

Targeting the Wagner Group: How the U.S. Can Strengthen Sanctions Against Russia

newamerica.org/future-frontlines/briefs/targeting-wagner-group-us-sanctions/

Brief



Andrey Sayfutdinov/Shutterstock

Feb. 22, 2024

At a Glance

- The Wagner Group and other irregular Russian paramilitaries have generated billions for Russian corporations and state entities by creating a smokescreen that shields the Kremlin's military-industrial complex from scrutiny and accountability.
- Misguided assumptions about the underlying structures and intermediaries that support Russian paramilitary operations have led U.S. sanctions to fall short of their goals and fail to disrupt illicit criminal networks effectively.
- Prominent Russian officials such as Andrey Averyanov and Konstantin Mirzayants, two leading Russian government coordinators of irregular forces, have so far avoided U.S. sanctions as of February 2024.

- To efficiently target Russian paramilitaries, the United States must in real time identify and monitor not only the entities themselves but also the intricate web of individuals, organizations, and activities that constitute a sprawling, Kremlin-directed paramilitary cartel.
- Easy-to-access, comprehensive sanctions data could empower private companies, partner nations, and civil society organizations to contribute to research and compliance efforts.
- Measures to curb the use of illicit finance by Russian irregulars, such as crowdfunding supplies through digital currencies, should be expanded and updated.
- Absent dedicated efforts to coordinate information collection and data sharing within the U.S. government, among allied U.S. partner nations, and with other public interest stakeholders, there is a strong risk of yet more policy missteps and missed opportunities to disrupt the illicit operations of Russia's paramilitary networks.

Beyond Wagner: Decoupling Behavior from Brand

By the time he plunged to his death in a plane crash in August 2023, Wagner Group chieftain Yevgeny Prigozhin was one of the most heavily sanctioned individuals in the world. From 2016 to 2023, the Wagner Group was the target of four U.S. sanctions regimes. Sanctions targeting gradually improved in accuracy as Russia expanded its influence in Africa, while the tempo of sanctions ramped up considerably after Russia launched its full-scale invasion of Ukraine in February 2022. On the whole, however, U.S. sanctions against Prigozhin and the Wagner Group were at best haphazard.

Efforts to identify and strike the right targets often fell wide of the mark because of inaccurate assumptions about the characteristics of Russia's irregular paramilitary forces and insufficient information collection about the Wagner Group's command and control structures, Kremlin decision-making processes, and the Russian policies and laws that enabled Wagner operations. Those failures can be attributed, in part, to an over-focus on the information warfare aspects of Prigozhin's business ventures instead of the military operations that contributed to widespread atrocities in multiple countries.

Preoccupation with headline-grabbing personalities like Prigozhin rather than the Kremlin's policies and practices ended up diverting attention away from central elements of Russia's military-industrial complex, such as the Main Operations Directorate (ГООУ ГШ ВС РФ) of Russia's General Staff, the Military-Industrial Commission, and the security and logistics divisions of Russian energy, weapons, and mining conglomerates, all of which made the Wagner Group's operations possible. Intermediary brokers who facilitated the extraction, transport, refinement, operational financing, and trade of the Russian defense ministry's ill-gotten gains from the exploitation of gold, gems, oil, and timber, meanwhile, often escaped scrutiny and remained virtually unscathed.

While Russia has continued its strategy of using off-book fighters for resource extraction, force mobilization, and co-optation of security forces in client states in Africa and the Middle East, the Kremlin has also taken steps to shuffle the deck by subordinating irregular groups via contracts with state security agencies and the creation of alternate paramilitary forces such as Russia's new Africa Corps. The Main Operations Directorate is restructuring its international operations and laying the groundwork for a more robust Russian military presence in Africa by replacing irregular paramilitaries with conventional Russian forces. At the same time, competitors and successors are vying for control of Prigozhin's business empire amid a concerted shift. Without dedicated efforts to coordinate information

collection and data sharing within the U.S. government, among allied U.S. partner nations, and with other public interest stakeholders, there is a high risk of further policy missteps and missed opportunities to disrupt Russia's paramilitary operations.

Especially while Russia's war in Ukraine persists, Russia's use of irregular forces will remain fluid. The United States and its allies must adapt accordingly. U.S. national security agencies must act more quickly to counter the Kremlin's efforts to circumvent sanctions and embargoes to ensure that sanctions hit the right targets, in the right place, at the right time—making them a stick to be feared rather than sidestepped. The United States must proactively address the limitations of its policy approaches. An exclusively government-driven effort to disrupt the illicit networks that fuel transnational criminal organizations like the Wagner Group and related irregular formations is unlikely to change much. Greater emphasis should be placed on information sharing among public interest stakeholders seeking to bring the networks that support Russian irregulars like the Wagner Group, Redut, Rusich, and Convoy to account. Unless and until the state-controlled apparatus that backs the Kremlin's paramilitary cartels is disrupted, Russia's irregular formations will continue to operate freely under one name or another. It is the behavior, not the brand, that the United States, Europe, and allied nations should be focused on when it comes to curbing Russian irregulars and their intermediaries.

Time Lags and Missed Opportunities

Sanctions are not a quick fix. They require careful consideration and accurate information to be effective, and they more often have the most impact when they are fitted for the purposes of disruption rather than deterrence. U.S. government sanctions against Prigozhin and his beneficial holdings became more targeted and effective over time, showing a growing understanding of the corporate and state structures that undergird the Wagner Group. But the U.S. Treasury and State Departments, as well as U.S. allies, were often stuck playing catch-up and whack-a-mole while the Wagner Group's growth outstripped expectations and increasingly became a go-to tool of Russian statecraft.

In December 2016, two years after Russia invaded and annexed Crimea, the United States and its allies began sanctioning Prigozhin and his companies. The Treasury Department's Office of Foreign Assets Control (OFAC) designated Prigozhin under Executive Order 13661 for providing "financial, material, or technological support for, or goods or services in support of, senior officials of the Russian Federation." The measures aimed to inhibit financial flows to Prigozhin and Wagner Group-related entities due to the paramilitary's operations in eastern Ukraine from 2014 to 2015.

By then, however, Wagner had moved on to other ventures: The Kremlin had already introduced the Wagner model of security assistance in exchange for resource extraction to a growing number of Russian partner states in Africa and the Middle East. Starting in September 2015, Wagner had expanded from Ukraine to Syria—supporting Bashar al-Assad's regime against anti-government militants, including the Islamic State—where Wagner fully developed its trademark fusion of military force and resource exploitation. Wagner assault detachments captured oil and gas infrastructure, from which Prigozhin's Evro Polis company extracted millions in revenue, operating the al-Shaer oil field with an annual revenue of \$301 million from 2016 until at least 2017.

In June 2017, Treasury specifically targeted two companies linked to Prigozhin—Concord Catering and Concord Management and Consulting—as well as the private military company Wagner, for “actions or policies that threaten the peace, security, stability, sovereignty, or territorial integrity of Ukraine.” Yet, as Prigozhin’s attorneys would later point out in multiple court filings and pre-trial hearings related to Concord’s financing of the Internet Research Agency, Concord Catering was more brand than company, leaving core operational elements of the Wagner network unaffected.

It took the United States until 2018 to sanction Evro Polis, the primary contracting company behind Russian paramilitary operations in Syria. Three other front companies—Kollektiv Servis, M-Invest, and M-Finans—soon supplanted Evro Polis as the primary engines of the Wagner Group’s operational network. All held multiple contracts through Voentorg, the logistics arm of the Russian defense ministry’s service supply conglomerate, Garnizon JSC. Yet, Voentorg and Garnizon received little scrutiny and remained untouched by sanctions until 2022. Prigozhin, accordingly, was able to expand the outfit’s combination of combat-for-hire and resource extraction to Sudan in 2017 and the Central African Republic and Libya in 2018.

As the U.S. government became increasingly aware of the scale of the Wagner Group’s global operations, it enacted a more comprehensive sanctions package in the summer of 2020, which targeted Wagner Group-related entities and individuals operating in Sudan and the Central African Republic. However, it took Russia’s full-scale invasion of Ukraine in February 2022 to prompt a surge in the use of sanctions to limit the Wagner Group’s operational capabilities. From February 2022 until January 2023, the U.S. Departments of the Treasury, State, and Commerce implemented three distinct sanctions packages to restrict Wagner’s purchasing and operational abilities, extending them to lesser-known companies associated with Wagner.

Russia’s full-scale invasion also led the U.S. government to unlock new punitive measures. A December 2022 modification to the Foreign Direct Product Rule, for example, limited the Wagner Group’s access to U.S. technology worldwide by requiring exporters to apply for a license for any transaction that involves or would knowingly benefit the Wagner Group. Calculated to impose “severe restrictions on the Wagner Group’s ability to acquire items globally to support the Russian government’s unprovoked war in Ukraine,” the enforcement action came one month after Prigozhin acquired access to Chinese satellites for battlefield intelligence. The extended rule may also have an impact on Wagner-affiliated businesses engaged in mining and logging, which often require commercial equipment subject to the Foreign Direct Product Rule.

In January 2023, Treasury escalated further by designating the Wagner Group as a transnational criminal organization (TCO), stating that “Wagner personnel have engaged in an ongoing pattern of serious criminal activity, including mass executions, rape, child abductions, and physical abuse in the Central African Republic (CAR) and Mali.” The move significantly empowered federal agencies to pursue criminal activities perpetrated by Wagner. The TCO designation could also encourage countries hesitant to collaborate with the United States on sanctions related to the Ukraine war to engage in joint efforts specifically focused on criminal sanctions and potentially even prosecutions for illicit activity. The designation showed an improved understanding of the Wagner network, targeting lesser-known companies such as Joint Stock Company Terra Tech, which supplied satellite images of Ukraine, and

Wagner Group front companies in the Central African Republic, such as Sewa Security Services. Additional sanctions in 2023 targeted Ivan Maslov, the head of the Wagner Group in Mali, and the network's gold-running operations.

Yet, despite these enforcement efforts, there are signs that the United States is once again lagging in its response. Since the Wagner Group's brief mutiny in June 2023, the Kremlin has aimed to alleviate uncertainty among its security partners in Africa by dispatching regular delegations of high-ranking defense and intelligence officials. Noteworthy figures among them include Deputy Defense Minister General Yunus-bek Yevkurov, deputy chief of Russia's military intelligence agency Andrey Averyanov, and Konstantin Mirzayants, a key figure in the Redut PMC recruiting network. As of February 2024, neither Averyanov nor Mirzayants have been subjected to U.S. sanctions, despite their highly visible roles in establishing the Africa Corps to replace the Wagner Group's Africa operations. Although Yevkurov has been under U.S. sanctions since March 2022, he and others in the Main Operations Directorate supervised the implementation of operational plans for Russian irregular paramilitaries deployed as part of train-and-equip missions to the Middle East and Africa.

Transnational Extremist Threats and Digital Dodges

If the U.S. sanctions against entities and individuals associated with the Wagner Group have been haphazard and lagged behind the group's growth, this pattern was even more pronounced for other related irregular Russian formations. Only in 2022 did Treasury's OFAC sanction the leaders of the Sabotage Assault Reconnaissance Group Rusich (DSHRG Rusich), an irregular formation with close ties to the Wagner Group and a history of military operations in Ukraine dating back to 2014. Likewise, the Russian Imperial Movement (RIM), a St. Petersburg-based ultranationalist organization that has been training fighters for the war in Ukraine since the beginning of the conflict, only faced sanction in 2020, when the U.S. State Department labeled RIM Specially Designated Global Terrorists. Although this is a historic move—the first of its kind for a white supremacist organization—it did not name RIM leaders outside the top leadership. Key RIM supporters, such as Stanislav Shevchuk and Alexander Zhuchkovsky, did not face sanctions until 2022. As of January 2024, members of both Rusich and RIM just below the top ranks have not been included in the sanctions list.

Both RIM and Rusich are known for cultivating international ties and, in some cases, sharing expertise and resources with allies outside Russia. Shevchuk, for example, met with American white nationalist and Unite the Right organizer Matthew Heimbach in 2017; the pair posed for photos in front of the White House. In 2016–17, members of the far-right group Nordic Resistance Movement bombed a cafe and migrant center in Sweden after receiving training at RIM's St. Petersburg facility. When Rusich began to crowdfund supplies with cryptocurrency in 2022, their wallets received hundreds of donations, including from exchanges like Coinbase that restricted Russian users from their services at the time of the transaction, implying that these donations came from outside the Russian Federation. These incidents highlight Russian paramilitary groups' global reach and transnational networking strategy, which predates U.S. sanctions by years.



Russian Imperial Movement leaders Stanislav Shevchuk (left), Denis Gariyev (second from right), and Stanislav Vorobyev (right) meet with Manuel Andrino Lobo (second from left), head of Spain's far-right La Falange group, in 2015.

Source: VKontakte/VOA



Stanislav Shevchuk (right) poses with Unite the Right organizer Matthew Heimbach (left) outside the White House in 2017.

Source: ThinkProgress

Rusich's cryptocurrency experiments began after the United States and its allies blocked several major Russian banks' access to SWIFT, the secure financial messaging service, on March 1, 2022. The loss of access to SWIFT, which facilitates international bank-to-bank transfers, significantly hampered financial flows into Russia from abroad. Within weeks, Rusich-linked Telegram accounts began advertising cryptocurrency addresses with the message, "For those who want to support Russian warriors from abroad, we have opened a BTC crypto wallet!" TRM Labs, a blockchain intelligence firm, estimated that by September 2022, the group had raised more than \$144,000 in cryptocurrency. Rusich regularly boasts about their success in crowdfunding essential equipment such as sidearm harnesses, quikclot packets, and medikits, as well as drones, scopes, and ammunition.

Rusich also raises funds through hacking and other forms of illicit finance. In November 2022, for example, the independent news outlet *Meduza* reported that Rusich had inserted one of its Bitcoin donation addresses into the Ukrainian charity site Happy New Life. On Telegram, Rusich confirmed *Meduza's* reporting and claimed to have internal units dedicated to "operations related to cryptocurrencies, precious stones, money laundering [...] and collection, including frequent business trips to interested large sponsors from among shadow businessmen." While Rusich's claims should be viewed with skepticism, on-chain analysis reveals that Rusich-linked cryptocurrency wallets have indeed received substantial sums. For example, a single address that several Rusich-linked accounts promoted in spring 2022 received the equivalent of \$46,500 in Bitcoin (at February 2024 valuations) over a three-month period.

In response, the Treasury Department sanctioned several cryptocurrency addresses associated with Rusich in September 2022. However, the five addresses in OFAC's database represent only a few Rusich-linked addresses with some of the smallest amounts of transacted cryptocurrency, totaling less than \$17,000 at February 2024 prices. This falls short of the amounts Rusich claims to have received on Telegram—one recent post claimed that a single collection had raised 1,750,000 rubles, equivalent to approximately \$19,000—as well as the verifiable volume that has flowed through Rusich-linked cryptocurrency addresses. Furthermore, blockchain analysis reveals that funds frequently pass through a series of wallets before being converted to fiat currency, a practice intended to obscure and complicate transactions. In short, OFAC appears to have largely missed its mark with cryptocurrency addresses associated with Rusich and Rusich-linked individuals. While the group has moved away from cryptocurrency solicitations in recent months, they could easily resume their efforts with new addresses, sidestepping existing designations.

Picking Targets

A scattershot and reactive application of economic sanctions can have unforeseen consequences. In 2018, the State Department published a hastily gathered list that included many of Russia's most powerful politicians and oligarchs. This list, a requirement of 2017's Countering America's Adversaries Through Sanctions Act (CAATSA), directly informed a package of sanctions that the Treasury Department released a few months later. Among those targeted was aluminum tycoon Oleg Deripaska, a longtime associate of Vladimir Putin who has been tied to several irregular military formations as well as Russia's interference in the 2016 U.S. presidential election. As detailed in Agathe Demarais's *Backfire: How Sanctions Reshape the World Against U.S. Interests*, Deripaska's designation wreaked havoc in world aluminum markets and led to a legal tussle between Deripaska and U.S. officials that reached the Supreme Court. Deripaska filed an appeal requesting that his designation be removed, claiming that the Treasury Department exceeded its authority. The Supreme Court dismissed the case in October 2022.

To minimize these sorts of knock-on effects, the Biden administration implemented measures such as temporary and partial waivers for sanctions on countries like Syria, which suffered a devastating earthquake in early 2023, and Iran, which supplies Iraq with a significant amount of electricity. Yet many in Washington seem to be torn between these more nuanced actions and a desire to grab the biggest hammer available—such as by calling to designate the Wagner Group as a terrorist organization.

A terrorist designation in this instance is not only reactive and unproductive, it risks blunting the sharpest weapon the West has in its arsenal: transparency. The U.S. Global War on Terror precipitated an unprecedented wave of overclassification of information about terrorist groups like al-Qaeda and their intermediaries. As noted in the 9/11 Commission report, high levels of secrecy led to blind spots, information hoarding, and siloing of information, all of which ultimately contributed to the thick fog that preceded the 2001 attacks on the World Trade Towers and the Pentagon.

Following the United Kingdom in designating the Wagner Group a terrorist organization would be the wrong call for several reasons. First and foremost, it confuses what the Wagner Group is and buys into the narrative that the group is primarily a private unitary organization rather than a networked covert arm of the Russian state. The Wagner Group has never been an independent actor—Putin himself said as

much after the Wagner mutiny. While the paramilitary's patterns of financing, smuggling, and human rights violations might resemble those of a transnational terrorist organization, the group undertakes these activities at the Kremlin's direction and for the benefit of the Russian state, which raises substantial questions about command responsibility and criminal liability for Russian government officials for breaches of the law of armed conflict.

Second, adding Wagner to the terrorist list would complicate the ability of the United States to interact with any government or private entity that has also done business with the group, further entrenching countries like Mali and the Central African Republic in their anti-Western orientation. Lastly, as we have seen since Prigozhin's death in August 2023, it is relatively simple for the Kremlin to stand up new versions of the Wagner Group paramilitary model that fulfill the same strategic aims and, often, involve the same cast of characters.

Instead, Washington should pursue a proactive, well-targeted sanctions approach with appropriate carve outs for humanitarian or strategic considerations. Doing so relies on accurate information about Russian irregulars and their relationship to the Kremlin—which the Kremlin does its best to obscure—and discarding the assumption that Russian irregulars roughly parallel the role of private military companies like Bancroft Global Development in the United States.

Since payments and profits rely on unique barter arrangements between Russia and its client states, it would be more accurate to treat Russian irregulars like the Wagner Group as a cartel that engages frequently in criminal conspiracies to achieve its ends and in which key Kremlin insiders and individuals close to Putin have a beneficial stake. It is critical for the United States to identify the network of government officials, military units, and businesses that support Russian irregular paramilitaries. Otherwise, the names and brands will change, but the networks, individuals, and behaviors will remain the same.

Sharpening Compliance and Making Sanctions Bite

When it comes to Russian irregulars such as the Wagner Group, Redut, Rusich, and Convoy, there are many moving targets, and the situation will remain fluid as Russia continues to wage its war of aggression in Ukraine. It is unlikely, therefore, that the U.S. government alone will consistently be able to apply the kind of resources and attention necessary to disrupt the operations of Russian irregulars. Encouraging regular information exchanges between U.S. allies and public interest stakeholders and selective declassification of data could serve as a force multiplier in the effort to drive forward accountability. Improving publicly available sanctions data would be a significant step in the right direction, facilitating compliance for businesses while also providing civil society watchdogs and investigators with critical research tools.

If the goal is to provide U.S. companies such as banks, credit card companies, and wire transfer services with the information they need to comply with U.S. sanctions easily and effectively, then the publicly available data from government sources is woefully inadequate. The Treasury Department offers several options for searching for sanctions. Their online search tool is rudimentary and identifies whether a company or individual has faced sanctions, but otherwise provides limited information about associated entities and the reason for the designation. Treasury also makes their sanctions lists

available in a variety of downloadable data formats. Their press releases give details about sanctioned individuals, companies, and the rationale behind the sanctions, but in a comparatively unstructured format.

In addition, U.S. companies carry the burden of determining whether their transaction partner is a sanctioned entity under OFAC's 50 percent rule, which specifies that companies that are owned more than 50 percent by a sanctioned entity automatically face the same sanctions. The complexity of identifying companies' ownership structures often leads large businesses to rely on costly external services.

A well-designed and comprehensive public database with stronger search functionality could enhance coordination for better enforcement and allow businesses seeking to avoid dealing with sanctioned entities to quickly and efficiently identify them, including those under the 50 percent rule. Moreover, a revamped public platform could operate as a portal, granting access to independent, non-governmental public interest investigators. Such access could extend to data regarding the underlying information and rationale behind sanction designations, which often remain opaque due to overclassification.

While sources and methods are often understandably sensitive, there are good grounds to consider whether and when it makes sense to share information or provide access to public interest stakeholders such as journalists, academics, human rights organizations, and international NGOs that may be able to shade in gray areas and triangulate transnational network connections. In short, an improved, interconnected, and well-designed data portal, combined with a continuous classification review process and the publication of background data on sanctions targets, could significantly contribute to the long-term effectiveness of sanctions.

There has been progress. The Biden administration, as part of its Strategy on Countering Corruption, has prioritized curbing illicit financial flows. Recent announcements include compelling companies operating in the United States to report information about their beneficial owners—the individuals who ultimately own or control them. Looking ahead, the administration plans to introduce new rules in 2024 aimed at blocking designated entities from laundering money through U.S. real estate. Furthermore, investment advisors will be required to implement new regulations designed to combat illicit finance.

Honing Strategies with Data

An analysis of the sanctioning of Prigozhin's corporate holdings, assets, and entities associated with the Wagner Group's operations over the past decade offers lessons for how to sharpen the bite of diplomatic and financial tools and contain the destabilizing effects of Russia's irregular forces. To shed light on how the U.S. government has utilized sanctions to curtail the capabilities of Russian irregular groups and how these measures have evolved over time, New America's Future Frontlines team compiled a dataset of U.S. sanctions targeting individuals and entities linked to Russian irregulars and the larger military-industrial machine that enables and controls them behind the scenes.

Russian Targets of U.S. Sanctions, 2014 to 2023

Irregular formations are just one facet of a vast military-industrial complex designed to bolster Putin's government against international and domestic challenges. Our dataset includes sanctions related to Russia's military-industrial complex, strategic-extractive sector, and finance sector. This broader net

reflects the reality of Russia's use of supposedly private, volunteer, and contract combat units—typically organized through state-owned companies in the extractive and logistics sectors or through seemingly independent oligarchs, giving the Kremlin a degree of separation from operational activities. This web of connections extends beyond the regular military hierarchy, intertwining with powerful economic entities that finance and facilitate Russia's strategic endeavors.

This dataset includes all relevant executive orders, acts, regulations, and directives issued by the U.S. government to sanction Russian entities involved in the Ukraine war between January 1, 2014, and January 31, 2023, including the Countering America's Adversaries Through Sanctions Act (CAATSA) of 2017. To ensure accuracy, the dataset relies exclusively on official U.S. government sources, drawing from Treasury Department press releases, information from the Department of State, data from the Department of Commerce's Bureau of Industry and Security, and archived documents in the Federal Register. Given the limitations of Treasury's search tool, our dataset is predominantly built around their press releases, which required researchers to extract and structure important information by hand and significantly increased the time needed to understand the myriad of sanctions applied to Russian entities. The dataset does not include any non-U.S. sanctions, such as those that the Council of Europe imposed in 2021 on select Wagner Group commanders and companies.

Challenges and Opportunities

While the U.S. government has consistently imposed new sanctions on Russian irregular groups and the defense sector, staying current with pertinent individuals and companies has proven challenging. Yevgeny Prigozhin, strategically placed at the forefront of U.S. sanctions, created a smokescreen that drew attention and punitive action from the West, allowing the Kremlin to conceal the many other entities, particularly state-owned enterprises, that benefit from Russia's expanding operations in Africa and the Middle East. In the wake of Prigozhin's death, the Kremlin has shifted its use of off-book irregulars to other organizations, while the U.S. response has been slow and incomplete. This delay is rooted in the deeply ingrained assumption that formations such as the Wagner Group are private entities, which hinders efforts to identify key nodes in the Kremlin's operation of irregular forces. Russian law, policy, and practice all indicate that these groups operate as extensions of the state. Until officials treat them as such, new iterations of the same strategy, with fresh branding, will continue to emerge.

Moreover, the government's focus on Wagner has allowed individuals affiliated with less well-known groups such as Rusich and the Russian Imperial Movement to escape the same degree of scrutiny. Although these organizations and their senior leaders faced sanctions and other punitive measures, these rarely extended to affiliated companies or direct supporters of the senior leaders, perpetuating the cycle of evasion. The limitations of publicly available data on U.S. sanctions put the burden of compliance on private companies, which can lead to unsatisfactory results. Better structured data would enable companies, allies, and researchers to track U.S. sanctions more effectively and accurately, resulting in a more efficient sanctions regime.

Russia's military brass and spymasters have proven adept at conjuring up phantoms for the West to chase while quietly carrying out the strategic work of forging new international relationships and extracting lucre for sanctions resilience. Vigilantly monitoring this evolving scheme will be critical for understanding the networks that support Russian irregular groups and limiting their capabilities through

proactive and informed enforcement. Washington must avoid the trap of relentlessly pursuing the latest ghost organization set up for precisely that purpose, instead targeting the model's architects and support network.