean shift but do represent short-duration drops in connectivity. For every oblast, we first selected a week before Russia's invasion as the reference standard deviation and identified all the time intervals where active probing values fall below four standard deviations from the mean of that segment. We used both the mean-shift change and standard deviation to capture a count of drops in connectivity per oblast.

Since IODA data indicates only whether outages occurred and does not detail the reasons behind them, we turned to a second source that identifies outages attributed to Moscow. Specifically, we utilized Access Now's #KeepItOn Shutdown Tracker Optimization Project (STOP), which relies on various local and international news reports, personal accounts, and technical sources[6] to record and contextualize Internet shutdowns (e.g., Russian cyber-attacks on Internet service providers; military operations targeting Internet infrastructure; or soldiers dismantling telecommunication equipment). Since IODA is unable to geolocate satellite network signals, it does not capture the Internet provided by Starlink. To make sure we capture such data, we complemented outages targeting Starlink already recorded in STOP with a few additional instances of such outages collected from public sources.

5.2 Main Explanatory Variable

Our main explanatory variable is a combatant's level of constraints, which is related to the military strategy they employ. According to our theory, maneuver and attrition warfare occur in contested territories along the frontline, whereas punishment warfare is conducted in opponent-controlled territories.

To determine which territories are contested and which are under opponent control, we use Zhukov (2023)'s Violent Incident Information from News Articles (VIINA) (v2.0) to create a factor variable for `Territorial Control`, which has three levels: "Russian occupation," "Contested," and "Ukrainian controlled." A region is classified into one of these categories when at least 80% of its territory is under Russian control, characterized as contested, or under Ukrainian control.[7] Using this classification, we identify operations that take place in contested regions along the frontline as

[6]These sources include Google Transparency Data, Facebook Transparency Report, CloudFlare Radar, and Oracle, among others. For more information on sources and methods, visit https://www.accessnow.org/campaign/keepiton/.

[7]We also use 70% as an alternative cutoff point (see Section 6.2).

maneuver or attrition warfare and operations in Ukrainian-controlled territories, where Russia lacks territorial control and faces greater operational constraints, as punishment.

Having differentiated between maneuver/attrition and punishment warfare based on location, we now turn to distinguishing between maneuver and attrition warfare, both of which occur in contested territories. To identify offensive and defensive maneuver warfare and attrition warfare, we relied on expert assessments provided by reputable research organizations and NGOs that have systematically tracked the progression of the conflict. Chief among these are the Center for Strategic and International Studies, the Institute for the Study of War, and other defense and security think tanks that have published widely-cited operational timelines and analyses. These organizations employ military analysts and regional experts with backgrounds in defense policy, intelligence analysis, and conflict studies, which qualifies them as credible sources for categorizing phases of warfare. Table 1 in Online Appendix Section 1 provides samples of these sources.

Based on these external classifications, we categorize actions on the contested territories as follows: 'Initial invasion' (2/24/22 – 4/7/22) is classified as 'Rus Offensive Maneuver'; the 'Southeastern front' (4/8/22 – 8/28/22), 'Second stalemate' (11/12/22 – 6/7/23), and 'Winter campaigns' (12/1/23 – 12/31/23) are categorizes as 'Attrition'; and 'Ukrainian counteroffensive I' (8/29/22 – 12/11/22) and 'Ukrainian counteroffensive II' (6/8/23 – 11/30/23) are classified as 'Rus Defensive Maneuver.'[8]

We also considered alternative ways to distinguish between maneuver and attrition warfare, such as tracking territorial gains, fatalities, or specific military tactics to capture finer, day-to-day battlefield dynamics. However, each of these measures has significant limitations. Territorial gains reflect successful maneuvers, which represent a small portion of overall maneuver efforts. Furthermore, there is no consensus on how much daily territorial change is needed to distinguish maneuver warfare from attrition warfare. Fatalities are similarly ambiguous—they occur in both maneuver and attrition contexts and often reflect force size or capabilities rather than strategy. Likewise, tactics like airstrikes can serve both offensive and defensive purposes (e.g., in counteroffensive operations), further complicating classification. We discuss these limitations in more detail in Online Appendix Section 1, demonstrating that expert-coded military strategy remains the best measure given the data at hand.

While not without limitations, our approach advances prior work by incorporating both spatial and temporal dynamics, offering a more nuanced understanding of how warfare unfolds across time and space. This approach advances previous work that primarily focuses on a single dominant strategy used either throughout an entire war (Stam 1998) or within a major battle (Biddle 2004).

Figure 1 shows the initiation dates of Russian-sponsored Internet outages (white lines) across the different oblasts. Three patterns stand out. First, outages were more frequent during offensive maneuver than during attrition, even though periods of maneuvering were much shorter. Second, attrition still saw more outages than defensive maneuver. Third, Russia executed fewer outages for punishment in Ukrainian-controlled areas than for maneuvering and attrition along the frontline.

Figure 2, which reports the total number of region-days with Russian-sponsored Internet outages, offers a complementary view by showing how often outages occurred relative to the duration of each strategy. Figure 2a, which focuses on contested territories, indicates that region-days with outages were far more frequent during offensive maneuver than during attrition, and more common during both offensive maneuver and attrition than during defensive maneuver. Figure 2b further shows that contested territories—where maneuver and attrition took place—experienced substantially more region-days with outages than Ukrainian-controlled territories, where Russia employed a punishment strategy.

5.3 Model Choice

[8] Where multiple sources provided overlapping or slightly differing timelines for the start and end dates of these phases, we cross-referenced them and reconciled discrepancies through consensus among expert assessments.

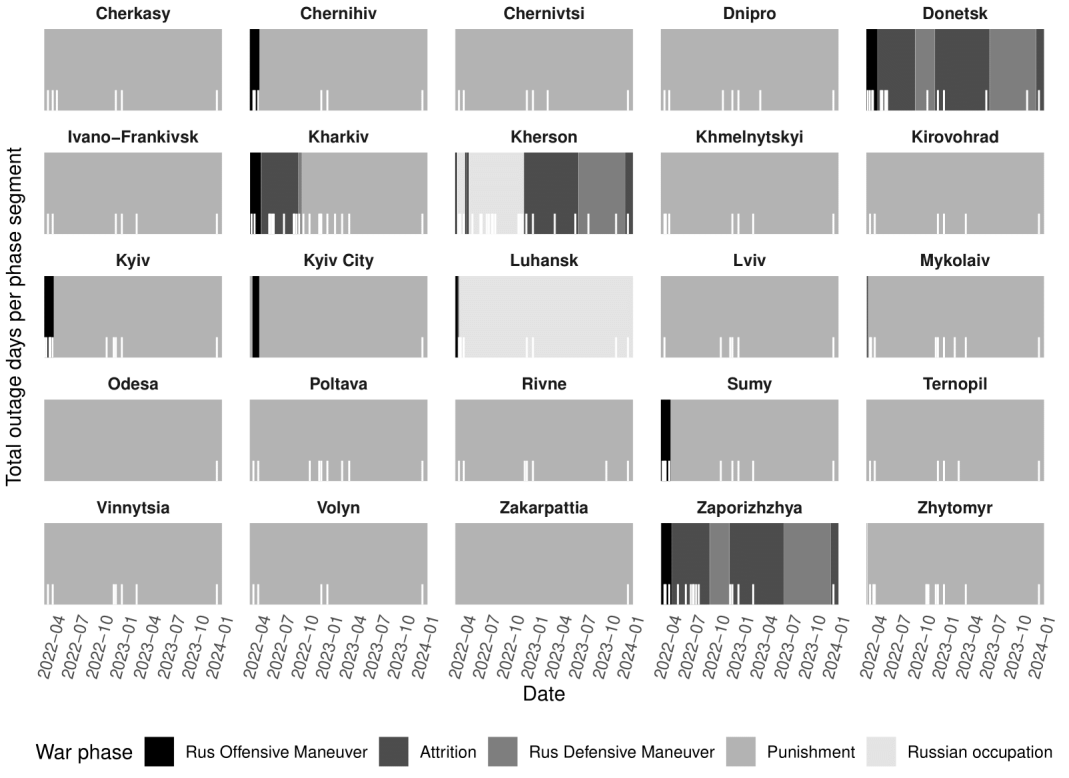


Figure 1. *Russian-sponsored Internet outage initiation (white lines) by oblast during different war strategies in the Russo-Ukrainian conflict.*

5.3.1 Maneuver versus Attrition

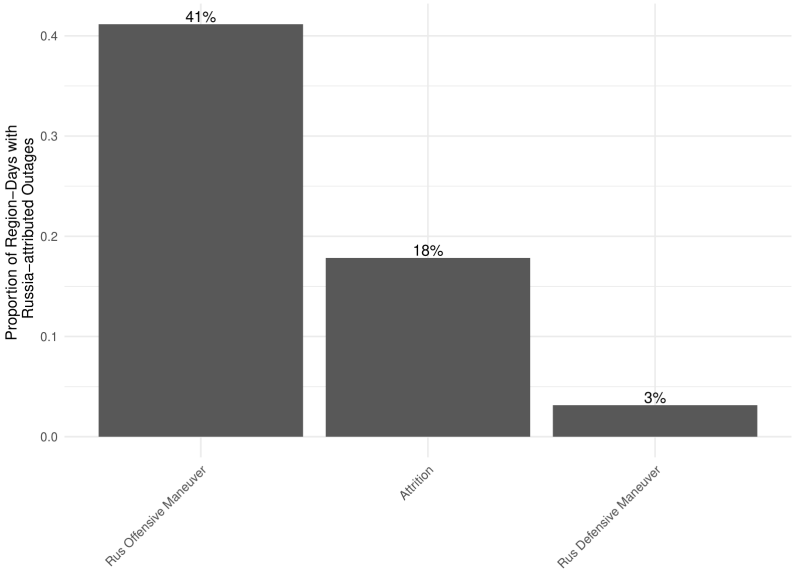
Using data from contested territories,[9] we test our hypotheses related to attrition and maneuver strategies by fitting the following generalized linear model:

$$\begin{aligned} logit(\text{Rus Internet Outage}_{it}, X_{it}) = \beta_0 + \beta_1 * \text{Rus Offensive Maneuver}_{t-1} + \\ \beta_2 * \text{Rus Defensive Maneuver}_{t-1} + \\ \beta_3 * \text{Rus Internet Outage}_{it-1} \\ + GX_{it} + \alpha_i + \epsilon_{it}, \alpha_i \sim_{iid} N(0, \sigma^2_\alpha) \end{aligned} \tag{1}$$

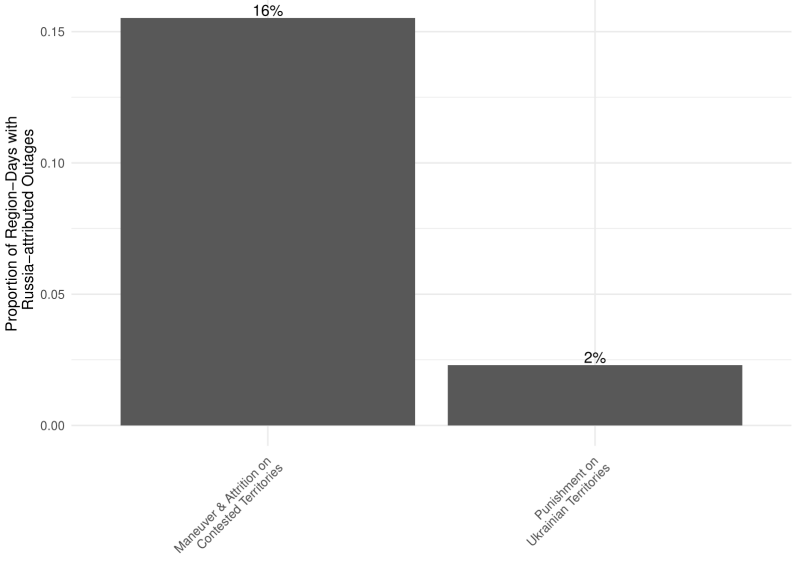
where $\texttt{Rus Internet Outage}_{it}$ is a dummy identifying whether the Russian-sponsored Internet outage occurred in region i on day t, and β_0 is an intercept. The primary exposures $\texttt{Rus Offensive Maneuver}_{it-1}$ and $\texttt{Rus Defensive Maneuver}_{it-1}$ are non-overlapping dummies identifying days during the Russian offensive and defensive maneuver campaigns, respectively, in contested territories on day $t-1$, with days where they both are zero representing the base category of `Attrition`. $X_{it} = [x_{1it}, \ldots, x_{nit}]'$ is a matrix of n exogenous variables, including a number of the Russian military operations in region i on day $t-1$ ($\texttt{Rus Kinetic}_{it-1}$),[10] a dummy variable for Ukrainian, Russian, and Soviet holidays (`Holidays`), and a dummy variable for a weekend (`Weekend`).

[9]Focusing only on contested territories results in 2,141 day-oblast observations.

[10]To account for Ukrainian actions when we study Russia-sponsored outages, we also controlled for Ukrainian military operations (`Ukr Kinetic`) as a robustness check. We excluded `Ukr Kinetic` from the main models due to a high degree of correlation between `Ukr Kinetic` and `Rus Kinetic`. Our results remain robust even when we include `Ukr Kinetic` in



(a) Distribution of Russia-attributed Internet outages during maneuver and attrition warfare in contested territories.



(b) Distribution of Russia-attributed Internet outages in contested territories, where maneuver and attrition warfare occur, versus Ukrainian-controlled territories, where Russia implements a punishment strategy.

Figure 2. *Proportion of region-days with Russia-attributed Internet outages based on different military strategies in its war in Ukraine (2022-2023).*

We control for the number of military operations to account for local variation in combat intensity, which may independently affect the likelihood of Internet outages. Because Internet disruptions can

our models.

sometimes complement or support military activity—for example, by undermining coordination or communication in targeted areas—this control allows us to better isolate the relationship between broader strategic shifts and other patterns of Internet disruption. We use Zhukov (2023)'s Violent Incident Information from News Articles (VIINA) as a source for military operations.[11] We control for holidays and weekends because research indicates a decrease in military activity during these times (Berman et al 2011). Finally, we add oblast (α_i) random effects. ϵ_{it} is an independent error term.

5.3.2 Punishment

Using data from the Ukrainian-controlled and contested territories,[12] we test our punishment hypothesis (*H2*) by fitting the following generalized linear model:

$$\begin{aligned} logit(\text{Rus Internet Outage}_{it}, X_{it}) = \beta_0 + \beta_1 * \text{Rus Punishment in Ukr Territories}_{t-1} + \\ \beta_2 * \text{Rus Internet Outage}_{it-1} \\ + GX_{it} + \alpha_i + \epsilon_{it}, \alpha_i \sim_{iid} N(0, \sigma^2_\alpha) \end{aligned} \tag{2}$$

where $\texttt{Rus Internet Outage}_{it}$ is a dummy identifying whether the Russian-sponsored Internet outage occurred in region i on day t, and β_0 is an intercept. The primary exposure $\texttt{Rus Punishment in Ukr Territories}_{it-1}$ is a dummy identifying whether region i was under the Ukrainian or contested control on day $t-1$. Therefore, β_1 represents the difference on the log-odds scale in Russian-attributed outages between the Ukrainian-controlled territories, where outages are interpreted as punishment, versus contested territories, where they are used during combat. All other terms are the same as defined in Equation 1.

6. Findings: Russia's use of Internet outages in Ukraine war

This section presents the results from the quantitative analysis of Russian use of Internet outages in the war in Ukraine (see Table 2). The analysis of Ukrainian actions appears in Online Appendix Section 3. Evidence from both sides confirms that actors strategically employ Internet disruptions more frequently during their offensive maneuver campaigns than during attrition or defensive maneuver combat, all of which take place on contested territories. Moreover, Internet outages tend to occur at a higher rate on contested territories than on enemy-controlled territories, where actors practice punishment.

6.1 Main Results

Table 2 presents the obtained results. The reported values in this table are the odds ratios and confidence intervals. Odds ratios larger than 1 identify positive correlation, and those smaller than 1 identify negative correlation.

[11] An important consideration when using media-based data in conflict research is the potential underreporting of violent incidents, especially in areas with limited media access or during fast-moving phases of combat. To mitigate these concerns, we rely on the VIINA dataset, which offers substantial advantages over other sources on this war. Unlike automated near-real-time datasets such as GDELT or ICEWS, VIINA draws exclusively on domestic Ukrainian and Russian media, avoiding the biases introduced by international reporting. International outlets tend to prioritize large, high-profile events—often in major cities—while underreporting smaller incidents along the front lines, a pattern that can artificially cluster events in urban centers. This distortion is especially evident in datasets like ACLED, which rely heavily on international news. By using local-language sources and rigorous validation procedures, VIINA provides more consistent and accurate coverage across both time and space, helping reduce many of the underreporting concerns typical of media-based conflict data.

[12] We excluded Russian-occupied territories on days when at least 80% of the oblast was under Russian control (662 days for Luhansk and 240 days for Kherson), reducing the sample from 16,900 to 15,974 oblast-day observations.

Table 2. Russia's use of Internet outages in its war in Ukraine (odds ratios and confidence intervals)

	DV: Rus Internet Outage			
	Attrition versus Maneuver		**Punishment**	
	Model 1 (w/out controls)	*Model 2* (w/ controls)	*Model 3* (w/out controls)	*Model 4* (w/ controls)
Rus Offens. Maneuv (lag)	2.3**(1.29; 4.12)	2.34**(1.31; 4.2)	——	——
Rus Defens. Maneuv (lag)	0.23***(0.11; 0.48)	0.23***(0.11; 0.48)	——	——
Rus Punishment in Ukr Territories (lag)	——	——	0.16***(0.1; 0.26)	0.15***(0.08; 0.25)
Rus Kinetic (lag,log)	——	1.49^(1; 2.22)	——	1.04(0.87; 1.24)
Holidays	——	0.71(0.2; 2.52)	——	0.37^(0.13; 1.01)
Weekend	——	0.46**(0.29; 0.74)	——	0.19***(0.14; 0.27)
Observations	2,141	2,141	15,974	15,974
Log Likelihood	-371.64	-363.87	-1,308.38	-1,247.69
AIC	753.28	743.74	2,624.76	2,509.38

Note: This table examines the use of Internet outages by the Russian military and/or government during different warfare strategies in its war in Ukraine. The reported values are the odds ratios and confidence intervals. Odds ratios larger than 1 identify positive correlation, and those smaller than 1 identify negative correlation. All models contain an intercept, a lag of a dependent variable, and region-random effects. Online Appendix contains complete results. Internet disruptions occur at a higher rate during offensive maneuver combat than during attrition combat or defensive maneuver. Internet outages are less likely to be used as a form of punishment on the Ukrainian-controlled territories than along the frontline on contested territories. ^ p<0.1; * p<0.05; ** p<0.01; *** p<0.001

Model 1 demonstrates how Russia's use of Internet outages varies across different types of combat. The findings indicate that during Russian offensive maneuver campaigns, the odds of experiencing a Russian-sponsored Internet outage are 130% higher than during attrition warfare, which serves as the base category in this model. In contrast, during Russian defensive maneuver campaigns, the odds of experiencing a Russian-sponsored Internet outage are 77% lower than during attrition warfare. These results hold when we account for additional controls in Model 2. For example, there is a 4.44% chance of a Russia-sponsored outage occurring during the Russian offensive maneuver campaign where the other variables are at the reference value of zero. In comparison, the likelihood of an outage during attrition warfare is just 1.95%. During defensive maneuver campaigns, this likelihood drops even further, to only 0.45%.

Together, these results support *H1A-H1C*, confirming that the Kremlin strategically employs Internet disruptions more frequently during its offensive maneuver campaigns than during its attrition or defensive maneuver campaigns. For example, during the 2022 invasion of Ukraine, Russia strategically used Internet outages in its offensive campaigns to disrupt Ukrainian communications, especially in contested regions like Kharkiv and Donetsk, where such disruptions were crucial for military maneuvering. In contrast, during defensive maneuvers, such as in regions like Luhansk, the use of Internet outages was less frequent, as the focus shifted to defending occupied territory rather than disrupting enemy communications.

Models 3 and 4 compare Russia's use of Internet outages as part of its punishment strategy on the Ukrainian-controlled territories versus its use during maneuver and attrition warfare on contested territories. Model 4 demonstrates that the odds of experiencing a Russian-sponsored Internet outage are 85% lower in Ukrainian-controlled territories than in contested territories. For example, there is an 6.8% chance of a Russia-sponsored outage occurring in a contested territory where the other variables are at the reference value of zero. In comparison, the likelihood of an outage on the Ukrainian-controlled territories is just 1%. These results support our hypothesis (*H2*) that Internet

disruption is less likely in punishment contexts, where combatants operate under tighter constraints and instead focus on institutional exploitation.

Models in Table 2 also reveal several interesting relationships between our dependent variable and the control variables. Model 2 shows a positive, marginally significant association between Russian military operations and Internet outages, indicating that such operations may be linked to increased outage likelihood during maneuver and attrition campaigns. The odds of experiencing a Russia-attributed Internet outage are lower on weekends compared to weekdays (e.g., OR: 0.19; CI: (0.14; 0.27) in Model 4).

6.2 Robustness checks and alternative explanations

We conducted a number of robustness checks to further confirm the plausibility of our theory, including (1) the alternative measure of territorial control (i.e., at least 70% as opposed to 80%); (2) the alternative model specification (i.e., probit, fixed effects); (3) the alternative measure of military strategy, which accounts for regional variations within a single war phase; (4) a sensitivity analysis assessing the potential misclassification of outage intentionality; and (5) a model estimated without the lagged dependent variable, treating all days of outage as potentially strategic. Our results remain robust to these tests (see Online Appendix Section 2.3).

Another potential concern is endogeneity, particularly the possibility of reverse causality between institutional disruption and strategic phases. To reduce these concerns, we lag our independent variables—a common approach in related work (e.g., Choi (2022))—and include region fixed effects as well as controls for temporal variation in conflict intensity. We further assessed the sensitivity of our findings to unmeasured confounding using an E-value analysis (Haneuse et al 2019). The E-value represents the minimum strength of association an unobserved confounder would need to have with both the exposure and the outcome to fully explain away the effect. In our case, the E-value is substantially high (see Online Appendix Section 2.3.6), suggesting that unmeasured confounding would need to be very strong to overturn our conclusions. While we remain cautious in making causal claims, the combined evidence suggests that the observed patterns are consistent with our theoretical expectations.

Here, we also consider several alternative explanations relevant to Russia's actions. The first focuses on Russia's significant cyber capabilities, addressing the disparity between an actor's actual and perceived capacity for cyber exploitation. Some might argue that Russia's belief in its cyber prowess for exploitation could explain its reluctance to completely shut down the Internet in Ukraine or to engage in cyber disruption tactics. A state that perceived itself as less capable in cyber exploitation might focus more on disruption. This explanation, however, raises a question: If Russia's actions were based on its reputation as one of the most capable actors in cyber exploitation, why would it resort to Internet outages at all? Moreover, the outages are not random; they exhibit clear territorial and temporal patterns, further undermining this alternative explanation. In fact, Russia's strong capabilities in cyber exploitation make this an even harder case to test our theory, as it represents the least likely scenario for Internet disruptions. Therefore, the support we found for our theory in this unlikely context only underscores the robustness and relevance of our explanations. It also reinforces our central claim that variation in institutional disruption stems not only from cyber capacity, but from the strategic and spatial conditions under which warfare is conducted.

Another alternative explanation—treating the Internet as infrastructure rather than as an institution—posits that Russia's primary goal is to deprive Ukrainians of public goods and disrupt critical infrastructure, making Internet outages a secondary, unintended consequence. If this infrastructure-disruption mechanism were correct, Russian military activity should be positively associated with Internet outages. The results in Model 2 (Table 2) show a positive but marginally statistically significant relationship between Russian military operations and outages during maneuver and attrition campaigns, suggesting at most a weak association. To probe this further, we estimated an additional

model controlling specifically for Russian airstrikes—operations frequently used to target infrastructure. As shown in Online Appendix Section 2.4.1, these results align with our main findings: outages do not appear to be merely a secondary effect of infrastructure attacks. Moreover, Model 4 (Table 2) indicates that Russian military activity is unlikely to drive outages in Ukrainian-controlled areas (OR: 1.04; CI: 0.87–1.24), and this pattern also holds when focusing solely on airstrikes (Online Appendix Section 2.4.1). Together, these results suggest that Russian Internet outages are not simply byproducts of broader destructive operations but are more consistent with a deliberate strategic choice.

We acknowledge that these results do not preclude the possibility that isolated, high-impact strikes on critical infrastructure—such as power substations or telecommunications nodes—may, in some instances, lead to significant disruptions. A single, strategically targeted strike could produce a substantial outage without generating a detectable pattern across the broader dataset. Importantly, the potential for such isolated incidents does not contradict our interpretation; rather, it supports it. The use of precision strikes against Internet infrastructure reflects strategic intent, aligning with our argument that many Internet disruptions are the result of deliberate targeting rather than incidental damage. Thus, while rare outlier events may occur, the absence of a consistent statistical relationship reinforces the conclusion that outages are not primarily unintended consequences of kinetic operations, but often intentional and systematic.

Another possible explanation concerns Ukraine's Internet resilience, which can be attributed to substantial Western support throughout the war. This resilience may influence the number of outages caused by Russia's cyber-operations, as the data captures only successful attempts and does not account for failed attacks. Given the significant boost to Ukraine's cyber defenses from Western support, we might expect to see a decline in the number of outages caused by cyber-operations over time. However, descriptive data, presented in Online Appendix Section 2.4.2, shows that this is not the case by demonstrating a higher number of Internet outages in winter 2023—almost two years into the conflict—compared to earlier phases of the war. Furthermore, even if the increase in resilience were to work, and we observed, as the war progressed, a decreasing number of Russia-sponsored Internet outages resulting from cyber operations, this would introduce a possible attenuation bias, indicating that our data likely represented the lower bound of true outages. As a result, we could conclude that the true coefficients were higher and that our findings underestimated the actual effect size of Internet outages, making our claims more conservative. This would suggest that the relationship between combat dynamics and Internet outages may be stronger than this article reports, further reinforcing our theory.

7. Evidence Beyond Ukraine

Evidence on Internet shutdowns in Azerbaijan, Armenia, India, Israel, Lebanon, Pakistan, and Yemen reveal that Internet connectivity has been a target of both military and cyber campaigns during active conflicts in these nations (Access Now 2021, 2024), suggesting that the lessons we glean about connectivity and combat from the Ukraine war could have broader relevance. To further demonstrate this, Online Appendix Section 4 briefly discusses the 2020 and 2023 Armenia-Azerbaijan conflicts over the Nagorno-Karabakh region. The evidence from both conflicts offers strong support for our theory, illustrating the applicability of our findings to other international disputes.

8. Discussion

This article has shown that combatants' decisions to maintain or disrupt collective institutions during war are not uniform or structurally determined, but, instead, vary predictably with battlefield dynamics. Specifically, we find that the degree of operational constraint—related to military strategy (maneuver, attrition, or punishment)—plays a central role in determining when and where combatants are willing to sacrifice or preserve collective institutions. These findings deepen our

understanding of how institutional interdependence is tactically managed during conflict, shifting the conversation from questions of war onset and termination to those of wartime conduct.

Using the Internet as a representative case of a collective institution, we show that combatants are more likely to disrupt connectivity when engaged in offensive maneuver operations, where a high degree of control and initiative provides opportunities for battlefield momentum and incentivizes prioritizing surprise. Conversely, combatants facing greater constraints—such as defenders in maneuver warfare—are more inclined to preserve Internet connectivity, as they depend more heavily on coordination and communication. Attrition strategies, with their more stable and reciprocal constraints, tend to produce selective disruptions, balancing the costs and benefits of connectivity. Our spatial analysis further reveals that Internet disruptions are concentrated in contested zones and are relatively rare in enemy-held areas, where punishment strategies dominate and institutional preservation may better serve indirect-influence goals.

Our approach is not without limitations, which offer opportunities for future work. Our theory assumes symmetric interdependence, where both sides rely similarly on shared institutional networks. In wartime, however, asymmetric interdependence can emerge when actors insulate themselves from shared networks, gaining strategic advantages while altering mutual vulnerability. For example, Ukraine's use of Starlink enhanced resilience by protecting military communications from Russian attacks on terrestrial infrastructure. Such measures also affect responsiveness, as secure communications enable more coordinated and timely actions. Investigating how asymmetric interdependence is exploited in war—and how actors navigate trade-offs between resilience and responsiveness—represents a promising avenue for future research, complementing what we already know from peacetime contexts (Farrell and Newman 2019).

Our analysis makes two main contributions, one methodological and one substantive. Methodologically, we demonstrate the potential of multidisciplinary collaboration. The Internet measurement community has developed sophisticated techniques for monitoring and characterizing large-scale information systems—including traffic patterns, outages, and protocol usage—that hold tremendous untapped potential for political science research. These data can be used as both dependent and independent variables and serve as proxies for economic interdependence and other political phenomena. In addition, our improved quantitative measure of the military strategies that combatants employ simultaneously across different localities enables near-real-time analysis of battlefield dynamics, providing a deeper understanding of how strategy shapes combatant decision-making as it unfolds. While this measure captures broad, theater-level shifts in strategy, localized variations may also be important. Limited data granularity and uncertainty about the intent behind individual actions currently constrain systematic identification of such patterns, but future access to more detailed operational records—particularly through archival releases—will allow researchers to better assess how micro-level battlefield decisions align with broader strategic objectives.

Our substantive contribution is a new theory of institutional targeting in war. Rather than treating collective institutions as either casualties of war or safeguards of peace, we argue that they are operational resources during conflict—tools to be preserved or disrupted depending on strategic objectives.

Although our empirical focus is on the Internet, our framework may extend to other wartime institutions. For example, in maneuver warfare, combatants may sever supply chains, block humanitarian aid, or disrupt trade to exploit their advantage. In contrast, during stalemates or in enemy-held areas, combatants may deliberately maintain those same institutions, both for strategic gain and to avoid backlash. Historical cases like World War I underscore this logic: Germany's 1918 Spring Offensive disrupted civilian relief efforts in newly captured territory, while earlier attritional phases saw both sides tolerate and exploit neutral trade and humanitarian flows.

Our findings also speak to broader theories of institutional resilience. Even under the extreme conditions of war, shared institutions can persist—not merely as remnants of peacetime order, but as

adaptable instruments shaped by strategic incentives. This supports theories that view institutions not just as constraints, but as political resources with which actors selectively engage (Coase 1981; Cox and McCubbins 2005). The propensity of combatants to preserve institutions under certain conditions illustrates how institutional "stickiness" operates not just in politics and economics, but also in armed conflict.

In conclusion, this study identifies a critical yet overlooked hinge point in international relations: the management of interdependence during war. Rather than collapsing under violence, institutions can be retooled and redeployed in service of war aims, with their fate contingent on shifting strategic demands of wartime operations. It also opens new avenues for IR research by highlighting the tactical, localized, and strategic logics that govern institutional use under extreme conditions.

Crucially, our findings have implications for post-war peacebuilding and the reconstruction of international order. When institutions are preserved or deliberately instrumentalized during war, they do not emerge from conflict as neutral remnants of a previous system but as shaped tools—either degraded or embedded in wartime power structures. Understanding this legacy is vital for designing effective post-conflict institutions that support genuine recovery rather than reinforce divisions. How institutions are used in war, in other words, helps determine the kind of peace that follows.

Acknowledgments We would like to thank Michael Colaresi, Andres Gannon, Erik Gartzke, Ryan Grauer, Harry Oppenheimer, Burcu Savun, Ryan Shandler, Brandon Valeriano, and the participants of the cyber conflict pre-conference workshop held at the 2023 American Political Science Association meeting, the Political Science Research Workshop at the Carnegie Mellon Institute for Strategy and Technology, and the Global Politics Seminar at the University of Pittsburgh.

Funding Statement This research received no specific grant from any funding agency, commercial or not-for-profit sectors.

Competing Interests None.

References

Access Now (2021) *The Return of Digital Authoritarianism: Internet shutdowns in 2021*. Accessed: 2025-03-19. Available at https://www.accessnow.org/wp-content/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

Access Now (2024) *Emboldened Offenders, Endangered Communities: Internet shutdowns in 2024*. Accessed: 2025-03-19. Available at https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf.

Berman E, Shapiro JN and Felter JH (2011) Can hearts and minds be bought? The economics of counterinsurgency in Iraq. *Journal of political Economy* **119**(4), 766–819.

Biddle SD (2004) *Military power: explaining victory and defeat in modern battle*. English. Princeton, NJ: Princeton University Press. ISBN: 0-691-11645-8 978-0-691-11645-7.

Branch J (2021) What's in a Name? Metaphors and Cybersecurity. *International Organization* **75**(1), 39–70.

Brantly AF and Brantly N (2024) The bitskrieg that was and wasn't: the military and intelligence implications of cyber operations during Russia's war on Ukraine. *Intelligence and National Security*, 1–21.

Carnegie A (2021) Secrecy in international relations and foreign policy. *Annual Review of Political Science* **24**, 213–233.

Carr M and Tanczer LM (2018) UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy* **3**(3), 430–444.

Choi SW (2022) Leader nationalism, ethnic identity, and terrorist violence. *British Journal of Political Science* **52**(3), 1151–1167.

Coase RH (1981) The Coase theorem and the empty core: a comment. *The Journal of Law and Economics* **24**(1), 183–187.

Cox GW and McCubbins MD (2005) *Setting the agenda: Responsible party government in the US House of Representatives*. Cambridge University Press.

Crescenzi MJ (2003) Economic exit, interdependence, and conflict. *The journal of Politics* **65**(3), 809–832.

DeNardis L (2014) *The Global War for Internet Governance*. English. New Haven: Yale University Press. ISBN: 978-0-300-18135-7.

Farrell H and Newman AL (2019) Weaponized interdependence: How global economic networks shape state coercion. *International Security* **44**(1), 42–79.

Gannon JA, Gartzke E, Lindsay JR and Schram P (2024) The shadow of deterrence: Why capable actors engage in contests short of war. *Journal of Conflict Resolution* **68**(2-3), 230–268.

Goddard SE (2018) Embedded revisionism: Networks, institutions, and challenges to world order. *International Organization* **72**(4), 763–797.
Goddard SE and Nexon DH (2016) The dynamics of global power politics: A framework for analysis. *Journal of Global Security Studies* **1**(1), 4–18.
Haneuse S, VanderWeele TJ and Arterburn D (2019) Using the E-value to assess the potential effect of unmeasured confounding in observational studies. *Jama* **321**(6), 602–603.
Internet Intelligence Lab (2022) IODA. Available at https://ioda.inetintel.cc.gatech.edu/resources?tab=repositories (accessed 8 September 2022).
Jepperson R (1991) Institutions, institutional effects, and institutionalism. *The new institutionalism in organizational analysis*, 143–163.
Kostyuk N and Brantly A (2022) War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation. *Contemporary Security Policy* **43**(3), 498–515.
Lake DA (2009) *Hierarchy in International Relations*. en. Cornell University Press. ISBN: 0-8014-4756-9.
Lanoszka A (2022) *Military Alliances in the Twenty-First Century*. English. Medford, MA: Polity. ISBN: 978-1-5095-4557-5.
Lindsay JR (2025) *Age of Deception: Cybersecurity as Secret Statecraft*. Cornell University Press.
Lindsay JR (2017) Restrained by design: The political economy of cybersecurity. *Digital Policy, Regulation and Governance* **19**(6), 493–514.
Mcconaughey M, Musgrave P and Nexon DH (2018) Beyond anarchy: logics of political organization, hierarchy, and international structure. en. *International Theory*, 29 May **10**(2), 181–218. ISSN: 1752-9719, 1752-9727. doi: 10.1017/S1752971918000040. https://www.cambridge.org/core/journals/international-theory/article/beyond-anarchy-logics-of-political-organization-hierarchy-and-international-structure/8E1C8F52C572E8A4383C170B81D3AD15 (accessed 29 May 2024).
Morrow JD (2014) *Order within anarchy: The laws of war as an international institution*. Cambridge University Press.
North DC (1990) *Institutions, Institutional Change, and Economic Performance.* New York: Cambridge University Press,
North DC, Wallis JJ and Weingast BR (2009) *Violence and social orders: A conceptual framework for interpreting recorded human history*. Cambridge University Press.
Oneal JR and Russett B (2001) Clear and clean: The fixed effects of the liberal peace. *International Organization* **55**(2), 469–485.
Ostrom E (1990) *Governing the commons: The evolution of institutions for collective action*. Cambridge university press.
Pape RA (1996) *Bombing to win: Air power and coercion in war*. Cornell University Press.
Stam AC (1998) *Win, lose, or draw: Domestic politics and the crucible of war*. University of Michigan Press.
Waltz KN (1979) *Theory of international politics*. McGraw-Hil.
Zhukov YM (2023) Near-real time analysis of war and economic activity during Russia's invasion of Ukraine. *Journal of Comparative Economics*.