ONLINE APPENDIX:
Data, Method, & Robustness Checks

"Strategic Interdependence:
How Combatants Manage Collective Institutions During War"

Nadiya Kostyuk, Jon Lindsay, Eunji Emily Kim, Zachary Bischof,
Aniket Anand, Amanda Meng, & Alberto Dainotti

January 8, 2026

Contents

1 Differentiating Military Strategies: Maneuver versus Attrition Warfare **2**

2 Russia's use of Internet outages in war **5**
2.1 Summary Statistics and Correlation Plots 5
2.2 Results 7
2.3 Robustness Checks 8
2.3.1 An alternative measure of territorial control 9
2.3.2 An alternative model specification 9
2.3.3 An alternative measure of military strategy 9
2.3.4 Sensitivity Analysis: Misclassification of Outage Intentionality 9
2.3.5 No lagged DV 10
2.3.6 E-value sensitivity analysis 11
2.4 Alternative Explanations 12
2.4.1 Internet outages as a secondary, unintended consequence 12
2.4.2 Resilience of Ukraine's Cyber Defenses 13

3 Ukraine's use of Internet outages as a tool of war **15**

4 Evidence Beyond Ukraine **19**
4.1 2020 and 2023 Armenia-Azerbaijan conflicts over the Nagorno-Karabakh region . . 19

1 Differentiating Military Strategies: Maneuver versus Attrition Warfare

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 (CSIS), the Institute for the Study of War (ISW), 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 provides samples of these sources.

Based on these external classifications, we categorize specific phases of the conflict as follows: 'Initial invasion' (February 24, 2022 – April 7, 2022) is classified as 'Offensive Maneuver (R)';[1] the 'Southeastern front' (April 8, 2022 – August 28, 2022), 'Second stalemate' (November 12, 2022 – June 7, 2023), and 'Winter campaigns' (December 1, 2023 – December 31, 2023) are categorizes as 'Attrition'; and 'Ukrainian counteroffensive I' (August 29, 2022 – November 11, 2022) and 'Ukrainian counteroffensive II' (June 8, 2023 – November 30, 2023) are classified as 'Defensive Maneuver (R)'. 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 majority agreement or consensus among expert assessments.

We also considered alternative methods to differentiate between maneuver and attrition warfare, such as using territorial gains, fatalities, or specific military tactics to capture finer, day-to-day battlefield dynamics. However, these proved problematic.

Territorial gains, for instance, only capture 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. To illustrate this, Figure 1 compares the percentage of Russian territorial gains in the Donetsk and Kharkiv regions, using a seven-day moving average. The data is broken down by various war phases identified by experts. In the figure, 'OM (R)' refers to Russian offensive maneuver campaigns, 'DM (R)' to Russian defensive maneuver campaigns, and 'A' to attrition warfare.

Figure 1a shows the percentage of Russian territorial gains in the Donetsk region, while Figure 1b shows the same for the Kharkiv region. These regions were selected due to their high levels of military activity and their prominent position on the frontline. Both figures reveal that the decision regarding the threshold for classifying daily territorial change as maneuver versus attrition warfare is somewhat arbitrary. For instance, in Donetsk, Russian forces were only able to gain around 1.5% of the region's territory during their most successful maneuvering, while in Kharkiv, they captured about 8% during peak maneuver campaigns.

The plots also illustrate fluctuations in territorial gains and losses within the same war phase. In the first war phase, which was primarily characterized by offensive maneuvering, for instance, Russian forces generally gained territory, although there were brief instances of territorial loss followed by recovery. These fluctuations differ across regions, suggesting that even if forces are engaged in offensive maneuvering in some areas, other areas may see defensive maneuvering or attrition. To address these localized exceptions, we conduct a sensitivity analysis (see Section 2.3.3), which confirms that our results remain robust despite these regional variations in military

[1] 'R' in parentheses stands for 'Russian'.

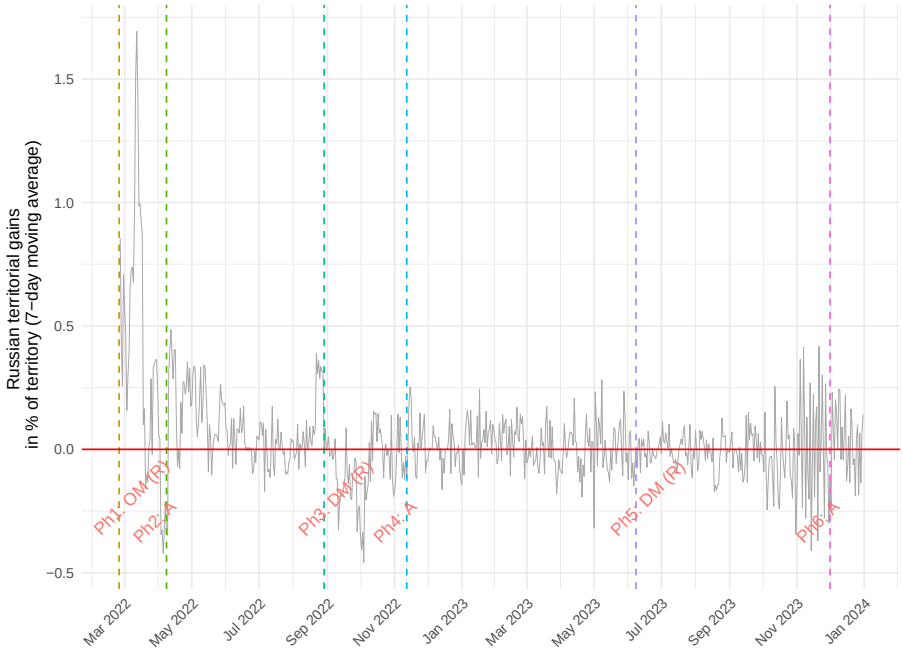
Campaign Type	War Phase Label	Supporting Evidence & Sources
Rus Offensive Maneuver	Initial Invasion (2/24/22–4/7/22)	Russia's ground forces invaded on multiple axes; rapid territorial gains. *Source:* Center for Strategic and International Studies (CSIS). "Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare." June 1 2022. Link; maps and information from the Institute for the Study of War (ISW) reports. "Russian Offensive Campaign Assessment" (from February 24, 2022 to December 31, 2023).
Attrition	Southeastern Front (4/8/22–8/28/22); Second Stalemate (11/12/22–6/7/23); Winter Campaigns (12/1/23-12/31/23)	"The war in Ukraine has become a war of attrition characterised by dug-in forces, trenches… artillery barrages, and high casualties." (p. 2). *Source*: CSIS. "Ukrainian Innovation in a War of Attrition." Feb 27 2023. Link; "Russian forces in Ukraine are now trapped in a cycle of attrition and are facing shortages of equipment and ammunition." (p. 3); *Source*: CSIS. "A War of Attrition: Assessing the Impact of Equipment Shortages on Russian Military Operations in Ukraine." July 31 2023. Link; maps and information from the Institute for the Study of War (ISW) reports. "Russian Offensive Campaign Assessment" (from February 24, 2022 to December 31, 2023).
Rus Defensive Maneuver	Ukrainian Counteroffensive I (8/29/22-11/11/22); Ukrainian Counteroffensive II (6/8/23–11/30/23)	"Ukrainian forces retain the initiative in the war but advanced an average of only 90 meters per day on the southern front during the peak of their summer offensive" (p. 1); "During its 2022 counteroffensive in the Kherson Oblast, Ukraine advanced 590 meters a day on average..." (p. 3). *Source*: CSIS. "Seizing the Initiative in Ukraine: Waging War in a Defense-Dominant World." Oct 12 2023. Link; maps and information from the Institute for the Study of War (ISW) reports. "Russian Offensive Campaign Assessment" (from February 24, 2022 to December 31, 2023).

Table 1: SAMPLE SOURCES FOR PHASE CLASSIFICATIONS OF THE UKRAINE WAR.

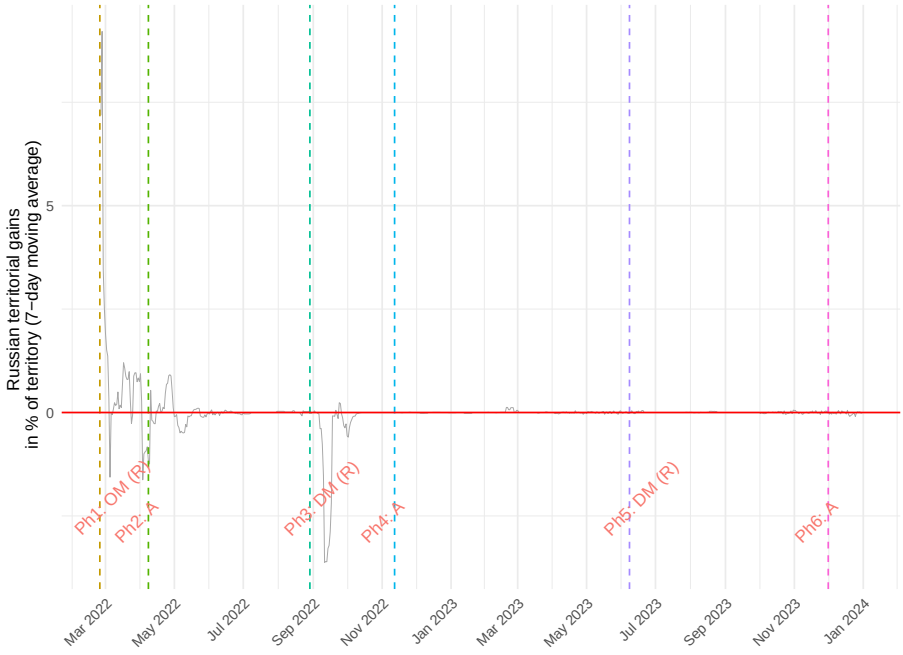
strategy.

Notably, the plots in Figure 1 show that, despite some fluctuations in territorial gains across war phases—making it difficult to use *territorial control* to definitively label war phases—the fluctuations generally align with expert-labeled phases. For instance, during the first war phase, identified by experts as Russia's offensive maneuvering, Russian forces in both Donetsk and Kharkiv predominantly gained territory, capturing 0.395% of Donetsk and 0.829% of Kharkiv. During attrition phases, territorial gains in both regions were close to zero. Conversely, during defensive maneuver campaigns, Russian territorial gains were generally negative, such as -0.0721% in Donetsk and -0.384% in Kharkiv during Phase 3. This evidence suggests that expert-labeled war phases more accurately capture battlefield dynamics and are better suited for analysis than relying on daily changes in territorial control.

Similarly, the number of fatalities is not a reliable indicator, as there is no clear threshold to distinguish between offensive and defensive operations. Fatalities can also occur in both maneu-



(a) Donetsk region.



(b) Kharkiv region

Figure 1: Percentage of Russian territorial gains across the Donetsk and Kharkiv regions, using a seven-day moving average, by war phases identified by experts (2022-2023). 'OM (R)': Russian offensive maneuver campaigns; 'DM (R)': Russian defensive maneuver campaigns; and 'A': attrition warfare.

Table 2: Territorial gains data for Donetsk and Kharkiv regions across various war phases (2022-2023).

Region Name	War Phase Names	Territorial Gains (in %)
Donetsk	Ph1: Russian Offensive Maneuver	0.395
Donetsk	Ph2: Attrition	0.0889
Donetsk	Ph3: Russian Defensive Maneuver	-0.0721
Donetsk	Ph4: Attrition	0.0148
Donetsk	Ph5: Russian Defensive Maneuver	-0.0114
Donetsk	Ph6: Attrition	0.0266
Kharkiv	Ph1: Russian Offensive Maneuver	0.829
Kharkiv	Ph2: Attrition	-0.00939
Kharkiv	Ph3: Russian Defensive Maneuver	-0.384
Kharkiv	Ph4: Attrition	0.00229
Kharkiv	Ph5: Russian Defensive Maneuver	0.00247
Kharkiv	Ph6: Attrition	-0.0130

ver and attrition strategies, and often reflect factors such as each side's capabilities and the size of their forces, rather than the strategies being employed.

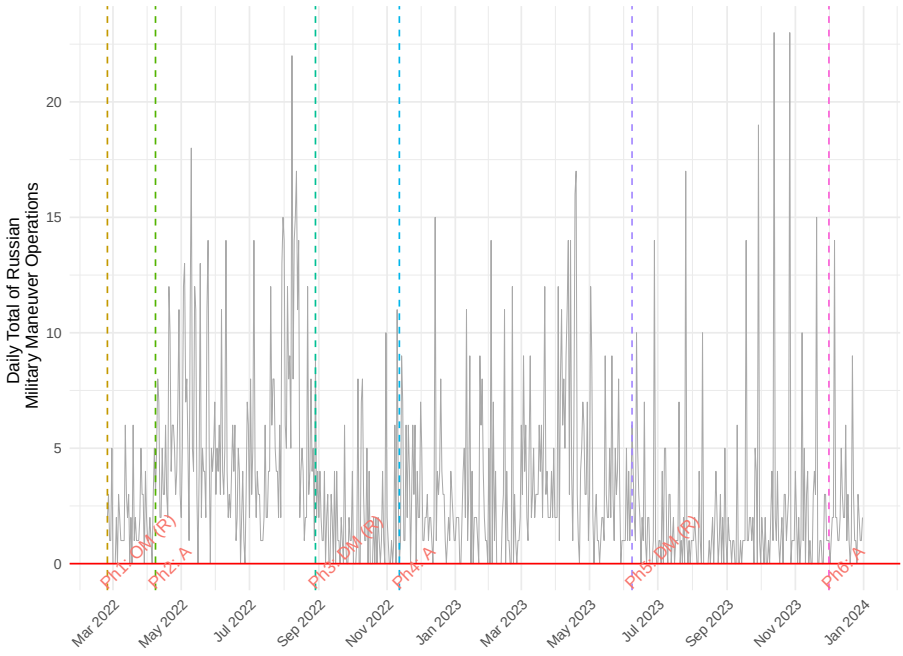
Lastly, tactics such as airstrikes can serve both offensive and defensive purposes (e.g., in counteroffensive operations), further complicating the classification process. To illustrate this, consider the distribution of Russian military operations that are typically seen as potential indicators of maneuvering, such as the occupation of territory or buildings, assaults by paratroopers or special forces, tank battles, and exchanges of gunfire involving handguns, semi-automatic rifles, automatic rifles, machine guns, and rocket-propelled grenades (RPGs).

Figure 2 shows the total number of Russian military maneuver operations across the Donetsk and Kharkiv regions, categorized by the war phases identified by experts (2022-2023). The figure reveals that many operations, which should be interpreted as signs of maneuvering, occur at a larger scale during the attrition phase. This doesn't imply that the war phases are mislabeled by experts; rather, it suggests that battlefield dynamics are complex. Without knowing the true intentions of the warring parties—information that may only be revealed through archives when classified details become available—we should rely on expert-labeled data, rather than attempting to create less precise measures of our own.

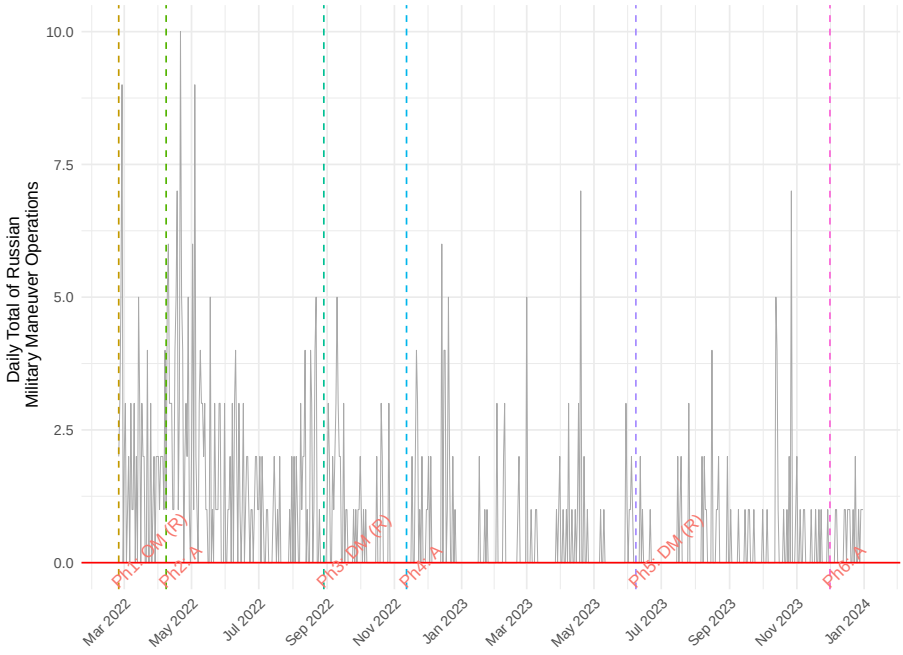
2 Russia's use of Internet outages in war

2.1 Summary Statistics and Correlation Plots

Figure 3 depicts the correlation plot for main variables of interest and controls. Table 3 shows the summary statistics for the main explanatory variables and controls.



(a) Donetsk region.



(b) Kharkiv region

Figure 2: Total number of Russian military maneuver operations, such as the occupation of territory or buildings, assaults by paratroopers or special forces, tank battles, and exchanges of gunfire, across the Donetsk and Kharkiv regions, by war phases identified by experts (2022-2023). 'OM (R)': Russian offensive maneuver campaigns; 'DM (R)': Russian defensive maneuver campaigns; and 'A': attrition warfare.

Table 3: Summary Statistics

Variable	Minimum	Median	Mean	Maximum
Rus Internet Outages	0.00	0.00	0.04	1.00
Rus Offensive Maneuver	0.00	0.00	0.06	1.00
Rus Defensive Maneuver	0.00	0.00	0.37	1.00
Attrition	0.00	1.00	0.57	1.00
Rus Kinetic	0.00	1.00	4.12	115.00
Holidays	0.00	0.00	0.03	1.00
Weekend	0.00	0.00	0.29	1.00

Figure 3: Correlation Plot

2.2 Results

This section presents the complete results for the tables included in the main manuscript. Table 4 analyzes the use of Internet outages by the Russian military and/or government during different

war strategies employed in its war in Ukraine. The results indicate that Internet disruptions occur at a higher rate during offensive maneuver combat compared to attrition or defensive maneuver combat. Internet outages are less likely to be used as a form of punishment on the Ukrainian-controlled territories than they are used along the frontline on contested territories.

Table 4: RUSSIA'S USE OF INTERNET OUTAGES IN ITS WAR IN UKRAINE (LOG ODDS AND STANDARD ERRORS)

	DV: `Internet Outage (R)`			
	Model 1 (w/out controls)	**Model 2** (w/ controls)	**Model 3** (w/out controls)	**Model 4** (w/ controls)
Rus Offensive Maneuver (lag)	0.834***	0.851***	——	——
	(0.297)	(0.298)		
Rus Defensive Maneuver (lag)	−1.465***	−1.471***	——	——
	(0.370)	(0.373)		
Punishment in Ukr Territories (lag)	——	——	−1.833***	−1.925***
			(0.242)	(0.280)
Rus Kinetic (lag)	——	0.396*	——	0.041
		(0.204)		(0.090)
Holidays	——	−0.339	——	−1.005*
		(0.644)		(0.519)
Weekend	——	−0.777***	——	−1.644***
		(0.242)		(0.171)
Rus Internet Outage (lag)	3.738***	3.798***	4.678***	4.940***
	(0.216)	(0.225)	(0.124)	(0.138)
(Intercept)	−3.095***	−3.920***	−2.936***	−2.624***
	(0.432)	(0.679)	(0.232)	(0.311)
Observations	2,141	2,141	15,974	15,974
Log Likelihood	−371.642	−363.869	−1,308.381	−1,247.691
Akaike Inf. Crit.	753.284	743.739	2,624.762	2,509.381

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. 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. All models contain oblast random effects. *p<0.1; **p<0.05; ***p<0.01.

2.3 Robustness Checks

We conduct the following robustness checks:

1. an alternative measure of territorial control (Section 2.3.1);
2. an alternative model specification (Section 2.3.2);
3. an alternative measure of military strategies (Section 2.3.3);
4. sensitivity analysis of outage intentionality (Section **??**);
5. no lagged dv (Section 2.3.5); and

6. an E-value sensitivity analysis assessing the robustness of the observed associations to potential unmeasured confounding, addressing endogeneity concerns inherent in observational data (Section 2.3.6).

2.3.1 An alternative measure of territorial control

As an alternative measure of territorial control, we classify a region as being under an enemy's control if this enemy holds more than seventy percent of this region's territory. Models 4 and 5 in Table 5, which present that obtained results, show that our results are robust to this alternative measure of territorial control.

2.3.2 An alternative model specification

Instead of a logistic regression model, we also fit a probit regression model. Models 6 and 7 in Table 5, which presents that obtained results, shows that our results are robust to this alternative model specification. Moreover, instead of region-random effects, we use region-fixed effects. Our results are robust to this alternative model specification.

2.3.3 An alternative measure of military strategy

We also conduct a sensitivity analysis to explore an alternative measure of military strategy. As discussed in Section 1, expert-labeled military strategies generally align with changes in territorial control—where gains often reflect successful offensive maneuvering, losses indicate successful defensive maneuvering, and no territorial change indicates attrition. However, fluctuations in territorial control can occur within a single expert-labeled war phase across different regions. These fluctuations suggest that, while forces may be engaged in offensive maneuvering in some areas, other areas might experience brief periods of defensive maneuvering or attrition even within the offensive maneuvering war phase.

To address these localized exceptions, we conduct a sensitivity analysis. Specifically, we classify Russian forces as engaging in offensive maneuvering when their 7-day moving average shows gains of at least 0.2% of a region's territory, and as engaging in defensive maneuvering when their 7-day moving average indicates losses of at least 0.1%. In all other cases, we retain the expert-labeled military strategies. The results from Models 8 and 9 in Table 6 demonstrate that our findings remain robust, even when accounting for regional variations in military strategy.

2.3.4 Sensitivity Analysis: Misclassification of Outage Intentionality

One potential concern is that some outages coded as unintentional may, in fact, be deliberate. Given the difficulty of conclusively identifying intent—particularly during wartime—we conduct a sensitivity analysis to assess how robust our results are to potential misclassification. Specifically, we randomly reclassify between 0% and 50% of outages initially coded as *unintentional* to *intentional* and re-estimate our main models a 100 times. Figures 4 and 5, which display our results from running these simulations, show that more than 50% of these outages would need to be incorrectly classified in order to overturn our main findings. This high threshold suggests that our results are robust to a reasonable degree of coding uncertainty.

Table 5: ROBUSTNESS CHECKS AND ALTERNATIVE EXPLANATIONS (LOG ODDS AND STANDARD ERRORS)

	DV: Rus Internet Outage			
	Model 4 (alt. territorial measure)	**Model 5** (alt. territorial measure)	**Model 6** (alt. model specif.)	**Model 7** (alt. model specif.)
Rus Offensive Maneuver (lag)	0.959***	——	0.464***	——
	(0.171)		(0.074)	
Rus Defensive Maneuver (lag)	−1.572***	——	−0.649***	——
	(0.213)		(0.084)	
Punishment in Ukr Territories (70%) (lag)	——	−1.885***	——	——
		(0.276)		
Punishment in Ukr Territories (80%) (lag)	——	——	——	−0.929***
				(0.128)
Rus Kinetic (log, lag)	0.319***	0.151*	0.154***	0.037
	(0.083)	(0.088)	(0.035)	(0.041)
Holidays	−0.862*	−0.935*	−0.458**	−0.528**
	(0.522)	(0.542)	(0.226)	(0.242)
Weekend	−1.794***	−1.808***	−0.743***	−0.755***
	(0.184)	(0.188)	(0.081)	(0.082)
Rus Internet Outage (lag)	4.816***	5.029***	2.514***	2.575***
	(0.148)	(0.148)	(0.070)	(0.071)
(Intercept)	−4.316***	−2.638***	−2.237***	−1.431***
	(0.154)	(0.314)	(0.066)	(0.142)
Observations	14,882	14,882	15,974	15,974
Log Likelihood	−1,069.577	−1,103.932	−1,207.506	−1,244.850
Akaike Inf. Crit.	2,155.153	2,221.865	2,431.011	2,503.700

Note: This table examines the use of Internet outages by the Russian military and/or government during different war strategies in Ukraine. Internet disruptions occur at a higher rate during offensive maneuver combat than during attrition combat or defensive maneuver combat on contested territories. All models contain region-fixed effects. *p<0.1; **p<0.05; ***p<0.01

2.3.5 No lagged DV

To account for the persistence of Internet outages, we include a lagged dependent variable in our main specification. Outages caused by military activity often last multiple days, and failing to lag the dependent variable would treat each day of an ongoing outage as a new, independent event. Including a lag helps capture the temporal dependence of outages and ensures that we focus on modeling the onset of new disruptions rather than their continuation. As a robustness check, we also estimate models without the lagged dependent variable, thereby allowing all days of an ongoing outage to be treated as potentially strategic. This alternative specification accounts for the possibility that sustained outages themselves reflect deliberate choices rather than purely residual effects. As Models 12 and 13 in Table 7 shows, our main results remain consistent across both approaches.

Table 6: ROBUSTNESS CHECKS AND ALTERNATIVE EXPLANATIONS (CONTINUED) (LOG ODDS AND STANDARD ERRORS)

	DV: Rus Internet Outage			
	Model 8 (alt. military measure)	**Model 9** (alt. military measure)	**Model 10** (alt. explanation)	**Model 11** (alt. explanation)
Rus Offensive Maneuver (lag)	0.729***	——	0.817***	——
	(0.279)		(0.302)	
Rus Defensive Maneuver (lag)	−0.526**	——	−1.455***	——
	(0.268)		(0.371)	
Punishment in Ukr Territories (lag)	——	−1.925***	——	−2.025***
		(0.280)		(0.253)
Rus Kinetic (log, lag)	0.314	0.041	——	——
	(0.200)	(0.090)		
Rus Airstrikes (log, lag)	——	——	0.151	−0.098
			(0.164)	(0.131)
Holidays	−0.408	−1.005*	−0.319	−1.017*
	(0.660)	(0.519)	(0.641)	(0.521)
Weekend	−0.836***	−1.644***	−0.794***	−1.648***
	(0.244)	(0.171)	(0.243)	(0.171)
Rus Internet Outage (lag)	4.012***	4.940***	3.834***	4.950***
	(0.223)	(0.138)	(0.225)	(0.137)
(Intercept)	−3.622***	−2.624***	−3.008***	−2.479***
	(0.662)	(0.311)	(0.454)	(0.251)
Observations	2,141	15,974	2,141	15,974
Log Likelihood	−371.748	−1,247.691	−365.394	−1,247.514
Akaike Inf. Crit.	759.496	2,509.381	746.787	2,509.027

Note: This table examines the use of Internet outages by the Russian military and/or government during different war strategies in Ukraine. Internet disruptions occur at a higher rate during offensive maneuver combat than during attrition combat or defensive maneuver combat on contested territories. All models contain region-fixed effects. *p<0.1; **p<0.05; ***p<0.01

2.3.6 E-value sensitivity analysis

As this study relies on observational data, there are inherent concerns about endogeneity. In particular, the decision to disrupt shared institutions like the Internet may be influenced by unobserved factors that also correlate with battlefield dynamics or territorial characteristics. To address this, we included region fixed effects and controlled for temporal variation in conflict intensity. In addition, we conducted an E-value sensitivity analysis to assess how robust the observed associations are to potential unmeasured confounding (VanderWeele and Ding, 2017; Haneuse, VanderWeele and Arterburn, 2019). The E-value represents the minimum strength of association that an unmeasured confounder would need to have with both the treatment and the outcome to explain away the observed effect.

In our case, the E-value for the association between Russia-sponsored internet outages and its offensive maneuver campaigns is 4.12 for the point estimate (RR = 2.34), and 1.93 for the lower bound of the 95% confidence interval (RR = 1.30), suggesting that our results are robust to unmeasured confounding. The E-value for the association between Russia-sponsored internet outages and its defensive maneuver campaigns is 8.17 for the point estimate (RR = 0.23), and 3.76 for the

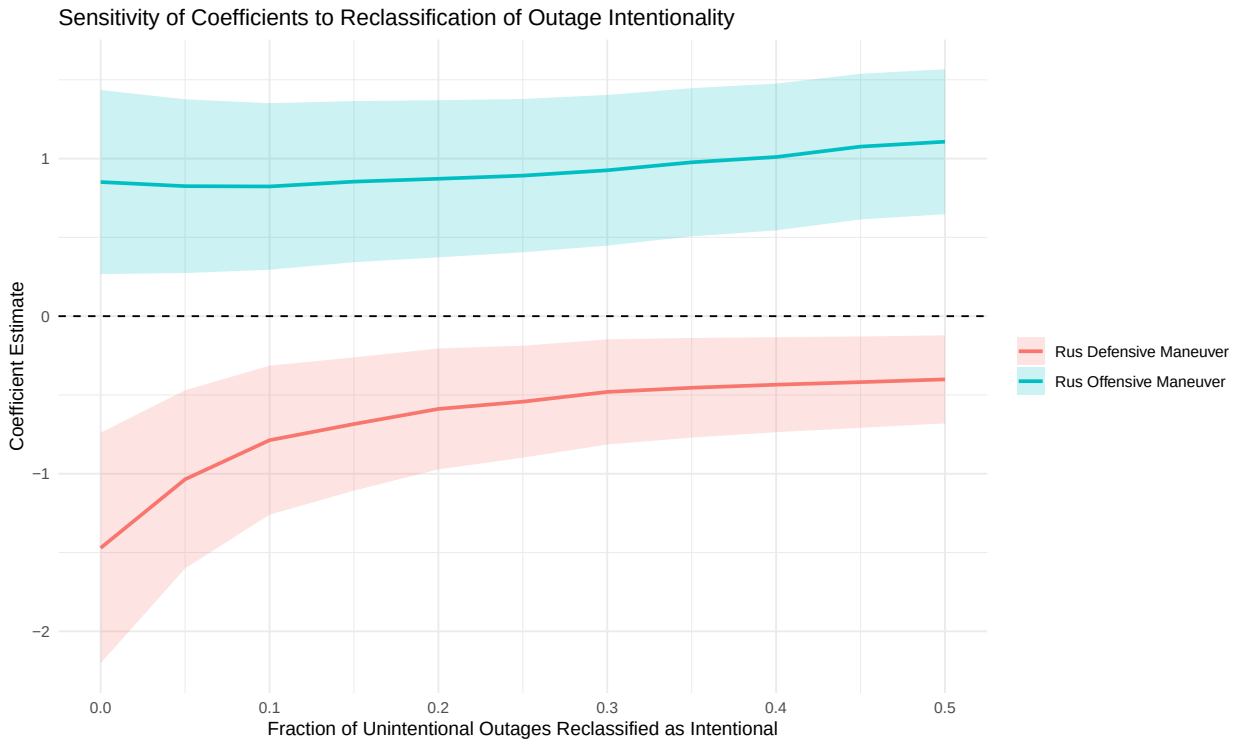


Figure 4: SENSITIVITY ANALYSIS: MISCLASSIFICATION OF OUTAGE INTENTIONALITY (MANEUVER VERSUS ATTRITION)

upper bound of the 95% confidence interval (RR = 0.47), suggesting that our results are robust to unmeasured confounding. Lastly, the E-value for the association between Russia-sponsored internet outages and the territory being under Ukrainian control is 13.19 for the point estimate (RR = 0.15), and 7.47 for the upper bound of the 95% confidence interval (RR = 0.25), suggesting that our results are robust to unmeasured confounding. While we remain cautious in making strong causal claims, these results provide further confidence in the observed patterns, which are consistent with our theory.

2.4 Alternative Explanations

2.4.1 Internet outages as a secondary, unintended consequence

As one of the alternative explanations that we consider is that Russia's primary goal is to deprive the Ukrainian people of public goods and disrupt critical infrastructure, with Internet outages being a secondary, unintended consequence. If this were true, we would expect to see a positive relationship between Russia's military operations and Internet outages, as these operations would aim to cause such disruptions. To investigate, we specifically control for Russian airstrikes, which were frequently used to target critical infrastructure. Our results, presented in Models 10 and 11 in Table 6, reaffirm the earlier findings, indicating that Russian Internet outages were not merely a secondary effect of its attacks on critical infrastructure. Instead, they appear to be a strategic choice made by the Kremlin.

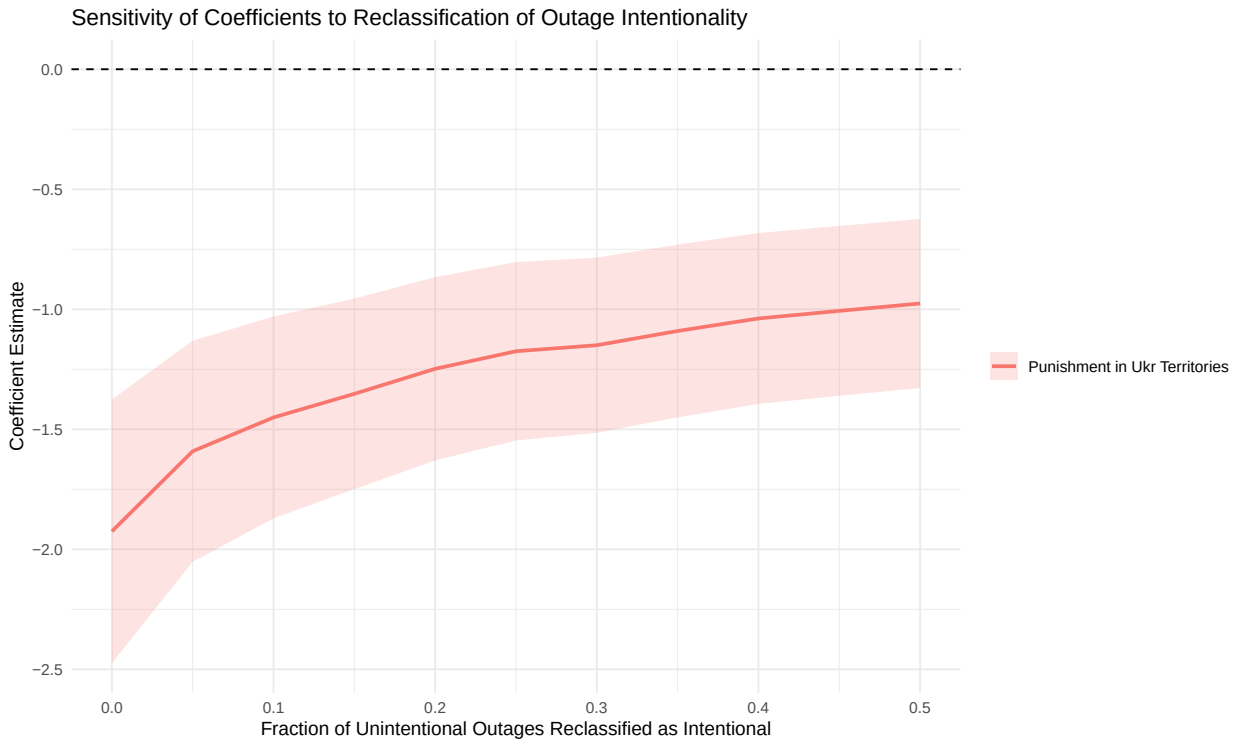


Figure 5: SENSITIVITY ANALYSIS: MISCLASSIFICATION OF OUTAGE INTENTIONALITY (PUNISHMENT ON UKR TERRITORIES)

2.4.2 Resilience of Ukraine's Cyber Defenses

Another possible explanation concerns Ukraine's internet resilience, which can be attributed to substantial Western support throughout the war. This resilience may impact the number of outages caused by Russia's cyber operations, as the data only captures 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, this is not the case. Descriptive data, shown in Figure 6, reveals a higher number of Internet outages in winter 2023–almost two years into the conflict—compared to earlier phases of the war. Furthermore, observing fewer Russia-sponsored Internet outages resulting from cyber operations introduces a possible attenuation bias. Consequently, the data that we have represents the lower bound of the true number of Internet outages, then the true coefficients should be higher, implying that the actual coefficients should be higher. As a result, our findings may underestimate the true effect size of Internet outages, making them more conservative. This suggests that the actual relationship between combat dynamics and Internet outages could be even stronger than previously reported, further reinforcing our theory.

Table 7: ROBUSTNESS CHECKS AND ALTERNATIVE EXPLANATIONS (CONTINUED) (LOG ODDS AND STANDARD ERRORS)

	DV: Rus Internet Outage	
	Model 12 (no lagged DV)	**Model 13** (no lagged DV)
Rus Offensive Maneuver (lag)	1.571***	——
	(0.245)	
Rus Defensive Maneuver (lag)	−1.966***	——
	(0.312)	
Punishment in Ukr Territories (lag)	——	−3.662***
		(0.198)
Rus Kinetic (log, lag)	0.501***	0.339***
	(0.169)	(0.078)
Holidays	−0.640	−1.234***
	(0.537)	(0.388)
Weekend	−0.514***	−0.919***
	(0.196)	(0.126)
(Intercept)	−3.740***	−0.846***
	(0.828)	(0.325)
Observations	2,141	15,974
Log Likelihood	−528.564	−1,979.323
Akaike Inf. Crit.	1,071.129	3,970.645

Note: This table examines the use of Internet outages by the Russian military and/or government during different war strategies in Ukraine. Internet disruptions occur at a higher rate during offensive maneuver combat than during attrition combat or defensive maneuver combat on contested territories. All models contain region-fixed effects. *p<0.1; **p<0.05; ***p<0.01

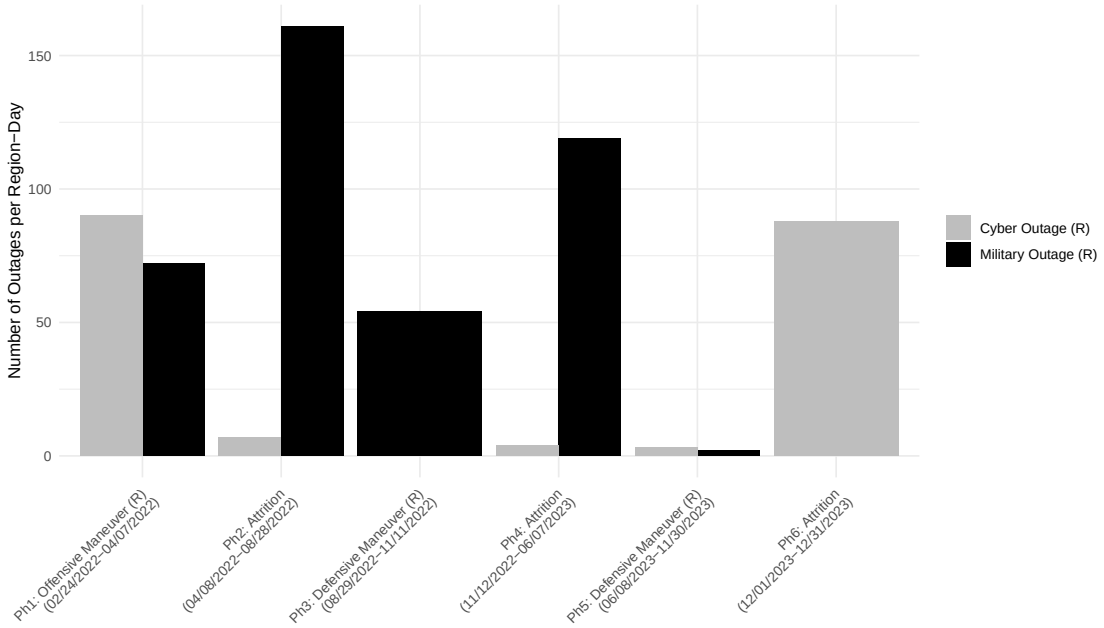


Figure 6: Distribution of Russia-sponsored Outages per Region-Day across Different War Phases in the Ukraine War (2022-2023)

3 Ukraine's use of Internet outages as a tool of war

This section focuses on Ukraine's use of Internet outages as a tool of war during the 2022-2023 Russia's invasion of Ukraine. We first describe the construction of our dependent and independent variables, then present our findings.

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

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 employs 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 3-week segment and 14 4-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 insure 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 Kyiv. 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[2] to record and contextualize Internet shutdowns.

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 enemy-controlled territories.

[2]These sources include Google Transparency Data, Facebook Transparency Report, CloudFlare Radar, Oracle, among others. For more information on sources and methods, visit KeepItOn.

To determine which territories are contested and which are under enemy 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. Using this classification, we consider that Ukraine engages in maneuver or attrition warfare in contested regions along the frontline and practices 'punishment' in Russian-occupied territories, where it lacks territorial control and faces greater operational constraints.

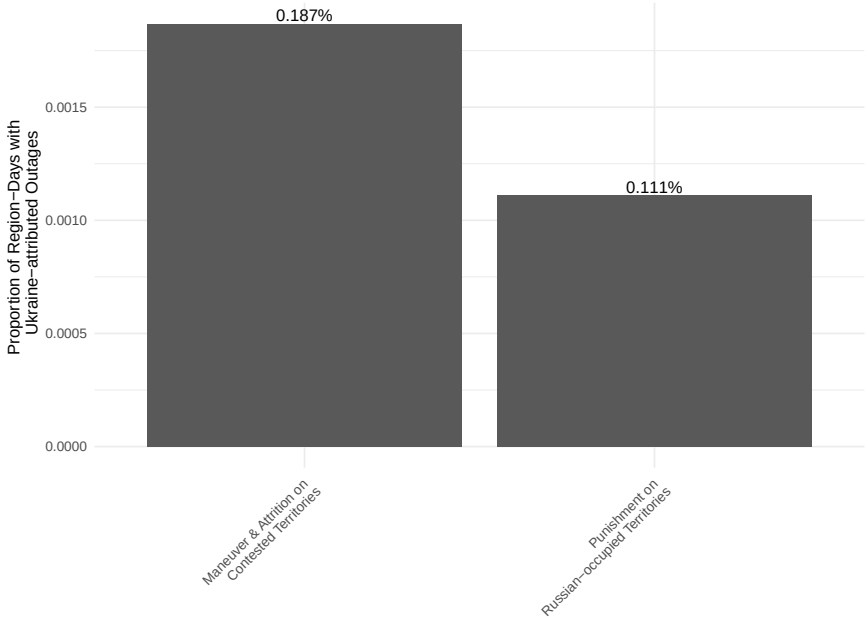
Having differentiated between maneuver/attrition and punishment warfare based on location, we now turn to distinguishing between maneuver and attrition warfare, both of which occur in contested territories. To identify offensive and defensive maneuver warfare and attrition warfare, we rely on expert opinion that categorize specific phases of the conflict as follows: 'Initial invasion' (February 24, 2022 – April 7, 2022) is classified as 'Ukr Defensive Maneuver'; the 'Southeastern front' (April 8, 2022 – August 28, 2022), 'Second stalemate' (November 12, 2022 – June 7, 2023), and 'Winter campaigns' (December 1, 2023 – December 31, 2023) are categorizes as 'Attrition'; and 'Ukrainian counteroffensive I' (August 29, 2022 – November 11, 2022) and 'Ukrainian counteroffensive II' (June 8, 2023 – November 30, 2023) are classified as 'Ukr Offensive Maneuver.' As explained in Section 1, we also also considered alternative methods to distinguish between maneuver and attrition warfare, such as using territorial gains, fatalities, or specific military tactics to capture finer, day-to-day battlefield dynamics. We explained the limitations of each of these measures in that section.

Research Design. Since we are interested in analyzing Ukraine's actions in Russia-contested and Russia-controlled territories, we excluded Ukrainian-controlled areas from our analysis, which included regions where at least 80% of the territory was under Kyiv's control on a given day. These regions included Zakarpattia, Volyn, Vinnytsia, Ternopil, Rivne, Poltava, Odesa, Lviv, Kirovohrad, Ivano-Frankivsk, Dnipro, Chernivtsi, Cherkasy, Zhytomyr, Mykolaiv, Kyiv, Kyiv City, Sumy, Chernihiv, and Kharkiv.

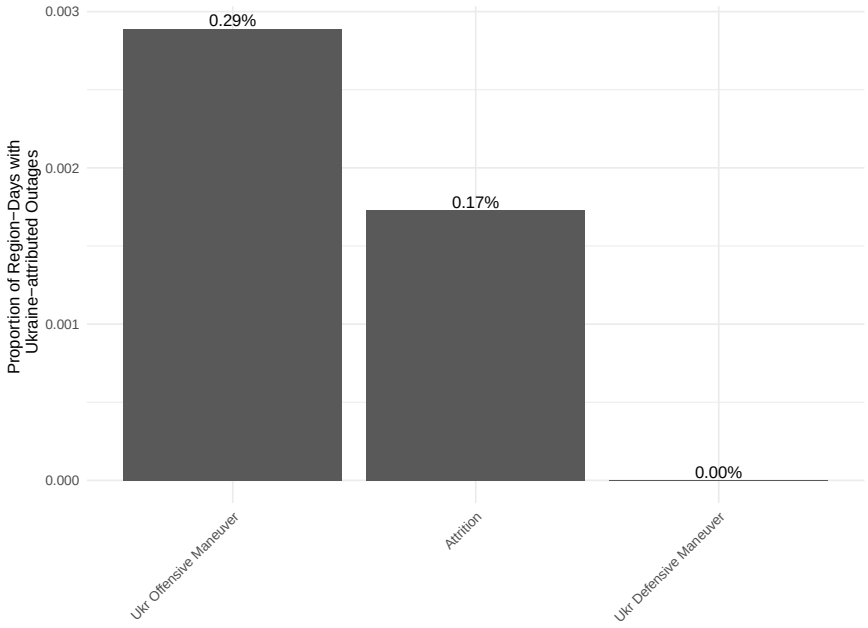
Although Ukraine also used Internet outages to disrupt enemy communications, there were too few instances to perform a quantitative analysis (see Figure 7 below). This is not surprising, as Ukrainian forces targeting Russia-contested or Russia-occupied areas in southern Ukraine aim to eventually reclaim these regions. If widespread outages were implemented, affecting the population, they would only reinforce Moscow's claim that the Ukrainian government represses Russian-speaking citizens in those areas. In contrast, when Moscow targets Ukrainian-controlled Western territories—territories it does not intend to retain—Internet outages are used more frequently and as a common tool. Due to the scarcity of Ukraine-attributed outages, which makes them unsuitable for quantitative analysis, we present descriptive evidence and anecdotal information to demonstrate that Ukrainian actions align with our theoretical expectations.

Findings. We begin with descriptive evidence. Figure 7 illustrates how Ukraine's use of Internet outages varied across different regions and over time during the war. This figure shows the total number of region-days with Ukrainian-sponsored Internet outages in both contested and Russian-occupied territories.

Since we differentiate between strategies based on their temporal dynamics—the punishment strategy, which occurs in enemy-controlled territories, and maneuver/attrition warfare in contested regions—we examine these distinctions by comparing the distribution of Ukraine-attributed



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



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

Figure 7: Proportion of region-days with Ukraine-attributed Internet outages based on different military strategies in its war against Russia (2022-2023). *Data sources:* Internet Outage Detection Analysis Data (IODA) (Internet Intelligence Lab, 2022); Access Now's #KeepItOn Shutdown Tracker Optimization Project (STOP); Violent Incident Information from News Articles (VIINA) data (Zhukov, 2023).

Internet outages across these two types of territories. Figure 7a displays the results, showing that there were significantly more region-day observations with Ukraine-sponsored Internet outages in contested territories—where maneuver and attrition warfare occurred—than in Russian-occupied territories, where Ukraine employed a punishment strategy.

Next, Figure 7b zooms in on the contested territories, focusing solely on the regions where Ukraine practiced maneuver and attrition warfare. The figure reveals that the number of region-days with Internet outages was significantly higher during maneuver offensive operations compared to attrition operations, despite the latter generally lasting much longer. Moreover, there were more region-day observations with Internet outages during both maneuver offensive and attrition operations than during maneuver defensive operations. Together, this descriptive evidence offers preliminary support for our hypotheses.

To provide further context, let us explore some instances of these outages. In 2022, the first year of Russia's invasion of Ukraine, the Ukrainian government focused on responding to Russia's Internet shutdowns (Access Now, 2022). Specifically, Ukraine established 4,000 "invincibility centers" where people could stay warm, eat, charge their devices, and access the internet (The Kyiv Independent, 2022). The government also mandated that internet service providers maintain sufficient batteries, generators, and solar panels to remain operational for at least three days during blackouts (The Kyiv Independent, 2022). Throughout this period, Ukrainian actors carried out various cyber operations against Russian entities within Russia (for examples, see for Cyber Security (2022)). However, these actions did not directly lead to outages, and thus fall outside the scope of this discussion.

In 2023, the second year of the war, Ukrainian-sponsored Internet outages became more prominent. During the ongoing attrition warfare, Ukrainian hackers successfully disabled the website of Russian internet service provider Miranda Media in May 2023. Miranda Media provides Internet connectivity to the Russia-occupied and Russia-contested territories (Lipscombe, 2022). The attack lasted for two days, May 25 and 26, disrupting Internet connectivity in the Russian-occupied Luhansk and contested Donetsk regions.

We observe a more frequent use of Internet outages during the Ukrainian offensive maneuver operations later that year. Specifically, at the end of June of 2023, a group of Ukrainian hackers launched cyberattacks on Dozor-Teleport, a Russian satellite communications provider used by energy companies as well as the country's defense and security services (Antoniuk, 2023*a*). Initially, the group behind the hack claimed to be affiliated with the notorious Wagner Group, the Russian private mercenary army that made global headlines the previous week for marching toward Moscow in a rebellion against the Russian government before returning to their positions. However, experts have since clarified that it was not the Wagner Group behind the attack. Instead, Ukrainian hackers conducted a false flag operation, deliberately leveraging the existing tensions between the Wagner Group and the Kremlin to shift the blame onto the mercenary group. The cyberattack, which occurred from June 25 to 29, 2023, targeted military and defense security forces, whose lack of Internet connectivity directly impacted the effectiveness of Russian military operations on the frontlines of the Ukraine war (Antoniuk, 2023*a*).

Further, in October 2023, the Ukraine IT Army—a collective of Ukrainian hackers—temporarily disabled the services of three Russian internet providers—Miranda Media, Krimtelekom, and MirTelekom—in Russian-contested territories including Donetsk, Kharkiv, Kherson, and Zaporizhzhya, with potential attacks also affecting the Russian-controlled region of Luhansk (Access Now, 2023). As one hacker stated, "This is yet another blow by our cyber army, disrupting enemy

military communications on the frontlines" (Antoniuk, 2023*b*). The affected internet providers confirmed that they were hit with an "unprecedented level of DDoS attacks" from Ukrainian hacker groups, temporarily disrupting cellular networks, phone calls, and internet connections. It took several days for the providers to fully restore their services (Antoniuk, 2023*b*).

4 Evidence Beyond Ukraine

Evidence on Internet shutdowns in Azerbaijan, Armenia, India, Israel, Lebanon, Pakistan, and Yemen reveal that Internet connectivity became a target of both military and cyber campaigns during active conflicts (Access Now, 2021, 2022, 2023, 2024), suggesting that the lessons from the Ukraine war could have broader applicability. To further demonstrate that, here we briefly discuss the 2020 and 2023 Armenia-Azerbaijan conflicts over the Nagorno-Karabakh region.

4.1 2020 and 2023 Armenia-Azerbaijan conflicts over the Nagorno-Karabakh region

Background. The conflict between Armenia and Azerbaijan over Nagorno-Karabakh has deep roots, shaped by ethnic, territorial, and political disputes, particularly following the collapse of the Soviet Union (International Crisis Group, 2020). The region, predominantly populated by ethnic Armenians, became a flashpoint in the late 1980s and early 1990s, leading to a full-scale war from 1988 to 1994. Although a ceasefire left Nagorno-Karabakh under Armenian control, tensions simmered for decades with periodic violence. In 2020, Azerbaijan regained significant territory in a six-week war, with Russian mediation leading to a ceasefire (International Crisis Group, 2020). However, in September 2023, Azerbaijan launched a large-scale military operation, quickly retaking Nagorno-Karabakh and displacing over 100,000 ethnic Armenians. This led to a new ceasefire agreement, with Azerbaijan asserting control over the region and offering autonomy to its Armenian population under Azerbaijani sovereignty.

Internet outages as a military tactics during this conflict. What role did Internet outages play during these two periods of intensified conflict?

Let us start with the 2020 six-week war, which lasted from September 27, 2020 to November 10, 2020. The conflict began with an Azerbaijani ground offensive, forcing Armenian and Artsakh[3] troops from their first line of defense in Artsakh's southeast and northern regions. From the first day of their offensive maneuvering, Azerbaijani troops targeted infrastructure throughout Artsakh, the contested region that was under the Armenian control since the 1990s. For instance, they disrupted Internet connectivity in Stepanakert, the capital of the contested Artsakh region (United Nations, 2021).

During the first three days of the conflict, between September 27th and 29th, 2020, Azerbaijani troops managed to make limited gains in the south of the region, suggesting successful offensive maneuvering by these troops. During this period, between September 27 and 30 September 2020, Armenia and Artsakh forces managed to counterattack, retaking some ground in the north; however, they suffered heavy losses when their armor and artillery units were exposed to Azerbaijani attack drones (Kofman and Nersisyan, 2020). For the following three days, between September 30th to October 2nd, 2020, both sides largely exchanged fire from fixed positions, suggesting that

[3]This is an Armenian name for the Nagorno-Karabakh region.

attempts at maneuvering were failing. During this period, Azerbaijan continued shelling the capital of Nagorno-Karabakh, resulting in disruption of Internet connectivity (United Nations, 2021). Azerbaijani forces also targeted Armenian ground lines of communication to prevent the deployment of reserves and stall counteroffensives (Kofman and Nersisyan, 2020).

On October 3rd, 2020, Azerbiajani forces continued shelling of Stepanakert, the capital of Nagorno-Karabakh, resulted in internet outages (United Nations, 2021), while Armenian forces launched strikes against targets in Azerbaijan (Kofman and Nersisyan, 2020). As major advances stalled in the north, Azerbaijan initiated a large-scale offensive in the south, targeting Jabrayil and Füzuli. They successfully broke through the multi-layered Armenian-Artsakh defensive lines, recapturing a stretch of territory previously held by Armenian troops as a buffer zone (Kofman and Nersisyan, 2020). During these operations, Azerbaijani forces also targeted critical internet infrastructure and military communications in the southern regions (United Nations, 2021). Despite these successes of maneuver operations in the south, the fighting eventually stalled. As military analysts Michael Kofman and Leonid Nersisyan noted, by the second week of the conflict, "Ground assaults have proven costly, and rather than a blitzkrieg, it has become a war of attrition" (Kofman and Nersisyan, 2020). As military operations turned into mostly attrition fighting, the number of new reported Internet outages has decreased, providing support for our *H1A-H1C*.

On October 10th, Armenia and Azerbaijan agreed to a temporary humanitarian ceasefire to retrieve the bodies of the dead, but fighting continued both within and outside the conflict zone. The second ceasefire attempt, on October 17th, and the third, on October 26th, both failed (BBC News, 2020). After Azerbaijani forces captured Shusha, the second-largest city in the region before the war, on November 9th, 2020, the final ceasefire agreement was signed by the President of Azerbaijan, the Prime Minister of Armenia, and the President of Russia, Vladimir Putin. The agreement brought an end to all hostilities in the Nagorno-Karabakh conflict zone, effective starting November 10th, 2020 (Novosti, 2020).

Let us now examine any spatial variation in Internet outages that took place during this conflict. Throughout the conflict, both sides targeted Stepanakert, the capital of the contested Artsakh region (United Nations, 2021). For instance, on October 3rd and 4th, 2020, forces attacked the Main Electrical Control Building and Substation, causing widespread power outages across the city. By late November of that year, power and Internet connectivity was still reportedly limited (United Nations, 2021, 3). Additionally, on October 4, 2020, forces struck the head office of Karabakh Telecom, which may have been used for military communications since October 2, 2020 (United Nations, 2021, 3). These attacks not only disrupted military communications in contested areas but also made it difficult for residents to access Internet. In addition to Stepanakert, both forces targeted several nearby cities within the contested region, including Askeran, Martakert, Martuni, Hadrut, Shusha, Lachin, and Kalbajar (United Nations, 2021).

Although most efforts to disrupt Internet connectivity were focused on the disputed territories of Nagorno-Karabakh, hackers worked hard to disrupt Internet connectivity of numerous Armenian news websites that reached both contested regions as well as Armenia, enemy-controlled territories. From the first day of the conflict until mid-November, hackers on both sides launched multiple distributed denial-of-service attacks on each other's news and government websites, rendering them inaccessible to the population (Spînu, 2020; Papyan, 2021). While these disruptions to Internet connectivity were noticeable, they were intermittent, in contrast to the more sustained outages caused primarily by military operations in contested territories. This evidence supports our hypothesis *H2*, which suggests that both sides prioritize Internet disruptions in contested ar-

eas than in enemy-controlled regions.

Lastly, let us briefly examine the use of Internet outages during the 2023 conflict, which lasted only two days. On September 19, 2023, Azerbaijan launched its so-called "local anti-terrorist" operation, attacking Armenian forces in Nagorno-Karabakh and retaking control of the territory. During both days of offensive maneuvering in the contested region of Nagorno-Karabakh, Azerbaijani forces disrupted Internet connectivity. Specifically, as Azerbaijan began its offensive, authorities throttled internet access in Karabakh's Fuzuli, Aghdam, and Terter districts to restrict the flow of information (Watch, 2023). Moreover, on September 20, Azerbaijani authorities also cut off mobile and internet access in Stepanakert City amid heavy bombardment (Lister et al., 2023). As a result of this "local anti-terror operation," the Stepanakert government surrendered, accepting the truce agreement outlined by Azerbaijan and Russia on September 20, 2023. Evidence from this brief conflict provides additional support for our hypotheses, suggesting that combatants will prioritize the use of Internet outages during offensive maneuvering over other conflict phases, and in contested territories rather than enemy-controlled territories.

Overall, evidence from both conflicts further supports our theory, indicating that the lessons learned from the Ukraine war have broader applicability.

References

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

Access Now. 2022. "Weapons of Control, Shields of Impunity.". Accessed: 2025-03-19.
URL: *https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf*

Access Now. 2023. "Shrinking Democracy, Growing Violence.". Accessed: 2025-03-19.
URL: *https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf*

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

Antoniuk, Daryna. 2023*a*. "Hackers claim to take down Russian satellite communications provider." *The Record* . Accessed: 2025-03-30.
URL: *https://therecord.media/hackers-take-down-russian-satellite-provider*

Antoniuk, Daryna. 2023*b*. "Ukrainian hackers disrupt internet providers in Russia-occupied territories." *The Record* . Accessed: 2025-03-30.
URL: *https://therecord.media/ukranian-hackers-disrupt-internet-providers-crimea*

BBC News. 2020. "Nagorno-Karabakh Conflict: US-brokered Ceasefire Frays Soon After Starting." *BBC News* . Accessed: 2023-03-25.
URL: *https://www.bbc.com/news/world-54783202*

for Cyber Security, Canadian Centre. 2022. "Cyber Threat Activity Related to the Russian Invasion of Ukraine.". Accessed: 2023-03-30.
URL: *https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf*

Haneuse, Sebastien, Tyler J VanderWeele and David Arterburn. 2019. "Using the E-value to assess the potential effect of unmeasured confounding in observational studies." *Jama* 321(6):602–603.

International Crisis Group. 2020. "Nagorno-Karabakh Conflict: Visual Explainer.". Accessed: 2025-03-24.
URL: *https://www.crisisgroup.org/content/nagorno-karabakh-conflict-visual-explainer*

Internet Intelligence Lab. 2022. "IODA.".
URL: *https://ioda.inetintel.cc.gatech.edu/resources?tab=repositories*

Kofman, Michael and Leonid Nersisyan. 2020. "The Second Nagorno-Karabakh War: Two Weeks In." *Waron the Rocks* . Accessed: 2025-04-07.
URL: *https://warontherocks.com/2020/10/the-second-nagorno-karabakh-war-two-weeks-in/*

Lipscombe, Paul. 2022. "Russian-backed Telco Miranda Media Operating in Parts of Occupied Ukraine.". Accessed: 2025-03-30.
URL: *https://www.datacenterdynamics.com/en/news/russian-backed-telco-miranda-media-operating-in-parts-of-occupied-ukraine/*

Lister, Time, Gianluca Mezzofiore, Christian Edwards, Anna Chernova and Nick Paton Walsh. 2023. "Azerbaijan's Bombardment of Nagorno-Karabakh: What You Need to Know." *CNN* . Accessed: 2025-04-07.
URL: *https://edition.cnn.com/2023/09/19/asia/armenia-azerbaijan-nagorno-karabakh-bombardment-intl/index.html*

Novosti, RIA. 2020. " ." *RIA Novosti* . Accessed: 2020-11-09.
URL: *https://ria.ru/20201109/karabakh-1584826720.html*

Papyan, Artur. 2021. "The Cyber Battlefield is Just as Important: Armenia's Cybersecurity.". Accessed: 2025-04-03.
URL: *https://evnreport.com/magazine-issues/the-cyber-battlefield-is-just-as-important-armenia-s-cybersecurity/*

Spînu, Natalia. 2020. "Armenia Cybersecurity Governance Assessment.". Accessed: 2025-04-03.
URL: *https://www.dcaf.ch/sites/default/files/publications/documents/ArmeniaCybersecurityGovernanceAssessment.pdf*

The Kyiv Independent. 2022. "People seek relief at 'invincibility centers' amid long power outages.". Accessed: 2023-02-18.
URL: *https://kyivindependent.com/news-feed/people-come-to-invincibility-centers-in-kyivamid-long-power-outages*

United Nations. 2021. "Mandates of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions; the Special Rapporteur in the Field of Cultural Rights; and the Special Rapporteur on Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment." Available at: `https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25857`. Accessed: 2025-04-03.

VanderWeele, Tyler J and Peng Ding. 2017. "Sensitivity analysis in observational research: introducing the E-value." *Annals of internal medicine* 167(4):268–274.

Watch, Azerbaijan Internet. 2023. "Internet Disruptions in Fuzuli." Online. Accessed: 2025-04-07.
URL: *https://www.az-netwatch.org/news/internet-disruptions-in-fuzuli/*

Zhukov, Yuri M. 2023. "Near-real time analysis of war and economic activity during Russia's invasion of Ukraine." *Journal of Comparative Economics* .