THREAT ANALYSIS

Recorded Future®

By Insikt Group®

February 9, 2023

Themes and Failures of Russia's War Against Ukraine

Executive Summary

A year after Russia launched its full-scale invasion of Ukraine, Russia remains unsuccessful in bringing Ukraine under its control as it struggles to overcome months of compounding strategic and tactical failures. Despite these challenges, the Kremlin's intent remains unchanged, leaving Ukraine and the international community at heightened risk. In anticipation of Russia's planned renewed offensive, this report reflects on Russia's key hybrid warfare themes over the past year, including military failures, exploitation of natural resources, reliance on "proxy" groups, and partnerships with anti-Western allies. By doing so, this report illuminates the Kremlin's strategic miscalculations and its strategies for overcoming its shortfalls.

In the near term, Russia will very likely launch a renewed offensive in Ukraine with a likely focus on the Donbas. Russian state-sponsored cyber threat actors, as well as pro-Russian cybercriminals and hacktivists, will almost certainly support this campaign through continued targeting of Ukrainian critical infrastructure, at least in part in an attempt to further degrade Ukraine's morale and will to fight. Meanwhile, Russia will also have to manage the direction of largely untrained troops and modern weapons shortages, with likely reliance on recently mobilized troops, "proxy" organizations like Wagner, and foreign weapon supplies from Iran and North Korea to augment its capabilities.

In the longer term, Russia's actions over the past year have caused lasting geopolitical shifts far beyond Ukraine. In particular, the success of Ukraine's collective defense model resonates globally, and European shifts away from reliance on Russian gas, serve to remind the international community about the benefits of allied cooperation and the importance of global partnerships. These partnerships are further supported by Russia's burgeoning military cooperation with Iran and North Korea, which creates a heightened global threat environment. As the war stretches on, the risk of Belarus's involvement, escalation in the conflict, degraded Ukrainian morale, and international complacency compound, further threatening the security of both Ukraine and the international community.

Key Judgments

- Russia was almost certainly challenged by Ukraine's cyber defenses, which were bolstered by its allies and industry partners, rendering cyber operations unable to substantively augment Russia's conventional military progress and demonstrating the importance of collective defense.
- Russia's persistent kinetic and cyber targeting of Ukraine's civilians and critical infrastructure throughout winter very likely reflects the Kremlin's intent to degrade Ukraine's morale ahead of an upcoming, renewed offensive.
- Russia's persistent use of "proxy" groups throughout the conflict, such as Wagner Group and pro-Russian cybercriminals, hacktivists, and influence actors, has revealed Kremlin control or direction over these groups, while further illuminating Russia's desire to have plausible deniability over its actions.
- Russia has strengthened international partnerships with key anti-Western allies, including Iran and North Korea, who are likely to continue providing material support to Russia for its war against Ukraine and pose increasing threats to the West as their military cooperation expands.
- Russia's leveraging of its natural resources over the past year has pushed the West to find alternative fuel sources, which will very likely decrease Russia's ability to exert pressure over the international community.
- While Russia maintains its intent to bring Ukraine under its control, the numerous, unaddressed challenges its military faced during the initial invasion, in addition to largely untrained troops, weapons shortages, and Ukraine's military being armed by the West, will very likely challenge future Russian successes on the battlefield.
- As the war continues, a variety of risks threaten both Ukraine and the international community, including formal Belarusian involvement, the potential for escalation, degraded Ukrainian morale, and international complacency.

Key Hybrid Warfare Themes

Hybrid Military Failures Reflect Putin's Strategic Miscalculations

On February 24, 2022, after amassing between 169,000 and 190,000 troops at Ukraine's border, Russia launched its full-scale invasion of Ukraine. Russia planned to seize Kyiv within a few days, dismantle Ukraine's government, and secure a decisive military victory. However, Russia's ambitions for its Ukraine offensive appeared misguided relative to the physical capacity it demonstrated on the frontlines. Similarly, its highly anticipated use of cyber operations to fulfill its hybrid warfare strategy consistently fell short without substantively enabling troop progress. Amid these failures, Russia's attempts to weaken Ukrainian morale have likely become increasingly critical to its warfighting strategy, particularly ahead of the very likely renewed Russian offensive in 2023.

Russia's Conventional Military Failures Illuminate Poorly Organized, Ill-Prepared Forces

Almost immediately, the Russian military struggled with command and control as it attempted to coordinate operations across multiple lines of efforts. Logistical challenges quickly stalled troop advancements and supply lines, while the troops themselves were ill-prepared for combat. Soldiers suffered from insufficient preparation, poor operational security practices, and subpar equipment and food, which contributed to declining troop morale. Even special forces units, including the VDV (an elite paratrooper and air assault force) and Spetsnaz (elite light infantry units), failed to accomplish their objectives, sustaining substantive personnel and equipment losses alongside the rest of Russia's military. The Kremlin continued to shift its objectives in Ukraine to smaller, more concentrated geographic areas, confirming its inability to sustain a dispersed ground offensive amid a united and fierce Ukrainian resistance.

These challenges compounded over time, particularly as Russia suffered substantive manpower losses on the frontlines. While exact figures vary, the United States government assessed that Russian casualties (killed and injured) exceeded 100,000 soldiers in November 2022. In January 2023, Ukrainian estimates reported that Russian losses, strictly referring to those killed in action, exceeded 118,000 individuals without accounting for injured personnel. To compensate, the Kremlin mobilized at least 300,000 relatively inexperienced citizens into its armed forces, which resulted in protests and a new wave of migration out of Russia. As of early February 2023, Ukrainian intelligence estimates Russia has over 300,000 troops in Ukraine, which is double Moscow's original invasion force.

Russia has also faced weapons shortages due to its protracted conflict, forcing it to resort to making modifications to aging weapon systems. As early as July 2022, the Russian military was seen employing modified Soviet-era anti-aircraft missiles to strike land-based targets, demonstrating its desperation to find new sources of munitions amid shortages. This technique continues to be relied on in 2023, as demonstrated with Russian shelling against Ukraine in mid-January. The United Kingdom's Ministry of Defence (MOD) also reported that Russia was removing nuclear warheads from its aging nuclear cruise missiles to fire at Ukraine unarmed, rendering them inert and reflecting the depletion of Russia's long-range missile stock. At the time of writing, Russia is also relying on international partnerships to overcome its shortages, as detailed later in this report.

Meanwhile, the Kremlin's rapid replacements of command elements, coupled with general military failures over the last year, very likely demonstrated Putin's dissatisfaction with the military's performance. The commander of Russia's Ukraine offensive was replaced 3 times since Army General Aleksandr Dvornikov assumed the role in April 2022, with Colonel General Gennady Zhidko in June 2022, Army General Sergey Surovikin in October 2022, and eventually the Chief of the General Staff Valery Gerasimov in January 2023. Gerasimov's appointment was particularly notable as he is only formally outranked by Sergei Shoigu, Russia's minister of defense, and Putin himself. Russian general staff publicly acknowledged that Gerasimov's appointment stemmed from the "need to organize closer interaction between the branches and arms of the Armed Forces" and improve "command and control", reflecting the Kremlin's awareness of its failures to date.

Offensive Cyber Warfare Failed to Augment Conventional Shortcomings, Highlights Importance of Collective Defense

Russia's cyber operations over the past year have similarly failed to contribute to any meaningful military victories or control of Ukraine's information environment, two likely elements of Russia's cyber objectives. In the buildup to Russia's invasion of Ukraine, and in the first few months of the war, there were multiple cyberattacks that aligned with Moscow's strategic objectives. These included (distributed) denial-of-service (DoS/DDoS) attacks, wipers, website defacements, and scam emails, targeting Ukrainian government organizations, media organizations, e-services used by citizens, and other private sector organizations, including an American satellite communications company that provided internet connectivity to Ukrainians. But as the war continued for longer than Russia originally intended, and as conventional military forces struggled to hold ground, the mass cyberattacks launched by Russia failed to significantly bolster Russia's conventional military progress.

Russia's historical and public use of offensive cyber operations around the world serve as a reference point for its sophisticated and damaging capabilities. Attacks include those launched against Ukraine's energy sector in 2015 and 2016, leaving hundreds of thousands of Ukrainians without power, and the use of NotPetya in 2017 to target Ukraine's financial system, which proliferated globally and resulted in more than $10 billion in damages. More recent operations, including the Russian Federation's successful breaches of harder targets like US government agencies and corporations in the 2020 SolarWinds breach, led the world to expect similarly skillful operations to be used against Ukraine. However, over the last year, the majority of tracked Russian cyber operations failed to inflict damage comparable to previous destructive cyber operations.

In fact, Russia's historical cyber targeting of Ukraine very likely contributed to its lack of success over the past year. Ukraine and its defenders have ample experience repelling repeated, persistent, and sophisticated Russia-nexus cyberattacks since at least 2014 and have learned and improved their cyber defenses continuously. Targets like Ukraine's energy sector had been hardened to offensive cyber operations largely due to joint Ukrainian-Allied efforts to shore up Ukrainian networks. For example, in April 2022, a cyberattack against Ukraine's energy sector using INDUSTROYER2 and CADDYWIPER malware was thwarted, unlike similar attacks in prior years. To date, the collaboration continues, as Ukraine formally joined the North Atlantic Treaty Organization's (NATO) Cyber Defense Center in January 2023.

This committed and unified response by allies and industry partners (particularly in cybersecurity and threat intelligence; 1, 2, 3) have bolstered Ukraine's cyber defenses and enabled them to resist Russian attacks, even in real time. Ukraine's ability to successfully mitigate the role of Russia-nexus cyberattacks stands as a model for successful defense that can be applied in future conflicts with adversarial nations who employ hybrid tactics. The collective defense of Ukraine by government, military, and cybersecurity and threat intelligence partners has almost certainly lessened the damage of cyberattacks in the war, reducing Russia's ability to achieve its strategic objectives.

Russia's Reinvigorated Attempts to Decrease Civilian Morale Emphasize Kremlin's Desperation

Throughout the war, Ukraine's steadfast response and willingness to fight the Russian Federation almost certainly contributed to Russia's wartime challenges. Substantially outnumbered Ukrainian troops found creative ways to fight back, such as by removing road signs so Russians would struggle to navigate foreign terrain. Ukrainian president Volodymyr Zelensky served as a beacon of opposition, unifying troop morale as he demonstrated his leadership through his frequent visits to the front lines despite warnings of assassination plots and offers from allied nations to evacuate. The international community rallied behind Zelensky and has supported Ukraine with substantive aid in the form of weapons, financial support, and punitive actions against the Russian Federation, which has further bolstered Ukrainian troops' ability to defend against Russian advancements.

Russia very likely prioritized the demoralization of Ukrainian troops to secure its victory, particularly as Ukraine's advancements persisted. In October 2022, Ukraine delivered a shocking blow to Russian leadership when it bombed the Kerch Strait Bridge, Russia's only land-based connecting point to Crimea, used to deliver supplies to Ukraine-based troops. And by November 2022, Ukraine had reclaimed over 50% of the territory initially seized by Russia, including major strategic points like Kharkiv and areas that Russia amended its constitution to claim, most notably Kherson. Throughout these advancements, the Kremlin increased critical infrastructure targeting in Ukraine, very likely out of desperation to decrease the morale of Ukraine's troops and citizens.

Since October 2022, Russia has attacked resources like water and electricity infrastructure, as well as civilians themselves, with some demonstrations of coordinated campaigns from conventional and cyber forces. Russia focused on striking Ukrainian water and transportation infrastructure in October 2022, reducing civilian access to essential services and leaving over 80% of households in Kyiv without water. By the end of November 2022, essentially all thermal and hydraulic power plants in Ukraine had been damaged, and according to the CEO of a Ukrainian energy provider, "Ukrainians will most likely have to live in a shutdown mode until at least the end of March [2023]" for the power grids to be restored. And in January 2023, Russia attacked 6 of Ukraine's oblasts (regions), killing over 40 civilians after striking an apartment complex in Dnipro. Notably, Russia had previously targeted substantial Ukrainian critical infrastructure earlier in the war, though the efforts appeared to have been less focused. Conversely, Russia's more recent targeting demonstrated coordination with Russian kinetic and cyber attacks against Ukrainian critical infrastructure elements, as reported by Microsoft in December 2022.

These operations were almost certainly conducted with planning for Russia's next phase of the war in mind, whereby Russia hoped that weakened enemy morale would increase its chances for success. The Kremlin has a long-standing strategy of using information and psychological effects in an effort to defeat enemies "from within", and Russia's psychological targeting through critical infrastructure damage pairs with the Kremlin's initiatives to spread disinformation that Russia was actually winning the war and that Ukraine had no hope to compete. After acknowledging in December 2022 that the war could be a "lengthy process", Putin included centralizing control of the Russian information space as a key goal to improve the Russian war effort, further confirming the Kremlin's objective of controlling the information environment to the detriment of the Ukrainian populace.

Reliance on "Proxy" Groups Reveals Deeper Connections

While Russia's historical reliance on proxy groups is well documented, Russia's war against Ukraine has demonstrated how private military companies (PMCs), cybercriminal and hacktivist groups, and influence operators have advanced Russia's strategic agenda with varying degrees of connections to the Russian state. In some cases, the war revealed closer ties between the Russian state and its proxies than originally suspected, while in others, Russian intelligence services were found to actually be responsible for the "proxies" themselves. Russia's failed attempts to exert power through proxies while maintaining plausible deniability sheds light on the importance the Kremlin places on information warfare and the lengths to which it will go to manipulate the information environment.

Wagner Group

Russia has relied on Wagner Group, a so-called PMC, to bolster its warfighting efforts over the past year. Wagner's support for Russia's war against Ukraine began just months into the war, as mercenaries were relocated from around the world, including from Libya, to support Russia's campaign. Reports indicate that Wagner's violent tactics have contributed to some of Russia's progress throughout the war, including January 2023 efforts to capture Soledar in the Donbas as part of a broader effort to cut off Ukrainian supply routes. Wagner reportedly had over 50,000 troops deployed in Ukraine after recruiting over 40,000 from Russian prisons with the promise to pardon individuals after fighting for 6 months, though January 2023 reporting indicates this number may have significantly declined in light of battlefield losses.

Over the last year, Wagner's activities have provided insight into its deeper connections to the Russian state. Videos showed Russian oligarch and Putin ally Yevgeny Prigozhin actively involved in prison recruitment despite his denials of involvement in the group. However, in September 2022, Prigozhin publicly confirmed his connections to Wagner Group when he admitted to owning the PMC. In January 2023, he admitted he also founded, led, and financed Wagner Group in 2014, whereby the group provided support to Russia's annexation of Crimea. Prigozhin has previously been identified as the leader and financier to other key Russian proxy projects, including the Internet Research Agency (IRA), the US Treasury's Office of Foreign Assets Control (OFAC)-designated Russian troll farm that was involved in 2016 US elections interference. As of January 26, 2023, Wagner Group itself was designated a significant transnational criminal organization for "widespread human rights abuses and extorting natural resources", among other criminal enterprises.

Moreover, Wagner appears to have integrated forces into Russia's warfighting effort rather than its mercenaries serving as distinct, independent elements, further undermining its claimed autonomy from the Russian state and, in some cases, its capabilities. In July, the UK's MOD reported that Russia had assigned Wagner roles on the frontlines in Ukraine, just as Russia would task out its own army units. Similarly, Wagner has appeared reliant on Russian MOD equipment, with the Institute for the Study of War (ISW) stating that the group is "functioning more as a parasite of the Russian Armed Forces than as the entirely self-contained, parastatal organization that Prigozhin tries to present it as being". Wagner also benefited from shipments of Iranian unmanned aerial vehicles (UAVs) and North Korean artillery shells in November and December of 2022. These shipments aligned with comparable provisions provided by these nations to Russia's actual military forces, further illuminating connections and interreliance between Wagner Group and the Russian state. As of late January 2023, Russian parliament is considering criminalizing public criticism of Wagner mercenaries, just as it has for its own armed forces.

Pro-Russian Cybercriminal and Hacktivist Groups

Russia has also benefited from cyber "proxy" groups advancing Russia's strategic interests, but researchers have uncovered that some of these groups are actually Russian intelligence services rather than independent cyber actors. For example, the Russian advanced persistent threat (APT) actor EMBER BEAR masqueraded as cybercriminal group "FreeCivilian" to leak information on the now-defunct website Raid Forums. Other noteworthy cases of Russian state-sponsored APT groups masquerading as cybercriminals while targeting Ukraine include Prestige ransomware, RansomBoggs, and Cyber Berkut, which have since been attributed to Russia's Main Directorate of the General Staff of the Armed Forces (GRU) by Microsoft, ESET, and the UK's National Cyber Security Centre, respectively.

Meanwhile, some cybercriminals and self-proclaimed "pro-Russian hacktivist" groups were found to be taking direct orders from the Russian state. After the now-defunct Conti ransomware group declared its allegiance to the Russian government on February 24, 2022, the Russian state began to coordinate APT campaigns with cybercriminal targets. Similarly, according to Mandiant, hacktivist groups that share a direct lineage with XakNet, such as the Information Coordination Center (ICC) and National Cyber Army of Russia REBORN, have overlapping victimology with wipers deployed in Ukraine by a Russian APT, indicating Russia is likely coordinating targeting efforts with the group. The overwhelming majority of attacks claimed by the pro-Russian hacktivist groups are false, misleading, or exaggerated in impact. However, their claims are often weaponized by Russia and international media to project support for Russia's objectives in Ukraine, as well as to stoke fear and degrade support for Ukraine, aligning with Russia's broader disinformation trends.

Importantly, attacks that appear to emanate from pro-Russian cybercriminals and hacktivist groups complicate potential international responses. These groups have targeted entities outside of Ukraine in retaliation for their support to Ukraine without fear of escalating the conflict due to their apparent independence from the Russian state. As further connections are drawn between these groups and Russian intelligence, the risk of escalation in response to some cybercriminal and hacktivist operations likely increases.

Cyber Front Z

Much as Russia has benefited from various "proxy" hacktivist groups, Russia has similarly relied on pro-Russian influence networks to support Russia's propaganda and disinformation ecosystem. Cyber Front Z is a Telegram-centric troll farm that launched in March 2022, consisting of both paid employees and volunteers, with a goal to "fight back in the information field the propagandists of the Kiev [sic] junta funded by the Western world". The group has largely echoed Russian state disinformation narratives online to over 115,000 subscribers and has established many working relationships and collaborative partnerships among other prominent pro-Russian Telegram "bloggers", public officials, as well as hacktivists, like the ICC and Killnet.

Cyber Front Z also has ties to Prigozhin and his projects according to the UK Government report from May 2022 and private industry. In August 2022, Meta announced that it had neutralized over 1,000 Instagram accounts and 45 Facebook accounts attributed to Cyber Front Z. Meta's report stated Cyber Front Z's activity "appeared to be a poorly executed attempt, publicly coordinated via a Telegram channel, to create a perception of grassroots online support for Russia's invasion by using fake accounts to post pro-Russia comments on content by influencers and media", and went on to identify links between the group and the IRA. Finally, the Prigozhin-connected PMC Wagner Center Telegram account introduced Cyber Front Z to its followers and stated it was a new tenant of PMC Wagner Center, further emphasizing connections between the "proxies".

Partnerships with Anti-Western Allies Amid International Isolation

In response to Russia's aggression, the international community has largely united to condemn the Kremlin's actions and provide Ukraine support. Over 75% of the United Nations General Assembly stood against Russia's actions in Ukraine, while Western sanctions have sought to cripple Russia's economy. Dozens of NATO nations also contributed to the aforementioned sending of weapons and economic support to Ukraine. Private sector companies have similarly allied against Russia's actions, with over 1,000 companies curtailing Russia-based operations in a show of solidarity.

In response to its increasing international isolation, the Kremlin has sought to strengthen partnerships with allies, to varying degrees of success. Iran and North Korea, for example, have publicly stood with Russia and provided material support for the war in exchange for Russian weapons and grain. Belarus has similarly supported Russia's war effort by providing Russia access to its territory for staging attacks against Ukraine. China has maintained a more neutral stance but has supported Russia's economy and broader war efforts by increasing its purchases of Russian exports. These partnerships, if lasting, pose numerous threats to Ukraine and the broader international community, including nearby access to key Russian targets like Kyiv, and the potential for collaboration to advance the military capabilities of Russia, Iran, and North Korea.

Iranian UAVs for Military Support

Russia has strengthened ties with Iran, particularly as Tehran has augmented Moscow's weapons shortages by providing material support for the war. As early as August 2022, Russia has used Iranian-supplied Shahed-136 UAVs in Ukraine, largely to target Ukrainian critical infrastructure and civilian structures en masse. Some reports indicate Iran has sold upwards of 6,000 UAVs to date, with Russia receiving Iranian military training on the operational employment of these devices. As previously mentioned, Wagner Group also appears to have benefited from Iranian UAV shipments.

In return, Russia is providing Iran with "unprecedented levels of military and technical support", according to US officials, including helicopters and air defense systems. For example, Iranian pilots were trained to operate Sukhoi Su-35 (NATO reporting name Flanker-E) fighter aircraft, with expected delivery of the aircraft to Iran in March 2023, which will almost certainly enhance Iran's aging air defense capabilities. Russia and Iran are also seeking to bolster collaboration on topics like trade, economics, energy, and regional security, demonstrating the broader effects of their burgeoning military partnership.[1]

North Korean Artillery Shells and Rockets for Grain

Russia has similarly bolstered its relationship with North Korea. In September 2022, Russia was reportedly in negotiations with North Korea to purchase "millions" of artillery shells and rockets, signaling Russia's desperation to find alternatives for weapons shortages. This collaboration presents unique opportunities for Russia, as North Korea maintains stockpiles of weapons compatible with Soviet-era systems and has domestic production facilities that can be used to augment Russia's depleted stockpiles. Just 1 month later, the US released information that North Korea was covertly supplying Russia with artillery shells for use in Ukraine, confirming the collaboration.

Wagner Group also benefited from North Korean artillery shells, much as it did from Iranian UAVs. This comes after North Korea offered public support for Russia by recognizing Russia's claim over the so-called Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR) in Ukraine's Donbas region and offering to send workers to help rebuild the Russian-occupied territory. In turn, Russia is attempting to ameliorate North Korea's food crisis by sending grain. In November 2022, railway trade between the countries also resumed for the first time since March 2020, which will very likely result in a greater exchange of Russian grain for North Korean arms.

Belarusian Territorial Access for Financial Gain

While Iran and North Korea augmented Russia's war largely with weapons shipments, Belarus enabled Russia primarily through its close access to key Ukrainian territory like Kyiv, as well as material support. From the beginning of the war, Minsk allowed Russia to launch its attack on Ukraine from its territory. Belarus also enabled Russia to bypass some Western sanctions for technology and software and was subsequently sanctioned itself. Meanwhile, the two militaries have increased partnerships, including through the formation of a "joint regional grouping of troops" based out of Belarus. Moreover, Belarus amended its constitution in 2022 to allow for the deployment of Russian nuclear weapons in Belarusian territory. To this end, Russia upgraded Belarusian Sukhoi Su-25 (NATO reporting name Frogfoot) close-air support jets to be able to carry nuclear weapons.[2] While there are no indications that Russia has already deployed nuclear weapons to Belarus, constitutional amendments and technical modifications reflect the level of military cooperation between the two countries. Russia has also offered Belarus stays on its repayment of over $1 billion USD in loans, provided additional loan funding, and is selling gas to Belarus at a historically low rate in trade.

Russia continues to use Belarus as a staging ground for its attacks on Ukraine, as seen in January 2023, when Russia launched a mass shelling of Ukraine from Belarus using S-300 and S-400 missile systems. And Belarus provides Russia the opportunity for a particularly dangerous scenario in future warfighting efforts whereby a major offensive could be launched against northern Ukraine, including Kyiv. However, at present, Russia likely lacks the command and control to effectively manage such a maneuver, according to analysis by the ISW. In the longer term, following 2023 joint Russian-Belarussian exercises however, this scenario becomes increasingly likely.

1 https://www.irna[.]ir/news/85007535

2 https://ria[.]ru/20221015/tekhnologii-1824221796.html

China's Political Balancing Act

China has taken a more measured, diplomatic role in response to Russia's war, stopping short of publically aligning with Russia. The Chinese party-state has not offered support for Russia or its actions in the way Iran, North Korea, and Belarus have, but China continues to place value in its partnerships with Russia and has sought to deepen its cooperation over the past year.[3][4] China has issued harsh criticism of US sanctions against Russia and placed blame on the West for its role in the conflict. China has also advocated for a peaceful, diplomatic solution to the war. However, China's imports from Russia expanded substantively in 2022 compared to the year prior, with China's own customs statistics showing over a 30% increase compared to 2021[5], reflecting strengthened energy collaboration in light of Western sanctions against Russia. In January 2023, the US approached China with reports that Chinese state-owned companies sold equipment including flak jackets and helmets to Russia for use in Ukraine, seeking to ascertain whether Beijing was aware. At the time of writing, China has not responded to US inquiries. Since then, the US Treasury's OFAC has sanctioned another Chinese company for providing satellite imagery on Ukraine to Wagner for the purposes of enabling combat operations.

Natural Resource Exploitation Shifts International Reliance Away from Russia

Over the past year, Russia has sought to capitalize on food and energy shortages by using its own resources, and those it could block from Ukraine, as international leverage. While no immediate alternatives have been identified for the grain shortages caused by the war, alternative export routes are being explored, and Russia has signed a grain deal through mid-March 2023 that prevented major price hikes stemming from the conflict. However, Russia largely failed to anticipate the unifying effect its war on Ukraine and subsequent exploitation would have on European nations, who have surged in efforts to shift away from Russian energy supplies. Europe's reinvigorated efforts to distance itself from Russian energy markets will very likely remove a significant power leverage Russia had over Europe for years to come.

Wartime Effects on Food and Energy Exports

Prior to the war, Russia and Ukraine were responsible for substantive food and energy exports used around the world. Together, the countries exported more than 25% of the world's supply of wheat, with Ukraine also serving as a major supplier of key crops like sunflower oil, maize, and barley. Ukraine's ability to harvest crops was almost immediately challenged by Russia's full-scale invasion, and its food exports were similarly hurt as shipping through the Black Sea was brought to a standstill, largely due to Russia's blockade of shipments and suspended shipping activity in light of heightened risk. Russia also stole and smuggled over $500 million USD in Ukrainian grain to ports in Turkey, Syria, and Lebanon in the process, even after attacking farms, grain silos, and shipping ports, in direct sabotage of both Ukraine and the international community.

In 2021, Russia also supplied EU countries with over 40% of their natural gas as the world's largest gas exporter. Following its invasion of Ukraine, Russia struggled to maintain food and energy exports, as bankers, insurers, and shipping lines refused to do business with it and sought alternative suppliers. Countries across the world felt the effects of price hikes as early as April 2022, when the World Bank predicted that food and energy prices would remain high for years to come, partly as a result of the war.

Russia's Attempted Exploitation of Food and Energy Shortages

Following a grain deal Russia signed with Ukraine in July 2022 that enabled Ukraine to export grain through the Black Sea, Russia spent months threatening the international community by claiming it would drop out. In October 2022, Russia actioned its threats by suspending its participation in the deal, resulting in immediate surges in global wheat prices. Russia rejoined the deal shortly thereafter in November and extended it for 120 days despite UN requests for a year-long agreement, likely to ensure it could leverage the threat of abandoning the deal as part of future negotiations. In December, the European Bank for Reconstruction and Development also lent $10 million USD to the Ukrainian government to improve and expand its overland export capacity, which aims to reduce Russian influence on grain flows through ports in the future.

3 https://tass[.]com/politics/1509633
4 https://www.fmprc.gov[.]cn/zyxw/202209/t20220915_10766653.shtml
5 http://stats.customs.gov[.]cn/indexEn

Throughout 2022, Russia similarly attempted to exploit its energy resources as "blackmail" for the West's support of Ukraine, according to European Commission president Ursula von der Leyen. In April 2022, Gazprom suspended gas deliveries to Poland and Bulgaria through the Yamal Pipeline, and similarly halted deliveries to Finland in May 2022 after they refused demands to pay for gas in Russian rubles. Russia continued by reducing supplies to companies in Denmark, Germany, and the Netherlands shortly thereafter. Throughout this period, Russia was also reducing gas supplies through Nord Stream 1, which carries natural gas from Russia to Germany under the Baltic Sea. By early September 2022, Gazprom had completely halted those gas transfers. This led to soaring gas and electricity prices and concern that Europe would have to resort to power rationing and blackouts throughout the winter. Similar to Russia's strategy of targeting Ukrainian infrastructure to damage enemy morale, Moscow very likely hoped to reduce Europe's support for Ukraine with its manipulation of energy markets.

Importantly, Russia has used its resources to coerce and threaten countries even prior to its invasion of Ukraine. Russia has historically exploited Moldova through its occupation of Transnistria, a Moldovan breakaway region, which houses important parts of Moldova's energy infrastructure. Since 1992, Russia's state-owned energy company Gazprom has charged Transnistria's gas bill to Moldova, raising Moldova's current gas debt to $8 billion. Prior to its invasion of Ukraine, Gazprom also threatened Moldova by claiming it would alter gas delivery prices if Moldova continued a trade agreement with the European Union. These threats continued into 2022, when Russia cut natural gas supplies to Moldova to half of previously agreed volumes. In light of Russia's invasion of Ukraine, the West has begun to respond to Russia's exploitation and reduce its ability to pressure countries like Moldova. Romania has started to transport natural gas to Moldova, while the United States' Agency for International Development sent Moldova $30 million in direct aid, "as it responds to unprecedented challenges in the wake of Putin's war against Ukraine".

Beyond Moldova, Europe also sought to decrease its dependence on Russian supplies in light of Russia's threats. Europe shifted its reliance away from Russian gas to liquified natural gas (LNG) imports from Norway and the US, the European Union pledged to phase out its reliance on Russian energy by diversifying gas supplies and speeding up renewable energy, and there are plans to expand additional European LNG storage facilities to avoid energy shortages. Europe and the UK further implemented a crude oil ban for Russian maritime imports after February 2023, and price caps have been established at $60 a barrel by the G7, with both efforts seeking to reduce Russian oil revenues for use in its war against Ukraine. Russia has found alternative buyers for its oil supply throughout this process. Countries like China, India, and Sri Lanka have increased their oil imports from Russia, with deals still in progress for other countries like Pakistan.

Outlook: Concerns for the Days Ahead

Despite Russia's conventional military setbacks and its failure to substantively advance its agenda through cyber operations, Russia maintains its intent to bring Ukraine under Russian control. Reporting indicates that Russia is very likely preparing for a new offensive in Ukraine in the near term, which aligns with its increased targeting of civilian morale over the winter. Russia is also reportedly deploying wiper malware against entities in Ukraine, reminiscent of what was observed before and at the start of the conflict.

Renewed attempts for Russian state-sponsored threat activity groups to target Ukrainian infrastructure through technical means is almost certain in the months to come, and will likely seek to support Russia's conventional military offensive. Russia will also very likely refocus its conventional military forces against smaller geographic objectives, with a likely focus on the Donbas rather than dispersed regions. As of late January 2023, for example, troops appear to be regrouping for an offensive around Donetsk and Luhansk, according to Ukraine's Main Intelligence Directorate.

However, after a year of fighting, Russian troops continue to struggle with many of the problems that plagued them at the beginning of the war: morale among fighters remains low, poor operational security continues to lead to Russian deaths, and soldiers have suffered through winter with poor supplies. Now, troops are also contending with poorly trained fighters augmenting their forces, weapons shortages, and Ukraine's supply of NATO-grade weaponry. Russia will very likely struggle to overcome these challenges in future action against Ukraine, particularly in light of Western reinforcements.

Beyond Russia's anticipated offensive, the protracted nature of this war presents a variety of other challenges for both Ukraine and the international community going forward. The following highlight what we assess to be some of the most dangerous risks in the long term:

- **The risk of full Belarusian participation**. While Russia's anticipated new offensive is likely to focus on Donbas, this will almost certainly just be a step towards the Kremlin's ultimate goal, meaning that Russia will eventually require future military operations to seize control of Ukraine. The Kremlin's collaboration with Belarus illuminates a particularly dangerous scenario in which Russia may seek to formally bring Belarus into its war with Ukraine. In this scenario, Russia and Belarus could stage a joint, coordinated offensive operation from southern Belarus into nearby Ukrainian territories, particularly Kyiv. Such an offensive would likely include Belarusian forces, providing the Kremlin with up to 50,000 additional troops and Soviet-era military equipment that is compatible with Russia's own supply. In the build-up for such an offensive, we would almost certainly observe preparations from Belarus and Russia, such as the establishment of a supply chain to ensure that the troops are provided with the necessary equipment and resources. To date, these indicators have not occurred, indicating that this joint effort is unlikely, at least in the near term.
- **The risk of escalation.** Russia may have intentionally withheld its more advanced cyber capabilities throughout the war, particularly as concern about escalation over cyberattacks entered the forefront of international discussion. On 9 March 2022, NATO Secretary General Jens Stoltenberg affirmed that cyberattacks could potentially trigger Article 5 of the NATO charter (collective defense), meaning that Russian cyberattacks that extended beyond Ukraine's borders could result in NATO intervention. However, the risk of Russia's state-sponsored threat actors expanding its cyber operations beyond Ukraine persists. For example, the West's allocation of advanced tanks to Ukraine in January 2023, including Germany's Leopard 2, resulted in Kremlin statements claiming that Germany and the West were escalating the conflict and insinuating that Russian "red lines" had been violated in the process. This rhetoric repeats Kremlin statements from earlier in the war, and Russia remains unlikely to risk NATO intervention at present, but the ongoing conflict presents continued risks for nations outside of Ukraine.

- **The risk of degraded Ukrainian morale.** The effect of the war on Ukrainian morale is also very likely a key factor in the months to come. Russia has emphasized that it is prepared for a war of attrition against Ukraine, meaning that Russia's renewed offensive would only be a part of the Kremlin's broader strategy in the region, even if it fails. Russia's targeting of Ukrainian morale, as we have seen over the past few months, will almost certainly persist as the war continues. This presents unique challenges to Ukrainian morale, where the war has killed tens of thousands of civilians and leveled cities. Russia's specific attempts to degrade Ukraine's will to fight over winter demonstrate the Kremlin's intent to employ psychological warfare to exhaust its enemy, and Ukraine's ability to remain steadfast will very likely be key to its success.
- **The risk of international complacency.** At present, the West remains largely supportive of Ukraine's struggle against Russia, but Russia's long-term approach to conflicts portends that this war could continue for years. In response, the West's preparedness to continue providing economic support, weapons shipments, and harsh punishments of Russia's actions will almost certainly be critical to the war. In January 2023, US secretary of defense Lloyd J. Austen III spoke at the Ukraine Defense Contract Group and claimed that the group, consisting of the US, Bulgaria, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, and Slovakia, would "support Ukraine against Russian aggression for the long haul". Similarly, British prime minister Rishi Sunak promised Ukraine that it could rely on the UK for long-term support. Despite official governmental support for continued aid to Ukraine, minority groups in the West have called to end military and financial aid to Ukraine. These narratives are amplified by Russian-affiliated propaganda websites that seek to exploit anti-Ukraine narratives in an effort to decrease Western aid for Ukraine.

After a full year, Russia's war has demonstrated much about the country's strategic objectives, capacity, and shortcomings. We have watched the Kremlin demonstrate strategic miscalculations about its military's capability and preparedness, its struggle to overcome cyber challenges in the face of collective defense, and its ability to manipulate European response to the war by exploiting natural resources. We have also watched Russia adapt in an attempt to find victory by focusing on degrading Ukraine's will to fight, relying on its "proxy" forces to bolster its capabilities, and strengthening anti-Western partnerships with countries like Iran and North Korea. With the knowledge that Russia is planning for a protracted war, these insights will prove critical to Ukraine and the international communities standing against Russia's aggression. Putin's acknowledgement of his own failures serves as the starting point for Moscow to remedy its deficiencies, and the steps Russia takes to improve should be closely monitored by the security community going forward to avoid strategic miscalculations of our own.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.