



Russia-Ukraine

| Conflict Update |

October 23, 2023

Introduction

Ukraine began its counteroffensive in early June 2023 and has since undergone multiple phases. Western media largely framed the offensive as a test of Ukraine's ability to utilize Western support and weapons to retake significant territory from Russian forces. Many media outlets and Western officials questioned the wisdom of additional large support packages for Ukraine if it was unable to prove it could retake large swaths of territory. This framing was largely detrimental to the public's expectations given that Ukrainian troops faced prepared and layered Russian defenses across Zaporizhzhia and Donetsk Oblasts. Open-source images and intelligence that detailed the immense challenge of maneuvering around these defenses indicated the counteroffensive would be a long, grinding effort.

The counteroffensive began with the maximalist goal of driving towards the Sea of Azov to cut off the land bridge from Crimea that connects Russian troops in the peninsula to other parts of occupied Ukraine. Several cities in this area of southern Ukraine serve as Russian logistics hubs, including Tokmak, Melitopol, and Berdyansk. Ukraine aims to sever the ground lines of communications located in these cities to split Russian forces. While it now appears unlikely Ukraine will reach the sea in the short term, it will likely continue its efforts into 2024. However, the war risks developing into a frozen conflict as it enters its third year. Russian President Vladimir Putin has a history of using frozen conflicts to bolster his stance, and he may attempt to freeze the current positions in Ukraine to rebuild Russia's defense sector. Meanwhile, 2024 will prove a crucial test of continued Western support for Ukraine. Domestic political developments in several countries (including the United States, Poland, and Slovakia) threaten to undermine the current high levels of economic and military aid for Ukraine.

Businesses that operate in either Russia or Ukraine face significant physical, economic, and cyber threats. In Russia, cyber and economic challenges present considerable risks. Since April 2023, Russia has nationalized the assets of four Western companies that threatened to exit the Russian market. However, in Ukraine, physical risks comprise the the largest threat to firms. Areas located near the front lines of course face the highest risk of violence; however, the capital Kyiv and other cities far from the front face intermittent strikes. Firms in the defense sector face the highest level of risk; Russian officials have consistently threatened to strike any facilities that support Ukraine's military efforts. Additionally, recent strikes suggest Russia is beginning another assault on Ukrainian energy infrastructure as the winter approaches, similar to its campaign last winter. Businesses operating in Ukraine should expect operational challenges stemming from frequent power and heating outages.

Key Threats



Russia-backed hackers groups pose risks to private investment in Ukraine.



Western firms with assets in Russia risk nationalization.



Russian airstrikes will likely again target Ukrainian infrastructure this winter.



Ukraine's drone program has increasingly targeted the Russian mainland.



The war risks devolving into a drawn out conflict lasting years.



Western support for Ukraine may be dwindling.

Key Findings

- Ukraine has achieved mixed successes across its three axes of advance. However, Ukrainian forces are unlikely to reach the Sea of Azov in the short term.
- Businesses operating in both Ukraine and Russia face physical security threats, supply chain risks, cybersecurity threats, and geopolitical challenges.
- Historical data and trends indicate the war risks developing into a frozen conflict. Russia likely favors freezing the current frontlines while it rebuilds its forces and military industrial complex.
- Western support for Ukraine shows signs of dwindling. Politicians in the United States, Slovakia, and Poland have resisted future funding, while the United Kingdom announced it no longer has enough weapons to continue supplying Ukraine. Additionally, the Israel-Hamas conflict will likely draw Western focus away from Ukraine.



Current State of the Counteroffensive

Overview

Ukraine opened three axes of advance to execute the counteroffensive. Two axes—one towards Melitopol and the second towards Berdyansk—aimed to drive through Russian defenses in Zaporizhia and Western Donetsk to the Sea of Azov. These axes carried the maximalist long-term goal of severing Russian ground lines of communication between occupied Crimea and Russian-controlled territory in eastern Ukraine. Such an achievement would have split Russian troops and created significant logistical issues for the Russian forces.

The third axis of advance around Bakhmut was, and continues to be, largely a fixing operation. Ukrainian operations in this region have pinned Russian forces in this area so they cannot support the Russian defense of Zaporizhia and Donetsk. While Ukraine has gained territory around Bakhmut in recent months, a decisive victory capturing Bakhmut was not a primary goal of the counteroffensive. Ukraine instead wanted to focus its main efforts to Zaporizhia and Donetsk.

The offensive has already undergone several different phases and will likely continue to evolve. Throughout the entire offensive, Ukrainian troops encountered—and continue to face—layered, prepared Russian defenses that are extremely difficult and costly to maneuver past. These defenses effectively slowed Ukraine's progress through each stage of the offensive. Early in the counteroffensive, Ukraine used limited forces to probe the frontlines to identify Russian weaknesses. By mid-August, Ukraine committed the bulk of its reserve forces to accelerate the advance and begin what was then described as the “decisive” effort. While Ukrainian troops achieved key successes in late August and September, this stage has proved far from decisive. Ukrainian forces are unlikely to reach the Sea of Azov in the short term. Ukraine's most advanced positions remain far from the sea and continue to struggle against Russia's well-prepared defense. The offensive remains ongoing, however, and Ukraine has achieved mixed results across the three axes.[1]

Zaporizhzhia-Melitopol Axis

The Zaporizhzhia axis represents the most strategically-important and heavily-defended area of the front. Ukrainian forces are attempting to drive towards the key Russian logistics hub of Melitopol near the Sea of Azov. Ukraine has committed most of its troops and Western weapons to the advance in Zaporizhzhia. Ukrainian forces have been advancing south since June, but complex, layered Russian defenses have slowed Ukraine's progress. In late August, Ukraine officially captured the city of Robotnye and overcame the main line of Russian defenses. While both Ukrainian and Western observers were hopeful this success could lead to rapid advances further south, such progress has not materialized. As of this writing, Ukrainian forces continue to make slow marginal advances around Robotnye.[2]

Meanwhile, Ukrainian General Oleksandr Tarnavsky recently adjusted his objectives, stating his current maximalist goal is to capture Tokmak, a major road and railway hub, which would sever Russian ground lines of communication. Tarnavsky has stated such a victory would mark a major breakthrough that would allow Ukraine to push even further south towards Melitopol.[3] As of early October, Ukrainian forces have advanced close enough to bring Tokmak under direct fire. While it is unclear whether Ukraine will be able to challenge Tokmak before weather conditions turn, Ukraine is still in a decent position to target Russian supply routes through the city.

Western Donetsk-Berdyansk Axis

Ukrainian forces in western Donetsk have attempted to drive south towards Velyka Novosilka to Berdyansk on the Sea of Azov. Like Melitopol, Berdyansk is a critical Russian transit and logistics hub. Recapturing Berdyansk would sever these critical ground lines of communication; however, entrenched Russian defenses again slowed the Ukrainian advance on this axis. Ukrainian forces have liberated several small towns in their advance south of Velyka Novosilka but have not won major gains. In early October, Russian forces launched a significant assault on the city of Avdiivka in eastern Donetsk Oblast. As of this writing, Ukrainian troops have been able to hold their positions and extract heavy casualties from the Russian side. Russian attacks on Avdiivka may continue; however, Russia is unlikely to significantly compromise Ukrainian positions in this area.[4]

Bakhmut Axis

Beginning in May, Ukraine conducted a series of flanking counterattacks surrounding Bakhmut. These attacks served to pin Russian forces in Bakhmut and prevent them from redeploying to Zaporizhzhia or western Donetsk when Ukraine began its main effort along those axes. While Ukraine does not consider retaking Bakhmut to be a key objective of the counteroffensive, Ukrainian troops have made incremental gains advancing towards the city. In early October, Ukrainian forces recaptured Klishchiivka, located about eight kilometers from Bakhmut. As of this writing, Ukrainian forces continue to press Bakhmut from the southwest, west, and north.[5]

Ukraine's Drone Program

The success of Ukraine's nascent drone program in 2023—in the past two months in particular—has opened a new dimension in the war. In the first nine months of 2023, Ukraine carried out over 190 drone attacks on Russian soil and occupied Crimea.[6] These attacks represent a new Ukrainian capability to launch long-range, successful drone attacks that was previously unseen in 2022.

Ukraine began investing heavily in its drone programs soon after the war began, and those investments are now leading to significant successes. Ukraine's Army of Drones program has trained over 10,000 drone operators in 2023, while over 200 drone startup companies are currently operating in Ukraine.[7] This investment has driven both public and private companies to quickly innovate drones that can evade Russian defenses.

Around August 2023, Ukraine began increased strikes on Russian soil and on Russian positions in the Crimean Peninsula using its domestically-produced drones. Such long-range strikes deep within Russian territory were previously unimaginable without the use of Western weapons. Western nations have warned Ukraine from using their weapons in attacks on Russian soil, meaning the development of Ukraine's drone program has allowed these strikes in particular to proliferate.[8]

FOOTNOTES

[1] <https://www.understandingwar.org/backgrounder/ukraine-conflict-updates>

[2] *Ibid.*

[3] <https://www.cnn.com/2023/09/23/europe/ukraine-biggest-counteroffensive-to-come-intl-hnk/index.html>

[4] <https://www.understandingwar.org/backgrounder/ukraine-conflict-updates>

[5] *Ibid.*

[6] <https://www.bbc.com/news/world-europe-65475333>

[7] <https://www.ukrainianworldcongress.org/united24/>

[8] <https://www.reuters.com/world/europe/ukraine-shouldnt-use-us-arms-inside-russia-us-general-says-2023-05-25/>



Risks to Businesses Operating in Russia & Ukraine

Physical Risk of Operating in Ukraine

Businesses located in Ukraine face a high physical security risk due to frequent Russian strikes throughout the country. Areas near the front lines in eastern and southern Ukraine face the highest incidence of Russian strikes. However, the capital of Kyiv and cities in western Ukraine continue to suffer intermittent strikes.[9] Personnel face obvious physical risks due to these strikes, while facilities may suffer physical damage or experience operational complications due to the disruption of critical infrastructure networks.

In the fall and winter of 2022, Russia launched a campaign to destroy Ukraine's electric grid and energy systems to pressure civilians. The campaign caused widespread electricity and heating outages. Russia began similar strikes at the end of September 2023, and on October 6, Ukrainian President Volodymyr Zelensky warned "this winter, Russian terrorists will again try to destroy our energy grid." [10] While Ukraine currently has more effective air defense systems in place than last winter, some Russian missiles will still likely penetrate these defenses. Businesses operating in Ukraine should expect increased airstrikes and operational disruptions due to electricity and heating outages during the upcoming winter months.

Companies in the defense sector face especially high physical security risks. Russia has repeatedly vowed to consider any facilities that support Ukraine's defense industry as legitimate military targets.[11] These threats apply even to Western firms that are based in NATO member states. While striking the facility of a NATO-based business would prove a sharp escalation, such an attack cannot be ruled out. Russia has demonstrated a high aptitude for risking conflict with NATO countries throughout the war. Debris from Russian missiles has landed in NATO member states Poland and Romania several times since 2022.[12]

Physical Risk of Operating in Russia

Companies that operate near the Russian border with Ukraine face increased security risks. Pro-Ukrainian volunteer fighting organizations such as the Russian Volunteer Corps and Freedom of Russia Legion frequently raid the border regions of Bryansk and Belgorod.[13] Additionally, Ukraine's newfound drone capabilities have led to increased drone strikes in Russia. These strikes typically target Russian military sites; however, collateral damage in areas near military targets cannot be ruled out.

Risk of Nationalization in Russia

In April 2023, President Putin signed a decree that allows the government to seize the Russian assets of any company based in an "unfriendly" country. The decree states Russia's Federal Agency for State Property Management will establish temporary administration of the seized assets. Russia maintains a list of over 40 countries that it considers unfriendly.[14] This list includes countries that have promoted anti-Russia policies or imposed sanctions on Russia. While there are several Asian countries on the list, such as South Korea and Japan, most of the "unfriendly" states include the United States and its Western allies.

Russia is most likely to seize the assets of Western companies that have previously expressed their intent to exit the Russian market. As of this writing, Russia has nationalized the assets of four Western firms: Finland's Fortum, Germany's Uniper, France's Danone, and the Netherlands' Carlsberg—all of which stated they would soon leave Russia.[15]

Regional Cyber Risks

Cyber activity continues to play a secondary role in the counteroffensive, with threat actors preferring to utilize criminal and political cyber intrusions over military ones. Threat actors from both sides have continued to target public and private company websites with disruption and website defacements. The mass proliferation of mis- and disinformation online about the war continues, with viral photos and videos circulated that have later been determined to be false or misleading.

Hacktivist groups remain the most obvious risk to business operations inside Ukraine. The most well-known is Killnet, a likely Russian-backed group that specializes in distributed denial-of-service (DDoS) attacks. Killnet emerged ahead of the war in Ukraine and has since expanded its hacktivism to the Middle East, where it has engaged in DDoS attacks in support of Palestine. (Killnet said they targeted Israel over its support for Ukraine.[16]) One of the most prominent threat actors since the counteroffensive began has been the Russian-backed group NoName057[17]; it has escalated its targeting of European websites and infrastructure facilities over perceived support for Ukraine. This has also included targeting Ukrainian-based websites. Other pro-Russian groups that have escalated their activity since the counteroffensive—largely carrying out DDoS attacks—include Народная Cyber Армия, NET-WORKER ALLIANCE, BLUENET RUSSIA, ZulikGroup, and **AltroX**. ZeroFox observed an increase in these sorts of attacks during the onset of the counteroffensive followed by a notable slowdown in August 2023.[18]

While less numerous, the cyber targeting of businesses in Russia is similar to that in Ukraine and is led by the IT Army of Ukraine, which routinely launches DDoS attacks against Russian entities ranging from financial services to government websites and energy firms. One of the most dominant pro-Ukraine-backed cyber groups since the counteroffensive began has been **теки инормации**, a data leak group that is targeting government and private industries inside Russia.[19] The leaks are likely aimed at exposing the personal information of backers of the war.

Russia has likely expanded its cyber intelligence and espionage efforts since the war decreased options for human intelligence. Russian intelligence agencies seeking information will likely need to engage in cyber espionage in order to gain information, especially when it comes to European support for Ukraine—including the amount and types of military support. In a report from late September 2023, Ukraine accused Russian-backed hackers of seeking to obtain information from Ukrainian law enforcement ranging from evidence of Russian war crimes to data on Russian attacks, including the effectiveness of Russian drone attacks on Ukraine. Similar attacks were allegedly aimed at private companies, including arms contractors and those along the military supply chain.[20]

Businesses operating in Ukraine, especially new ones entering the market, are highly vulnerable to these sorts of attacks because Russian threat actors want to deter new investment and growth in Ukraine. While this politically-motivated targeting against government agencies, critical infrastructure, and financial institutions receives significant media attention, it typically has limited impact, causing short service outages and disrupting access to information.

FOOTNOTES

- [9] <https://acleddata.com/ukraine-conflict-monitor/>
- [10] <https://www.radiosvoboda.org/a/news-zelenskyy-stavka-viyna-rosiya/32626531.html>
- [11] <https://www.bbc.com/news/business-66679312>
- [12] <https://www.nytimes.com/2023/09/13/world/europe/russian-drone-romania.html>
- [13] <https://www.reuters.com/world/europe/who-are-armed-fighters-russias-belgorod-region-2023-06-05/>
- [14] <https://publication.pravda.gov/ru/Document/View/0001202304250033?rangeSize=1&index=1>

- [15] <https://www.bloomberg.com/news/articles/2023-07-16/russia-takes-temporary-control-of-danone-and-carlsberg-assets>
- [16] https://t.me/killnet_reservs/7674
- [17] ZeroFox Internal Collections
- [18] *Ibid.*
- [19] *Ibid.*
- [20] [https://regmedia\[.\]co.uk/2023/09/25/russia_cyber_tactics_hl_2023.pdf](https://regmedia[.]co.uk/2023/09/25/russia_cyber_tactics_hl_2023.pdf)



Forward Look

Weather Conditions

Cold and wet autumn weather conditions will set in across the front within the next month. Muddy conditions will hamper armed vehicle maneuvers and likely slow Ukrainian operations. However, President Zelensky and other Ukrainian military officials have firmly stated the counteroffensive will continue through adverse weather.[21] Ukraine may attempt to maintain counteroffensive operations through the winter, when a hard ground freeze would allow vehicles to easily traverse terrain. Ukraine may be reluctant to ever officially declare an end to the counteroffensive without achieving more marked successes. Some observers have suggested rhetoric surrounding the “counteroffensive” may continue well into the spring or summer, despite traditional counteroffensives typically lasting only months.[22] ZeroFox assesses this would mark a rhetorical change rather than an operational shift. Irrespective of whether the counteroffensive has a definitive end date, the fighting will generally follow the seasonal patterns of last year. The fighting will slow towards the end of autumn and winter before ramping up again in the spring and peaking in the summer.

Risk of a Frozen Conflict

The war looks increasingly likely to become a long, drawn out conflict as it approaches its third year. Russian President Vladimir Putin likely supports forcing Ukraine into a frozen conflict, which would allow time for Russia to rebuild its forces and military industrial sector. Putin also likely believes Western support for Ukraine will wane over time, allowing Russia to degrade Ukrainian forces and essentially wait out Ukraine. Putin has historically adopted a strategy of freezing conflicts to bolster his position, most notably in this very conflict. After Russia annexed Crimea in 2014, Russia emboldened nonstate groups in Donetsk and Luhansk to continue fighting in eastern Ukraine. Russia would occasionally ratchet up the pressure to exact concessions but largely waited eight years to further develop its military before launching its full invasion in February 2022.

Data from past wars also supports the possibility of a stalemate. According to the Center for Strategic and International Studies, interstate wars that last for over one year extend to over a decade on average.[23] A frozen conflict in Ukraine would likely resemble the situation after Russia annexed Crimea in 2014. Most of the fighting would likely occur along the frontlines in southern and eastern Ukraine, while areas far from the front could experience a precarious calm. However, even in this scenario, regions far from the front could continue to face sporadic airstrikes. In this event, both sides will likely increase their cyber operations, seeking to weaken private and public companies. Cyber espionage efforts that replace the human intelligence capabilities both sides had prior to the war are also likely in the event of a stalemate.

Western Aid

The next year will prove a critical test of Western support for Ukraine. While some assistance is already slated to go ahead in 2024, volumes could significantly drop off towards the end of 2024 into 2025. The recent war in Israel may now redirect the United States’ focus and supplies from Ukraine to its longtime ally, Israel. Moreover, recent domestic political developments in several countries indicate Western material support for the war may be waning.

In Slovakia, populist former Prime Minister Robert Fico was re-elected to lead the country on September 30. During his campaign, Fico promised to halt military aid to Ukraine and criticized Western sanctions on Russia. In October, Fico’s Smer-SSD party formed a coalition with the center left Hlas and nationalist SNS parties, which looks poised to reduce aid to Ukraine.[24]

In September, Poland’s populist ruling Law and Justice (PiS) party indicated it would halt future military aid to Ukraine amid rising tensions over Ukrainian grain exports. However, the results of Poland’s recent October 15 elections suggest a more liberal, pro-European Union governing coalition will come to power, which will likely demonstrate continued support for Ukraine.[25]

In the United States, Congress excluded aid to Ukraine in the stopgap deal to avoid a government shutdown. House Republicans assured they would hold a separate vote on Ukraine funding; however, the ousting of Speaker Kevin McCarthy and subsequent tumult have delayed any such vote.[26] Meanwhile, several Republican presidential candidates for the 2024 elections have indicated they would reduce funding and military support to Ukraine.[27]

The Israel-Hamas conflict will also likely complicate Western aid. The United States is a staunch Israeli ally and has already promised to provide Israel with weapons and other military aid as the conflict progresses.[28] While the two conflicts require different forms of military aid, opponents would still be able to argue that the United States cannot afford to arm two simultaneous wars. This challenge could lead the government to decrease aid for Ukraine to reserve greater support for Israel.

The Biden administration is considering combining aid for Ukraine and Israel into one bill to increase the odds Congress will approve further support for Ukraine.[29] However, this would likely involve a one-time deal between the administration and representatives. The longer both conflicts drag on, the more like it is that Congress may force the Biden administration to prioritize Israel. Support for Ukraine is unlikely to disappear all together, but the amount of aid would likely diminish over time.

Assessment:

- Weather conditions will soon affect the pace of Ukraine’s counteroffensive. However, Ukrainian officials are adamant fighting will continue through the fall.
- The pace of fighting will likely follow seasonal patterns observed last year. Fighting will slow in the fall and winter before ramping up in spring and peaking in summer.
- The war looks increasingly likely to develop into a frozen conflict.
- Domestic political conditions in several Western countries may affect the level of aid for Ukraine in 2024 and 2025.

FOOTNOTES

[21] <https://www.youtube.com/watch?v=Inbl5R6MjFY>
 [22] <https://www.understandingwar.org/backgrounder/ukraine-conflict-updates>
 [23] <https://www.washingtonpost.com/national-security/2023/08/17/ukraine-counteroffensive-melitopol/>
 [24] <https://euromaidanpress.com/2023/10/16/slovak-coalition-agreement-signals-reducing-support-for-ukraine/>
 [25] <https://www.politico.eu/article/opposition-wins-polish-election-according-to-exit-poll-poland-kaczynski-aida-tusk-election-rule-of-law/>

[26] <https://foreignpolicy.com/2023/10/16/congress-israel-ukraine-house-speaker-republicans-foreign-policy/>
 [27] <https://www.nytimes.com/interactive/2023/09/18/us/politics/republican-candidates-2024-ukraine.html>
 [28] <https://www.c-span.org/video/?531206-1/president-biden-remarks-us-support-israel>
 [29] <https://www.bloomberg.com/news/articles/2023-10-10/biden-weighs-combining-ukraine-israel-aid-as-some-in-gop-balk>



APPENDIX A:

ZeroFox Intelligence Probability Scale

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

APPENDIX B:

Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: GREEN

HOW IT IS USED

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: AMBER

HOW IT IS USED

Sources may use TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: CLEAR

HOW IT IS USED

Sources may use TLP: CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP: CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident, and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers—including some of the largest public-sector organizations, as well as finance, media, technology, and retail companies—to stay ahead of adversaries and address the entire lifecycle of external cyber risks.

READY TO SEE FOR YOURSELF?

Request a Demo:

Sign up on zerofox.com/request-a-demo

Learn More:

Visit zerofox.com

Contact us at sales@zerofox.com / 855.736.1400

