DFRLab

#ACcyber

CYBER STATECRAFT
INITIATIVE

ISSUE BRIEF

JULY 2022

Hackers, Hoodies, and Helmets:
Technology and the Changing Face of Russian Private Military Contractors

EMMA SCHROEDER, GAVIN WILDE, JUSTIN SHERMAN, AND TREY HERR

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security

INTRODUCTION

The *first* time Russia invaded Ukraine in the twenty-first century, the Wagner Group was born. The now widely profiled private military company (PMC) played an important role in exercising Russian national power over the Crimea and portions of the Donbas—while giving Moscow a semblance of plausible deniability. In the near decade since, the Russian PMC sector has grown considerably, and is active in more than a dozen countries around the world. PMCs are paramilitary organizations established and run as private companies—though they often operate in contract with one or more states. They are profit-motivated, expeditionary groups that make a business of the conduct of war.[1] PMCs are in no way a uniquely Russian phenomenon, yet the expanding footprint of Russian PMCs and their links to state interests call for a particularly Russian-focused analysis of the industry. The growth of these firms and their direct links to the Kremlin's oligarch network as well as Moscow's foreign media, industrial, and cyber activities present a challenge to the United States and its allies as they seek to counter Russian malicious activities abroad.

As signals intelligence and offensive cyber capabilities, drones and counter-drone systems, and encrypted communications become more accessible, these technologies will prove ever more decisive to both battlefield outcomes and statecraft. More exhaustive research on these issues is necessary. The ongoing conflict resulting from Russia's second invasion of Ukraine in this young century seems likely to shape the conduct of Russian foreign policy and security behavior for years to come—and these firms will play a part.

The activities of these PMCs include high-intensity combat operations, as evidenced in Syria in 2018 and Ukraine in 2022, and a mix of population control, escort and close protection, and local direct-action activities, as seen

1 Sean McFate, *Mercenaries and Privatized Warfare Current Trends and Developments*, Office of the United Nations High Commissioner for Human Rights (OHCHR), April 24, 2020, https://www.ohchr.org/sites/default/files/Documents/issues/Mercenaries/WG/OtherStakeholders/sean-mcfate-submission.pdf.

in Libya, Mali, and elsewhere.[2] Given the sourcing and dependence of Russian PMCs on Russian military service personnel and no small influence of Russian doctrine, the questions to reasonably ask include: How do changes in the Russian conduct of war and adoption of new technologies influence these PMCs? Moreover, how might these technological changes influence the role these PMCs play in Russian strategic goals and activity abroad? The accelerating frequency of PMCs found operating around the world and the proliferation of private hacking, surveillance, and social media manipulation tools suggest that Russian PMCs will pose diverse policy challenges to the United States and allies going forward. This issue brief seeks to offer an initial expoloration of these questions in the context of how these PMCs came about and how they are employed today. The section below addresses the origin and operations of PMCs in Russian international security strategy, and also profiles the changing role of technology in conflict and the activities of the changing roles of PMCs. The last section closes with a set of open research questions.

PMCS IN RUSSIAN INTERNATIONAL SECURITY STRATEGY AND THE INFLUENCE OF TECHNOLOGY

Historically, Moscow has benefited from using mercenaries to advance its aims abroad. Imperial Russia extensively deployed Cossack brigades in the Napoleonic wars and, domestically, to quell peasant uprisings. Tsar Aleksandr II used them as a tool to balance pan-Slavic fervor against the imperial policy of nonintervention in the burgeoning Balkan-Ottoman conflict of the 1870s.[3] Joseph Stalin rallied sympathetic brigades in support of the Republican faction in the late 1930s Spanish Civil War.[4] More recent conflicts demonstrate the abiding imperatives which make PMCs an attractive tool of Russian statecraft.

The number and prevalence of Russian PMCs as a turnkey model deployed in service of Moscow's niche foreign objectives have increased over the past decade. Russian PMCs provide the Russian government and, if applicable, their overseas clients (foreign governments and/or companies) with a range of capabilities to augment or mimic Russian military and intelligence activity. This includes training foreign armed forces and groups, providing armed security/protection, conducting "political warfare" (from assassinations to running drones), and performing military-style functions. It also potentially includes surveillance and cyber(ed) activities that could be reliant on industry capabilities or further built out in the future. Moscow exercises control and provides support for these capabilities to varying degrees, and each of these capabilities feeds into benefits for the PMCs and for the oligarchs at their helm.

Training Military Forces Abroad

Russian PMCs train foreign armed forces and groups. In the early 1990s, for instance, Rubikon, a security firm based in St. Petersburg and "supervised by Russian security services," helped organize volunteers to fight for the Serbs in then-Yugoslavia.[5] This trend has continued through to recent times, with Russia's Vladimir Putin even publicly stating in 2012 that Russian private military companies could be used to train foreign military personnel.[6] Recently, it appears that Russian private PMC ENOT Corp has run "military-type training camps for right-wing activists from foreign countries."[7] Russian PMCs in Libya have trained Libyan National Army (LNA) forces and even repaired their military equipment.[8] And a July 2021 assessment from the US Office of the Director of National Intelligence found that some "Russian private paramilitary groups" that are "trying to recruit and train Western RMVEs [racially and ethnically motivated violent extremists] to expand their reach into the West, increase membership, and raise money."[9]

These organizations also provide armed security/protection to government, corporate, and individual clients. Indeed, part of the Russian PMC industry outgrowth stems from the chaos

2 Ministry of Defence (@DefenceHQ), "Latest Defence Intelligence update on the situation in Ukraine - 18 July 2022," Twitter, July 18, 2022, 2:12 a.m., https://twitter.com/DefenceHQ/status/1548913656410226688; Ruslan Trad, "Wagner Group Continues Involvement in Russian Operations in Eastern Ukraine," Digital Forensic Research Lab (DFRLab), July 8, 2022, https://medium.com/dfrlab/wagner-group-continues-involvement-in-russian-operations-in-eastern-ukraine-4c1c9b07e954; "Russian Troops Ill-Prepared for Ukraine War, Says Ex-Kremlin Mercenary," Reuters, May 12, 2022, https://www.reuters.com/world/us/russian-troops-ill-prepared-ukraine-war-says-ex-kremlin-mercenary-2022-05-10/; Miriam Berger, "What Is the Wagner Group, The Russian Mercenary Entity in Ukraine?" Washington Post, April 9, 2022, https:// www.washingtonpost.com/world/2022/04/09/wagner-group-russia-uraine-mercenaries/; Thomas Gibbons-Neff, "How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," New York Times, May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html; Ilya Barabanov and Nader Ibrahim, "Wagner: Scale of Russian Mercenary Mission in Libya Exposed," BBC News, August 11, 2021, https://www.bbc.com/news/world-africa-58009514; and Jason Burke and Emmanuel Akinwotu, "Russian Mercenaries Linked to Civilian Massacres in Mali," Guardian (US edition), May 4, 2022, https://www.theguardian.com/world/2022/may/04/russian-mercenaries-wagner-group-linked-to-civilian-massacres-in-mali.

3 Alexis Heraclides and Ada Dialla, "The Balkan Crisis of 1875–78 and Russia: Between Humanitarianism and Pragmatism," in *Humanitarian Intervention in the Long Nineteenth Century: Setting the Precedent* (United Kingdom: Manchester University Press, 2015), 173, https://www.jstor.org/stable/j.ctt1mf71b8.14?seq=5.

4 Matthew Wills, "The International Brigades," *JSTOR Daily* (online magazine), JSTOR (digital library), April 20, 2022, https://daily.jstor.org/the-international-brigades/.

5 Tor Bukkvoll and Åse Gilje Østensen, *"The Emergence of Russian Private Military Companies: A New Tool of Clandestine Warfare*, Norwegian Defense Research Establishment, 2020, 3, https://publications.ffi.no/nb/item/asset/dspace:6751/1811576.pdf.

6 András Rácz, "Band of Brothers: The Wagner Group and the Russian State," Center for Strategic and International Studies (blog), September 21, 2020, https://www.csis.org/blogs/post-soviet-post/band-brothers-wagner-group-and-russian-state.

7 Bukkvoll and Østensen, *The Emergence of Russian Private Military Companies*, 14.

8 R. Kim Cragin and Lachlan MacKenzie, "*Russia's Escalating Use of Private Military Companies in Africa*," *Strategic Insights*, Institute for National Strategic Studies, November 24, 2020, https://inss.ndu.edu/Media/News/Article/2425797/russias-escalating-use-of-private-militarycompanies-in-africa/.

9 US Office of the Director of National Intelligence, *Russian Federation Support of Racially and Ethnically Motivated Violent Extremists*, Office of the Director of National Intelligence, July 2021, https://www.scribd.com/document/558091662/ODNI-Report-Russian-Federation-Support-of-Racially-and-Ethnically-Motivated-Violent-Extremists#fullscreen&from_embed. Published as part of: Zach Dorfman and Jana Winter, "U.S. Intelligence Report Details 'Indirect' Russian Government Support for Western Neofascist Groups," Yahoo! News, February 10, 2022, https://news.yahoo.com/us-intelligence-report-details-indirect-russian-government-support-for-western-neo-fascist-groups-233831082.html.

in the post-Soviet period of the 1990s, when former Soviet soldiers, intelligence personnel, and other members of the security apparatus formed companies to provide security for businesses.[10] In the early days of Gazprom, Rosatom, Rosneft, and Russian Railways—all state-owned enterprises—Russian PMCs protected their assets overseas.[11] Years later, then-Prime Minister Putin noted that PMCs could act as extensions of Russian influence in conducting such protection operations at important facilities abroad, outside of Russian enterprises.[12] Russian PMCs have provided protective services in the Central African Republic,[13] in Mali,[14] and to energy fields in Syria,[15] in addition to other countries.

The Wagner Group deployed to Mali in December 2021, following the withdrawal of French forces from the country, to train the Malian Armed Forces (FAMa) and provide protection for senior officials. At the time, the French government attempted to stop the reportedly $10.8 million deal, but the Malian government defended the prospect of closer cooperation with Russia.[16] Immediately upon the Wagner Group's arrival, it began to construct a base near a Malian air force installation at Bamako's Modibo Keita International Airport.[17] FAMa, according to a Mali army spokesperson, "had new acquisitions of planes and equipment from [the Russians] . . . It costs a lot less to train us on site than for us to go over there."[18] Less than a month after the Wagner Group's arrival, French reporting indicated that at least one Wagner member was injured when a FAMa convoy was attacked in the center of the country—where insurgents ambushed the convoy and employed an improvised explosive device against one of the armored vehicles, leading to a firefight.[19] Though the Wagner Group's mission in Mali is training local forces for direct combat, not engaging in it itself, the mission is clearly one that requires it to work in parallel with local forces and thus consistently places Wagner forces in combat situations.

Resource Security

While the Kremlin realizes strategic benefits from PMC operations worldwide, the PMCs themselves and PMC proprietors, often members of Putin's inner circle of oligarchs, reap financial windfalls. Through opaque ownership structures and cutouts, the model essentially provides paramilitary muscle and political support in exchange for preferential access to—if not control over—mineral rights and other sources of rent extraction for Moscow and its oligarch class.[20] Particularly in areas where the main sources of Russian economic might—arms and energy—are already prevalent like in Syria, PMCs act as a force multiplier and reinforce Moscow as an indispensable partner for regime stability. For instance, in Africa—where Russian arms comprise half the continent's market, and Moscow looks to invest big in oil, gas, and nuclear projects—PMCs act as an insurance policy.[21]

In the Central African Republic, the Wagner Group has been used to bolster support for President Faustin-Archange Touadéra's government—training local soldiers, protecting leaders, and providing security services at the country's diamond mines—following the exit of French peacekeeping forces in 2017.[22] Yevgeniy Prigozhin, the Russian oligarch known as "Putin's Chef," runs the Wagner Group,[23] a military force that is neither a single entity nor truly private or independent. The group also has close ties with the GRU[24] and its direction appears dictated by the state, which aids in the procurement of contracts internationally. The group is funded partially through Prigozhin, but Wagner also receives direct

10 Andrew S. Bowen, "Russian Private Military Companies (PMCs)," In Focus (series), US Congressional Research Service, September 16, 2020, 1, https://sgp.fas.org/crs/row/IF11650.pdf.

11 Asymmetric Warfare Group Study, *Russian Private Military Companies: Their Use and How to Consider Them in Operations, Competition, and Conflict* (Fort Eustis: US Army, October 2020), 13.

12 Rácz, "Band of Brothers."

13 Raphael Parens, *The Wagner Group's Playbook in Africa: Mali*, Foreign Policy Research Institute, March 2022, 6, https://www.fpri.org/article/2022/03/the-wagner-groups-playbook-in-africa-mali/.

14 Parens, *The Wagner Group's Playbook in Africa*, 9.

15 Swedish Defence Research Agency (FOI), "Russia's (Not So) Private Military Companies," FOI Memo 6653, January 2019, 2, https://www.foi.se/rest-api/report/FOI%20MEMO%206653.

16 John Irish and David Lewis, "Exclusive: Deal Allowing Russian Mercenaries into Mali Is Close–Sources," Reuters, September 13, 2021, https://www.reuters.com/world/africa/exclusive-deal-allowing-russian-mercenaries-into-mali-is-close-sources-2021-09-13/.

17 Jared Thompson, Catrina Doxsee, and Joseph Bermudez, "Tracking the Arrival of Russia's Wagner Group in Mali," Commentary, Center for Strategic and International Studies (CSIS), February 2, 2022, https://www.csis.org/analysis/tracking-arrival-russias-wagner-group-mali.

18 "Russian Troops Deploy to Timbuktu in Mali After French Withdrawal," Reuters, January 6, 2022, https://www.reuters.com/article/mali-security-russia-idAFL8N2TM47J.

19 Tanguy Berthemet, "Au Mali, premiers accrochages entre Wagner et djihadistes," *Le Figaro*, last updated June 1, 2022, https://www.lefigaro.fr/international/au-mali-premiers-accrochages-entre-wagner-et-djihadistes-20220105.

20 US Department of the Treasury, "Treasury Targets Financier's Illicit Sanctions Evasion Activity," News Release, July 15, 2020, https://home.treasury.gov/news/press-releases/sm1058; and Kimberly Marten, "Russia's Use of Semi-State Security Forces: The Case of the Wagner Group," *Post-Soviet Affairs* 35, no. 3 (March 2019): 181-204, doi:10.1080/1060586x.2019.1591142.

21 Pieter Wezeman et al., "Trends in International Arms Transfers, 2019," Stockholm International Peace Research Institute, SIPRI Fact Sheet, March 2020, doi:10.55163/YJYW4676; and Eklavya Gupte and Rosemary Griffin, "Analysis: Russia Looks to Africa to Broaden Its Global Energy Influence," S&P Global, October 22, 2019, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/102219-analysis-russia-looks-to-africa-to-broaden-its-global-energy-influence.

22 Eric Schmitt, "Russia's Military Mission Creep Advances to a New Front: Africa," *New York Times*, March 31, 2019, https://www.nytimes.com/2019/03/31/world/africa/russia-military-africa.html; United Nations Security Council, *Final Report of the Panel of Experts on the Central African Republic Extended Pursuant to Security Council Resolution 2399 (2018)*, with Cover Letter Dated 14 December 2018 to the President of the Security Council, United Nations Security Council, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2018_1119.pdf; and Dionne Searcey, "Gems, Warlords and Mercenaries: Russia's Playbook in Central African Republic, *New York Times*, last updated May 4, 2020, https://www.nytimes.com/2019/09/30/world/russia-diamonds-africa-prigozhin.html.

23 "Wagner Group, Yevgeniy Prigozhin, and Russia's Disinformation in Africa," US Department of State (website), May 24, 2022, https://www.state.gov/disarming-disinformation/wagner-group-yevgeniy-prigozhin-and-russias-disinformation-in-africa/.

24 *Glavnoye Razvedyvatelnoye Upravlenie*, Russia's main intelligence directorate

foreign funding through its contracts. The Touadéra contract is a prime example. Many of the Central African Republic's diamond mines have passed back and forth between government and rebel hands—a key source of funding for both the Touadéra government and the rebel groups. These mines, back in government hands, now fund Wagner. A portion of Wagner's payment is provided in diamonds, avoiding formal financial systems and therefore international sanctions, and in resource extraction permits to Russian companies linked to Prigozhin.[25] Wagner, however, does not just deal with the government: it also has made deals with the rebels themselves to obtain illegally mined diamonds, cashing in on and likely exacerbating the conflict.[26] Kimberley Marten, a scholar studying the Wagner Group, has suggested that Prigozhin may also use these connections and contracts to "engage in money-laundering or other criminal activity like smuggling, with the full knowledge and support of the Kremlin."[27]

It is quite possible, as the Russian government outsources more activities to PMCs, that it increasingly does so with cyber and information operations. For the PMCs, especially those with foreign government and foreign corporate clients, it is likely that market demands for these capabilities—as part of protective services, military combat augmentation, or something else—will drive them to increasingly develop or procure newer surveillance and cyber capabilities as well.

In operations less closely tied to Russian forces, PMCs may pursue or build on technical capabilities in a different manner, likely focusing on expanding their political warfare tool kit rather than combat adjacent capabilities. Security deployments to resource extraction sites are already profitable for the PMCs, but they also provide a wealth of strategic opportunities. PMCs in Africa, for instance, already conduct or work in tandem with Russian influence operations and the integration of additional technological capabilities may heighten their effects.[28] More advanced capabilities, such as cyber intrusion, represent an opportunity for PMCs to add or strengthen the political warfare layer of their operations while reaping profit.

Combat Missions

In Ukraine in 2014, soldiers without insignia, dubbed little green men, illegally invaded, attacked, and occupied territory, laying the path for a full-on Russian invasion of the country in 2022. This incursion into Crimea and the Donbas region of Ukraine leveraged a loose confederation of militia members and nonuniformed volunteers in mostly ancillary roles like diversion and sabotage.[29] Ukraine's Security Service accused the Wagner Group of assassinating Luhansk rebel leaders who disobeyed Russian orders.[30] The conflict served, in many ways, as a proving ground for PMCs that would later deploy to other theaters like Syria and Libya—where their combat and support roles would become far more substantial and integrated with the Russian military. And where Wagner would prove the more professional, capable, and better equipped.

PMCs like the Wagner Group perform military-style functions, engaging in armed combat, sometimes alongside the Russian military. In the fall of 2015, the Putin regime formally began its own intervention in Syria; by then, it had already sent hundreds of Wagner fighters into the country.[31] Wagner forces have fought repeatedly in battles in Syria on behalf of Bashar al-Assad's regime,[32] both in the course of providing protection services and, in at least one instance, while Wagner fighters stayed at a GRU base in the country.[33] Former Wagner fighters have described the PMC's equipment in Syria as including "mortars, howitzers, tanks, infantry fighting vehicles, and armored personnel carriers" as well as man-portable surface-to-air missiles, anti-tank systems, and grenade launchers[34]—conventional military equipment for the battlefield. Wagner took part in training and equipping Syrian regime forces alongside—but distinct from—uniformed Russian soldiers.

25 "The Wagner Group: A Russian Symphony of Profit and Politics," *Cipher Brief*, accessed June 24, 2022, https://www.thecipherbrief.com/column_article/the-wagner-group-a-russian-symphony-of-profit-and-politics.

26 Searcey, "Gems, Warlords and Mercenaries"; Federica Saini Fasanotti, "Russia's Wagner Group in Africa: Influence, Commercial Concessions, Rights Violations, and Counterinsurgency Failure," *Order From Chaos* (blog), Brookings Institution, February 8, 2022, https://www.brookings.edu/blog/order-from-chaos/2022/02/08/russias-wagner-group-in-africa-influence-commercial-concessions-rights-violations-and-counterinsurgency-failure/; and Luke Harding and Jason Burke, "Russian Mercenaries Behind Human Rights Abuses in CAR, Say UN Experts," *Guardian* (US edition), March 30, 2021, https://www.theguardian.com/world/2021/mar/30/russian-mercenaries-accused-of-human-rights-abuses-in-car-un-group-experts-wagner-group-violence-election.

27 Kimberly Marten, "Where's Wagner? The All-New Exploits of Russia's 'Private' Military Company," Program on New Approaches to Research and Security in Eurasia, PONARS Eurasia Policy Memo, September 15, 2020, https://www.ponarseurasia.org/where-s-wagner-the-all-new-exploits-of-russia-s-private-military-company/.

28 Jean Le Roux, "Pro-Russian Facebook Assets in Mali Coordinated Support for Wagner Group, Anti-Democracy Protests," DFRLab, Atlantic Council, February 17, 2022, https://medium.com/dfrlab/pro-russian-facebook-assets-in-mali-coordinated-support-for-wagner-group-anti-democracy-protests-2abaac4d87c4; Wassim Nasr, "France Says Mercenaries from Russia's Wagner Group Staged 'French Atrocity' in Mali," France 24, April 22, 2022, https://www.france24.com/en/africa/20220422-france-says-mercenaries-from-russia-s-wagner-group-staged-french-atrocity-in-mali.

29 Sergey Sukhankin, *Unleashing the PMCs and Irregulars in Ukraine: Crimea and Donbas*, Jamestown Foundation, September 3, 2019, https://jamestown.org/program/unleashing-the-pmcs-and-irregulars-in-ukraine-crimea-and-donbas/.

30 Owen Matthews, "Putin's Secret Armies Waged War in Syria—Where Will They Fight Next?" Newsweek, January 17, 2018, https://www.newsweek.com/2018/01/26/putin-secret-army-waged-war-syria-782762.html.

31 Nathaniel Reynolds, *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group*, Carnegie Endowment for International Peace, July 2019, 3, https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442.

32 See, for example, "How 'Wagner' Came to Syria," *Economist*, November 2, 2017, https://www.economist.com/europe/2017/11/02/how-wagner-came-to-syria; and Reynolds, *Putin's Not-So-Secret Mercenaries*, 5.

33 Rinat Sagdiev, Anton Zverev, and Maria Tsvetkova, "Exclusive: Kids' Camp on a Defense Base? How Russian Firms Masked Secret Military Work," Reuters, April 4, 2019, https://www.reuters.com/article/us-mideast-crisis-syria-russia-prigozhin/exclusive-kids-camp-on-a-defense-base-how-russian-firms-masked-secret-military-work-idUSKCN1RG1QT.

34 Justin Bristow, *Russian Private Military Companies: An Evolving Set of Tools in Russian Military Strategy* (Fort Leavenworth: US Foreign Military Studies Office, August 2019), 8-9; and Bukkvoll and Østensen, *The Emergence of Russian Private Military Companies*, 11.

As part of these operations, Russian PMCs leverage a range of surveillance-, cyber-, and intelligence-related capabilities—which appear to be growing in number. RSB Group set up a cyber attachment in 2016 that was reportedly capable of both defensive and offensive activities.[35] Russian PMCs in Syria have placed "intelligence specialists" on the front lines of armed combat to "better direct Russian airstrikes and enable pro-regime ground maneuvers."[36] Other PMC units "recruit human intelligence sources, guide [intelligence, surveillance, and reconnaissance] platforms and systems, collect signals intelligence, and analyze intelligence and open-source information," according to a Center for Strategic & International Studies report (citing a presentation by Kiril Avramov, a nonresident fellow at the Intelligence Studies Project at University of Texas at Austin).[37]

The widening adoption of surveillance and other technologies also poses a challenge to traditional PMC staffing and their own training, which may further pull companies in toward the Russian state. The classic pipeline for Russian service members to many PMCs begins in elite military units such as the VDV (abbreviation for *Vozdushno-desantnye voyska*, Russian Airborne Forces), Russian special forces, and various *Spetsnaz*[38] formations—enabling them to serve a broad range of familiar functions, both embedded within and alongside Russian military forces. While these groups may provide a range of useful kinetic skills and small unit combat training, they are more likely to lead to specialized combat and maneuver skills like parachuting, covert insertion, and marksmanship rather than electronic warfare or cyber operations. The pipeline then for PMCs to support the acquisition and use of these technologies must look appreciably different, and source from new communities across the Russian armed forces.

In Syria, Wagner has also taken contracts to secure resource extraction, specifically oil and gas. However, the presence of Western forces in the many-front conflict has complicated the mission, and members of the group have engaged in direct combat with the intention of protecting and preserving oil and gas access for the Assad regime. Wagner's presence in Syria is perhaps best known for a 2018 incident near a Conoco gas plant in the eastern part of the country. A pro-Assad group that included Wagner forces launched an attack on a US-supported Kurdish outpost where US soldiers were present, resulting in the death of hundreds of pro-Assad fighters.[39] The Pentagon later reported that in the hours leading up to the assault, US officials were in contact with their Russian counterparts and alerted them to an impending counterattack, but that the Russian command asserted that there were no Russians present. There is no evidence of Russian attempts to warn or interdict the Wagner forces on the ground. In the aftermath, the Russian Foreign Ministry said that "about five people who were 'presumably Russian citizens' may have been killed." Yet, other reports pointed to "substantial losses."[40] Despite expectations that Wagner would lessen its presence in the region following the incident, companies linked to Prigozhin have gained contracts to develop and guard new oil and gas fields in Syria, including in the same region where the firefight with US forces took place.[41] The additional contracts with the Assad regime follows—in no small part—the fact that Wagner receives payment at least partially in oil and gas, enabling it to skirt sanctions and financial regulations with its profit.[42]

Building on battlefield successes in both countries, Wagner emerged as Moscow's premier PMC, as evidenced by Prigozhin's appearance alongside Defense Minister Sergey Shoygu in deliberations with the LNA commander, Khalifa Haftar, in 2018.[43] Reported tensions between Shoygu's defense ministry and Wagner notwithstanding,[44] by the February 2022 invasion of Ukraine, the integration of PMCs—particularly Wagner—in Russian military operations had matured significantly. The Digital Forensics Research Lab has monitored Wagner activity across Ukraine, including in Zaporizhzhia, Volodymyrivka, and Klynove. Wagner activities in Ukraine appear to be intertwined with the Russian military, including Spetsnaz special forces.[45] According to the UK Ministry of Defence, the Wagner Group was engaged in direct combat in Ukraine to reinforce front-line Russian military forces in the capture of Popasna and Lysyschansk. Wagner is seeing heavy casualties in combat, and increas-

35 Margarete Klein, *Private Military Companies–A Growing Instrument in Russia's Foreign and Security Policy Toolbox*, European Centre of Excellence for Countering Hybrid Threats (Helsinki), June 2019, 3-4; and Bukkvoll and Østensen, *The Emergence of Russian Private Military Companies*, 14.

36 Seth G. Jones et al., *Russia's Corporate Soldiers: The Global Expansion of Russia's Private Military Companies*, A Report of the CSIS Transnational Threats Project (Lanham, Maryland: Rowman & Littlefield, July 2021), 18, 20, https://www.csis.org/analysis/russias-corporate-soldiers-global-expansion-russias-private-military-companies.

37 Jones et al., *Russia's Corporate Soldiers*, 18-20. Avramov, an assistant professor at UT-Austin, also serves as director of its Global (Dis)Information Lab.

38 *Spetsialnogo naznacheniya*, meaning special purpose

39 Kimberly Marten, "The Puzzle of Russian Behavior in Deir al-Zour," *War on The Rocks*, July 5, 2018, https://warontherocks.com/2018/07/the-puzzle-of-russian-behavior-in-deir-al-zour/.

40 Marten, "The Puzzle of Russian"; Mike Eckel, "Pentagon Says U.S. Was Told No Russians Involved in Syria Attack," Radio Free Europe/Radio Liberty, February 23, 2018, https://www.rferl.org/a/syria-deir-zor-attack-pentagon-russians-involved/29058555.html, and Gibbons-Neff, "How a 4-Hour Battle Between Russian Mercenaries."

41 Marten, "Where's Wagner? The All-New Exploits."

42 "The Wagner Group: A Russian Symphony," *Cipher Brief*.

43 Kate Baughman, "Russia's Not-So-Invisible Role in the Libyan Conflict," *in-depth* (blog), CNA, November 12, 2019, https://www.cna.org/our-media/indepth/2019/11/russias-not-so-invisible-role-in-the-libyan-conflict.

44 Warsaw Institute, "Shoigu's Revenge," *Russia Monitor*, February 25, 2018, https://warsawinstitute.org/shoigus-revenge/.

45 Trad, "Wagner Group Continues Involvement;" and Rob Lee (@RALee85), "Russian spetsnaz and Wagner private military contractors reportedly in Svitlodarsk and Myronivskyi," Twitter, May 24, 2022, 6:59 p.m., https://twitter.com/RALee85/status/1529235651094360064.

ingly, lost Wagner troops are being replaced with minimally qualified and trained recruits, including convicts.[46] Indeed, Wagner's experience in the comparatively permissive Syrian and Libyan theaters has proven insufficient to repeat their battlefield success, as they face far better trained and equipped Ukrainian forces.[47]

To the extent plausible deniability was ever a motivation for the Kremlin to rely on PMCs, their notoriety since 2014—Wagner's in particular—reveals an equally likely imperative: expendability. Contracted mercenaries simply require less accountability from the state, cost far less than training and outfitting conscripts, and entail fewer potential domestic constraints.

Moscow has long had to contend with the mothers of soldiers lost to war, and has a poor track record of transparency regarding conflict casualties.[48] In Donbas earlier this year, Ukrainian officials allege that Russia deployed mobile crematoria to dispose of its fallen soldiers, rather than sending them home.[49] The Kremlin was slow to acknowledge any casualties whatsoever, and the Defense Ministry has sought to classify the notification process for families.[50] While he is unlikely to face substantial public backlash for the Russian military's catastrophic performance in Ukraine, Putin's continued insistence on characterizing the war as a "special military operation," and his apparent reticence to call for a general mobilization to support it, signal some wariness of the war's political ramifications.[51] Meanwhile, as the war in Ukraine looks to grind further on, the demand for expendable forces is likely to increase.

Against that backdrop, PMCs like Wagner are an attractive option because they shift at least some of the burden of war away from the state—particularly as they cast combat operations as a commercial enterprise, versus a political one.[52] As Putin stated in late 2018, "We can ban the private security business altogether, but once we do that, I think you will get a lot of petitions to protect this labor market. As for their presence somewhere abroad, if, I repeat again, they do not violate Russian law, they have the right to work and push their business interests anywhere in the world."[53]

Political Warfare

Russian PMCs are also increasingly involved in conducting "political warfare" activities, ranging from subversive activities to assassination, reminiscent of the kinds of "active measures" that Soviet intelligence services deployed throughout the Cold War. In Syria in 2015, the Russian government spread propaganda prior to its involvement[54] and used PMCs on the ground to augment its forces once in the country. In the Central African Republic in 2018, three Russian journalists who were investigating Wagner's activities in Africa were killed, and while there is no conclusive documentation of the killer(s), the journalists' driver that day was in contact with a police officer working with a member of the Wagner Group.[55] Other reports describe PMCs as conducting political warfare activities such as kidnapping, sabotage, subversion, and blackmail.[56] Moscow is increasingly placing cyber and information proxies overseas, to launch operations from within other countries and ostensibly to create deniability—such as establishing Russian Internet Research Agency (IRA) facilities in Ghana, Nigeria, and Mexico.[57] In the Central African Republic, Prigozhin's profit-seeking activities do not end with the Wagner Group. The oligarch has also built hospitals through his mining companies, created a Russian radio station with a wider reach than the state station, and created a children's cartoon featuring a Russian bear saving its animal friends in Africa.[58] Such activities exemplify the duality of PMC's role in expanding Russian influence—pairing profit with propaganda.

46 Ministry of Defence (@DefenceHQ), "Latest Defence Intelligence update on the situation in Ukraine - 18 July 2022," Twitter, July 18, 2022, 2:12 a.m., \https://twitter.com/DefenceHQ/status/1548913656410226688.

47 Reuters, "Russian Troops Ill-Prepared for Ukraine War."

48 Reuters, "Russian Troops Ill-Prepared for Ukraine War"; "'Private Pivovarov Is on Assignment': How Russia Hides Its Military Casualties," *Moscow Times*, April 6, 2022, https://www.themoscowtimes.com/2022/04/06/private-pivovarov-is-on-assignment-how-russia-hides-its-military-casualties-a77247.

49 Russia Abandons Its Dead Soldiers on the Battlefield, Claims Ukraine," *Times* (United Kingdom), March 30, 2022, https://www.thetimes.co.uk/article/russia-abandons-its-dead-soldiers-on-the-battlefield-claims-ukraine-wh8c092n2.

50 Lisa Kim, "Putin Spokesperson Admits 'Significant Losses' of Russian Troops in Ukraine," Forbes, April 7, 2022, https://www.forbes.com/sites/lisakim/2022/04/07/putin-spokesperson-admits-significant-losses-of-russian-troops-in-ukraine/?sh=15deb12e2cfb; and "Russia to Classify Information on Ukraine Troop Deaths," *Moscow Times*, April 20, 2022, https://www.themoscowtimes.com/2022/04/20/russia-to-classify-information-on-ukraine-troop-deaths-a77416.

51 Andrew Osborn and Polina Nikolskaya, "Russia's Putin Authorises 'Special Military Operation' against Ukraine," Reuters, February 24, 2022, https://www.reuters.com/world/europe/russias-putin-authorises-military-operations-donbass-domestic-media-2022-02-24/; and Jay Beecher, "ISW Russian Offensive Campaign Assessment, July 4," *Kyiv Post*, July 5, https://www.kyivpost.com/russias-war/isw-russian-offensive-campaign-assessment-july-4.html.

52 "A mercenaries' war: How Russia's invasion of Ukraine led to a 'secret mobilization' that allowed oligarch Evgeny Prigozhin to win back Putin's favor," Meduza, July 14, 2022, https://meduza.io/en/feature/2022/07/14/a-mercenaries-war.

53 "Big Press Conference of Vladimir Putin," Interfax-Russia (news agency), December 20, 2018, https://www.interfax.ru/russia/643241.

54 Peter Pomerantsev, "Inside the Kremlin's Hall of Mirrors," The Guardian, April 9, 2015, https://www.theguardian.com/news/2015/apr/09/kremlin-hall-of-mirrors-military-information-psychology.

55 Tim Lister and Sebastian Skukla, "Murdered journalists were tracked by police with shadowy Russian links," CNN, January 10, 2019, https://www.cnn.com/2019/01/10/africa/russian-journalists-car-ambush-intl/index.html.

56 Jones et al., *Russia's Corporate Soldiers*, 18.

57 US Office of the Director of National Intelligence. *Foreign Threats to the 2020 US Federal Elections*. ICA 2020-00078D. Washington, D.C.: US Office of the Director of National Intelligence, March 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf. 4.

58 Searcey, "Gems, Warlords and Mercenaries"; *Afrique Média*, "Reportage sur la Radio Lengo Songo RCA Ngadi Kwa Vanessa," YouTube video, January 31, 2019, https://www.youtube.com/watch?v=CQ9qWX3bQfYn; Улыбаемся Машем, *Lionbear*, YouTube video, July 18, 2019, https://www.youtube.com/watch?v=NCZ0YSyWVhk&t=4s.

Prigozhin, in addition to heading the Wagner Group, is also at least partially responsible for the activities of the IRA, better known within the United States as the Russian Troll Factory. The US government has both sanctioned and indicted Prigozhin and associated companies in connection with IRA support of the 2014 invasion of Ukraine and its attempts to influence the 2016 US presidential election.[59] Though this agency and the Wagner Group are not officially aligned, IRA activity has been uncovered in tandem with Wagner operations. A 2022 Twitter disclosure, for example, exposed a coordinated campaign within the Central African Republic of pro-Russian propaganda from both real and fake Twitter accounts linked to the IRA.[60] In addition, Wagner's activities in Mali appear closely buttressed by IRA efforts. In preparation for Wagner's deployment to the country, "a coordinated network of Facebook pages in Mali promoted Russia as a 'viable partner' and 'alternative to the West,' encouraged postponement of democratic elections, and attempted to create local support for Wagner."[61] This disinformation machine also deployed earlier this year to deny and deflect responsibilities for massacres tied to the Wagner Group in Mail, such as those in Mourah and Gossi.[62]

ACCESSING OFFENSIVE CYBER AND INFORMATION TECHNOLOGIES IN THE PMC COMMUNITY

The fusion of several quasi-state models of digital subversion with the paramilitary prowess of Russian PMCs should also not be ruled out. One dimension of Russian PMCs acquiring these capabilities is the possibility that they might access existing public/private relationships established by organs of Russian intelligence or even the commercial market. The commercial development, sale, and support of offensive cyber capabilities and electronic surveillance services includes dozens of firms, some of whom have access to the latest security vulnerabilities and considerable technical design and development talent.[63] With the addition of boutique cyber-surveillance tools, like those developed by commercial outfits like NSO Group and DarkMatter, to disruptive attacks-as-a-service brokered by ransomware collectives, like REvil, PMCs could vastly expand their clientele among global autocrats and oligarchs—thus substantially enhancing their utility to the Kremlin. These latter companies could provide access to technology systems and are well-positioned to provide PMCs with intelligence gathering and ongoing high-value target surveillance capacity across the world.[64]

An alternative, especially in the case of offensive cyber capabilities, may be for these PMCs to partner with Russian private companies or state labs working as proxies for Russian military and intelligence organizations. In 2018, FireEye Intelligence pointed to Russia's Central Scientific Research Institute of Chemistry and Mechanics as likely supporting the deployment of Triton, an operational technology-focused malware, and the US government later sanctioned the lab.[65] The US government claims that a private Russian firm, Positive Technologies—which the US Treasury identified as supporting the Russian Federal Security Service (FSB) and sanctioned—continues to develop offensive cyber capabilities on behalf of the Russian government.[66] Leveraging the capabilities of such organizations would prevent PMCs from needing to develop significant and costly new in-house talent or drawing the added scrutiny of Russian government authorities.

WHERE DO PMCs GO FROM HERE?

Major course corrections in Russia's geopolitical trajectory seem unlikely so long as Putin remains in power, and the trajectory of Moscow's war effort in Ukraine remains speculative at best. Importantly, the driving forces for Russian PMC involvement in locations like Libya,

59 "U.S. Widens Sanctions Net Against Kremlin-Connected Backer of 'Troll Factory,' Mercenary Group," Radio Free Europe/Radio Liberty, September 23, 2020, https://www.rferl.org/a/u-s-widens-sanctions-net-against-kremlin-connected-backer-of-troll-factory-mercenary-group/30854350.html; US Department of Treasury, "Treasury Increases Pressure on Russian Financier," News Release, September 23, 2020, https://home.treasury.gov/news/press-releases/sm1133; "U.S. Imposes New Sanctions Targeting Russian 'Troll Farm,' Owner Prigozhin," Radio Free Europe/Radio Liberty, September 30, 2019, https://www.rferl.org/a/us-imposes-new-sanctions-targeting-russian-troll-farm-owner-prigozhin/30191701.html; and United States v. Internet Research Agency, No. 1:18-cr-00032-DLF, (D.D.C. 2018), https://www.justice.gov/file/1035477/download. US District Court for the District of Columbia.

60 Twitter Safety (@TwitterSafety), "Disclosing State-Linked Information Operations We've Removed," Twitter, December 2, 2021, https://archive.ph/ZXw4k; and US Department of State, "Wagner Group, Yevgeniy Prigozhin, and Russia's Disinformation in Africa."

61 US Department of State, "Wagner Group, Yevgeniy Prigozhin, and Russia's Disinformation in Africa"; Le Roux, "Pro-Russian Facebook Assets in Mali"; and Nasr, "France Says Mercenaries."

62 US Department of State, "Wagner Group, Yevgeniy Prigozhin, and Russia's Disinformation in Africa"; Emmanual Akinwotu, "Russian Mercenaries and Mali Army Accused of Killing 300 Civilians," *Guardian* (US edition), April 5, 2022, https:/www.theguardian.com/world/2022/apr/05/russian-mercenaries-and-mali-army-accused-of-killing-300-civilians; "Mali: l'armée annonce avoir tué plus de 200 «combattants» terroristes lors d'une opération," RT France (Russian state-controlled media), April 2, 2022, https://archive.ph/pYOJT; Sam Mednick, "French Accuse Russian Mercenaries of Staging Burials in Mali," *Washington Post*, April 22, 2022, https://web.archive.org/web/20220425175005/https:/www.washingtonpost.com/world/russians-accused-of-staging-french-burial-of-bodies-in-mali/2022/04/22/c6b768a4-c228-11ec-b5df-1fba61a66c75_story.html; and "La pensée de l'expert russe, Maxime Shugaley, sur les atrocités à Gossi," Mali ACTU, April 28, 2022, https://maliactu.net/la-pensee-de-lexpert-russe-maxime-shugaley-sur-les-atrocites-a-gossi/.

63 Winnona DeSombre et al., "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets," Atlantic Council, Issue Brief, November 8, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/.

64 Winnona DeSombre et al., *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service*, Atlantic Council, March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

65 FireEye Intelligence, "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers," Mandiant, October 23, 2018, (FireEye is now part of Symphony Technology Group), https://www.mandiant.com/resources/triton-attribution-russian-government-owned-lab-most-likely-built-tools; and Catalin Cimpanu, "US Treasury Sanctions Russian Research Institute Behind Triton Malware," *ZDNet*, October 23, 2020, https://www.zdnet.com/article/us-treasury-sanctions-russian-research-institute-behind-triton-malware/.

66 US Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," Press Release, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0127; and Patrick Howell O'Neill, "The $1 Billion Russian Cyber Company That the US Says Hacks for Moscow," *MIT Technology Review*, April 15, 2021, https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/.

Syria, Ukraine, Mali, and the Central African Republic appear diverse. In some instances, PMCs act alongside or immediately in lieu of still uniformed Russian forces. In other cases, these firms appear to be operating with greater independence, often with clear profit motive.

Putin's inner circle of oligarchs control and have interest in a wide range of industries, and often they and their close relatives are involved in various companies. These companies have several lines of revenue: thinly veiled authorized theft from the state, direct business revenue, and unofficially sanctioned criminal activity. In the oil and gas, entertainment, finance, and similar industries, this breakdown of oligarch profit is fairly straightforward. However, private military companies and those at their helm have a more complicated relationship with the workings of the Kremlin.

The involvement of Russian PMCs in extractive and more purely profit-seeking activities raises questions about how their incentive structure will change in the aftermath of the ongoing war in Ukraine and in the face of the adoption and employment of new technologies in conflict. These include:

- What levers (sanctions, export controls, etc.) can the transatlantic community use to curb the flow of illicit kinetic and digital arms alike, not only to the Russian state, but to commercial entities or third countries that might enable PMCs?
- How can the United States and its allies and partners work together to disincentivize the use of PMCs for regime and mineral-deposit security among leaders in Africa and elsewhere? What alternatives can they offer?
- What lessons is the Kremlin drawing and not drawing from its open war on Ukraine? How might that shape future decision-making about PMCs and conflict?
- If the Russian military and state defense apparatus is involved with supplying PMCs, does that extend to technological and cyber capabilities today? Might it in the future, and if so, how? What do those relationships and dependencies look like?

These quasi-private military forces are a useful tool that Russia can deploy to manage risk, foment instability, and exploit geopolitical and economic opportunities around the world in advance of, in addition to, or instead of Russian state capabilities. These groups, often run by Russian oligarchs, are employed in a wide range of operations that support, sometimes directly and sometimes more opaquely, Russian strategic objectives. The Russian state benefits from having a nominally independent additional reserve that can project force in places where state-tied operations may carry additional risk—from conflict zones where the state's forces require additional support to areas of insecurity where PMCs can enrich themselves while projecting Russian power and influence abroad.

The technological capabilities that these companies develop may serve as an indication of Russian strategic priority and perhaps its points of perceived weakness in the years to come. The wide remit of operations under the PMC umbrella means that there exists a foundation for these companies to develop in myriad ways. A more combat-focused PMC, for example, will not pursue the same technologies as a PMC focused on political warfare in non-warfare zones. The unique position of Russian PMCs—motivated both by profit and policy—exemplify the ongoing tension in Russia's kleptocratic leadership and thus may be an effective way for the United States and its allies to understand Russian priorities and engage with them in a more persistent manner.

AUTHORS

Emma Schroeder is an assistant director with the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. Her focus in this role is on developing statecraft and strategy for cyberspace that are useful for both policymakers and practitioners.

Gavin Wilde a senior fellow at the Carnegie Foundation for International Peace and a nonresident fellow at Defense Priorities. He previously served as director for Russia, Baltic, and Caucasus affairs at the National Security Council, where his focus areas included election security and countering foreign malign influence and disinformation.

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative, where his work focuses on the geopolitics, governance, and security of the global Internet. He is also a research fellow at the Tech, Law & Security Program at American University Washington College of Law, a fellow at Duke University's Sanford School of Public Policy, and a contributor at WIRED magazine.

Dr. Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on the role of the technology industry in geopolitics, cyber conflict, the security of the internet, cyber safety, and growing a more capable cybersecurity policy workforce.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
*Rafic A. Bizri
*Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
Beth Connaughty
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
Mark T. Esper
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Frank Haun
Michael V. Hayden
Amos Hochstein
Tim Holt
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Ashraf Qazi
Robert Rangel
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of July 13, 2021