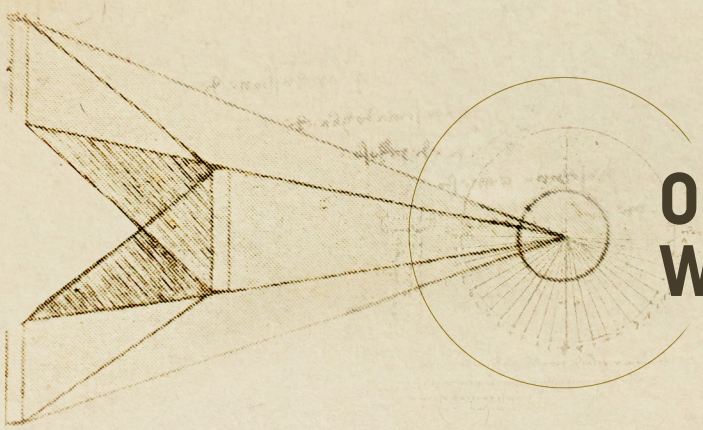

ON FUTURE WAR

Statistical Appendix

This appendix outlines a series of statistical tests based on the larger research effort describing how Russia approached using cyber operations during the first year of the war in Ukraine. The findings are all based on the Dyadic Cyber Incident and Dispute dataset, which has been peer-reviewed and used in multiple, prior academic studies.

Hypothesis 1: The period before and after the initiation of hostilities should see an increase in the frequency of cyber incidents but a decrease in their severity.

To test this hypothesis, the research team divides the variables that measure cyber severity into two groups: the pre-February 2022 group and the post-February 2022 group, the latter of which includes likely shaping cyber operations weeks before the actual February 24 invasion. Table 1 shows crosstabulations with Pearson residuals (z-scores) and chi-squared score of the two groups. The expected value is that there is an increase in the number of observations but a statistically significant decrease in the severity score. The null hypothesis is that there is no change in the observation and severity.

Table 1: Crosstabulations with Pearson Residuals and Chi-Squared Results Comparing Cyber Severity of Pre- and Post-February 24 Cyber Operations Initiated by Russia

Group	0	1	2	3	4	5
Pre-invasion	1 (0.37) 1.03	0 (4.11) -2.03	9 (8.96) 0.01	7 (7.47) -0.17	5 (3.73) 0.66	6 (3.36) 1.44*
Post-invasion	0 (0.63) -0.79	11 (6.89) 1.56*	15 (15.04) -0.01	13 (12.53) 0.13	5 (6.27) -0.51	3 (5.64) -1.11

Note: (Expected counts in parentheses)
Pearson chi-squared score = 12.2744**
Likelihood ratio chi-squared = 16.1328***
***p<.01, **p<.05, *p<.10
Counts less than 5 cannot be analyzed for statistical significance.
Severity score is 0-10. The results reported only went up to a level 5 representing single or multiple critical network infiltration and physical attempted destruction.

The Pearson chi-squared score is 12.27, which is significant at the 95 percent confidence level, and the log-likelihood chi-squared score is 16.13 and is significant at the 99 percent confidence level, indicating that there is a significant difference between severity scores of cyber operations launched by Russia during the two phases of the conflict under investigation. This also indicates that the difference between expected and actual counts on severity levels between the two groups is also significantly different. The raw counts of observed cyber incidents and larger campaigns show a larger increase in frequency. In other words, while the frequency of cyberattacks increased, the severity declined in the first year of the war in Ukraine. Looking at Table 1, the research team observes low-level probes and disruptions of Ukrainian networks (severity score 1) increased after the February 24 invasion. For severity level 5 operations, the research teams observes these operations reduced by half after the invasion.

Hypothesis 2: The period before and after the initiation of hostilities should see no change in Russian cyber targeting.

To test this hypothesis, the research team compares targets of Russian cyber operations pre- and post-invasion using a logic similar to hypothesis one. The expected value is that there should be no change in Russian cyber targeting between the two periods. The null is that Russian targeting of military targets increases.

Table 2 shows evidence that allows us to reject the notion that Russia will move away from targeting civilian infrastructure in favor of military targets in order to coerce Ukraine into submission. However, there is no significant difference in the means of the two groups, and the chi-squared shows that the difference between the expected and observed counts of the variables in these two groups is negligible. Russia's targets continue to be civilian-dominated. In other words, Russia has not altered its targeting preference.

Table 2: Crosstabulations with Pearson Residuals and Chi-Squared Results Comparing Target Type via Cyber Operations of Pre- and Post-February 24 Cyber Operations Initiated by Russia

Group	Private/Civilian	Gov't Non-military	Gov't Military
Pre-invasion	16 (16.43) -0.11	9 (8.96) 0.01	3 (2.61) 0.24
Post-invasion	28 (27.57) 0.08	15 (15.04) -0.01	4 (4.39) -0.19

Note: (Expected counts in parentheses)
Pearson chi-squared score = 0.1093
Likelihood ratio chi-squared = 0.1077
***p<.01, **p<.05

Lastly, given that most Russia's past cyber incidents are low-cost, low-payoff operations, the research team expects that its overall cyber strategy will continue to be comprised of mostly disruption and espionage efforts, rather than degradative efforts, leading to our third hypothesis:

Hypothesis 3: Russia will continue to leverage disruptive shaping activities and espionage to alter the balance of risk calculations prior to and during the conflict.

Table 3 shows the results of the two phases of the conflict between Russia and Ukraine since 2014. The research team finds that the mean value of objective type goes down significantly, indicating the preference of utilizing disruptive techniques at the expense of espionage and degradations. As articulated above, as the conflict has shifted from a hybrid, lower-intensity conflict to a full-scale war, the role of cyber operations has also shifted. More severe, degrading cyber operations are being replaced by more conventional means of destruction on Ukrainian targets by the Russian military.

Table 3: Crosstabulations with Pearson Residuals and Chi-Squared Results Comparing Cyber Objectives of Pre- and Post-February 24 Cyber Operations Initiated by Russia

Group	Private/Civilian	Gov't Non-military	Gov't Military
Pre-invasion	7 (12.69) -1.60*	13 (8.59) **1.51***	8 (6.72) 0.49
Post-invasion	27 (21.31) 1.23	10 (14.41) -1.16	10 (11.28) -0.38

Note: (Expected counts in parentheses)
Pearson chi-squared score = 8.0837**
Likelihood ratio chi-squared = 8.3083**
***p<.01, **p<.05, *p<.10

The Pearson chi-squared score of 8.08 and the likelihood ratio chi-squared score of 8.31 are significant at the 95 percent confidence level, which indicates there is a significant change in the cyber objective choice by Russia in the two groups. Furthermore, these scores indicate that that there is a significant difference between observed variable values and the expected ones. Russia has slowed its use of espionage or degradation cyber operations and have increased the low-cost, low pain disruptive techniques, which are often accompanied by information operations that contain propaganda.

That degradation has not been Russia's primary focus during the first few months of the Russo-Ukrainian war, therefore, is perhaps not as surprising. Therefore, given that there has not been a shift in the cyber objective patterns implemented by Russia, the research team finds support for the third hypothesis of a continuation of disruptive operations but fewer espionage and degradation operations. It can be assumed that the lack of degrading incidents is being substituted with conventional weapons of destruction, as evidenced in Russia's current onslaught of drones and missiles on Ukraine's critical infrastructure.

Leonardo da Vinci Sketches: wowinside/AdobeStock