Report

Democracy in the Crosshairs

Five Key Trends Driving Foreign Interference in Democracies

G | M | F Alliance for Securing Democracy

Vassilis Ntousas, David Salvo

Table of Contents

Introduction

Combating foreign interference in democracies, once a fringe policy issue on both sides of the Atlantic, has become one of the key policy and societal challenges of our time. It was not long ago when this set of issues would be buried in official communiqués in sections labeled “hybrid threats” and walled off to be studied by specialists in nascent institutions, if not virtually ignored, across the transatlantic space.

Russia’s comprehensive interference operation in the 2016 US presidential election changed that calculus, as did high-profile interference cases targeting European countries in the subsequent years. Since that time, adversaries have grown in numbers, appetite, and sophistication, launching increasingly disruptive campaigns that take direct aim at the democratic fabric of the transatlantic community. In response, most national governments and multilateral institutions like the EU and NATO have ramped up their attempts to defend against and respond to foreign interference.

Yet the threat of foreign interference has evolved rapidly, in some cases outpacing efforts to address it. This is not just due to slow or sclerotic bureaucracies having to adapt quickly—and, unfortunately, not always successfully—to the challenge at hand. Foreign interference threats have targeted all sectors of democratic society and aggressively exploited technological innovations to make their offensives more complex and far more demanding to tackle in real time for governments, private industry, and civil society alike.

This report by the Alliance for Securing Democracy (ASD) at the German Marshall Fund of the United States (GMF) explains five key trends that have shaped the foreign interference threat landscape since Russia’s comprehensive operation in the United States eight years ago. It focuses both on the explosion of malign actors and their ever-changing tactics. In a year full of consequential elections in democracies on both sides of the Atlantic and around the globe, analyzing these trends and their impact will help various stakeholders in different sectors build more meaningful and impactful responses in coming years. It is also significant for understanding the very real dangers that foreign interference threats continue to pose to national security and democratic stability, as democracy itself remains in the crosshairs.

1. Old Adversaries Are Increasingly Aggressive and Aligned

Russia and the People's Republic of China (PRC) remain the two primary vectors of foreign interference targeting the United States and Europe. The global renaissance of geopolitical competition and a growing perception that democratic exhaustion is gaining momentum have given both nation states greater confidence to launch interference campaigns. Importantly, these operations are aimed not simply at influencing policy outcomes or swaying electoral outcomes, but at undermining democracy itself.

Russia's interference toolkit remains largely unchanged from years past, relying on threat vectors like information operations and malign finance to undermine democratic institutions, elections, and societies in the West. But it continues to find new tactical approaches within this toolkit to remain a perpetually disruptive—and increasingly dangerous—player on the global stage. Meanwhile, the PRC has increasingly turned to such hybrid tools to advance its interests abroad, undermine US leadership globally, subvert civil society in other countries, and promote illiberalism at democracy's expense.

Russia

Russia's government remains as serious a threat to the democratic order as ever, a fact punctuated by its full-scale invasion of Ukraine in February 2022 and attempt to overthrow its democratically elected government. The Kremlin has a vested interest in democratic disorder around the globe, and particularly across the transatlantic space. President Vladimir Putin's authoritarian, kleptocratic regime has become increasingly dictatorial, not only punishing Russia's neighbors in Ukraine but its own citizens too. By tamping down dissent and political opposition like never before, Russia's authoritarian system more and more embodies some of the sinister aspects of its Soviet predecessor. The results of the 2024 Russian presidential election, in which Putin was reelected with more than 87% of the vote after Russian authorities jailed, silenced, or killed most of the country's meaningful political opposition, dispensed with even the slightest pretense of democracy. Conducting malign interference operations to further destabilize democracies serves Russian domestic purposes just as much as it serves its foreign policy objectives. Democracies in disarray allow Russian state propagandists more fodder for justifying the Kremlin's iron-fisted rule and authoritarian agenda at home.

But foreign policy objectives undoubtedly feature prominently in the Russian state's interference operations abroad, especially as it continues its illegal and unprovoked war in Ukraine. Exacerbating divisions and weaknesses in the Euro-Atlantic alliance over support for Ukraine and amplifying politicians—often on the far ends of the political spectrum—who advocate isolationist positions or are overtly pro-Russian in their worldview remain cardinal goals of Russian interference operations. In its first-ever report on threats focusing especially on the Foreign Information Manipulation and Interference (FIMI) domain published in February 2023, the European External Action Service (EEAS) alarmingly confirmed that "there is no longer any distance between the Kremlin's diplomatic and FIMI arms".

The Kremlin's attempts to shape public and political debates over the war in Ukraine are emblematic of this. As analyzed in an ASD report, in the first six months after the full-scale invasion began, Russian state-sponsored outlets churned out content attempting to persuade Western audiences that Russia had been provoked into attacking Ukraine and that the atrocities and war crimes committed by the Russian military were conspiracies that Ukraine had orchestrated. These narratives had little impact in the United States and Europe, where a cross-partisan, transnational alliance rose up in support of Ukraine.

In fall 2022, however, this set of narratives began to change, emphasizing the economic consequences of Western sanctions not for Russia, but for the West itself. Drawing on data from ASD's Hamilton 2.0 Dashboard, compared to the first six months of the war, tweets by Russian-linked accounts from August 2022 to January 2023 that mentioned "both 'energy' and 'Ukraine' increased by 267%, while tweets mentioning 'cost of living' increased 66%". Just as telling, in their messaging to American and European audiences during the first 11 months of the war, "Kremlin-affiliated accounts tweeted the terms 'inflation', 'recession', 'economy', or 'economic' more than 15,500 times, generating more than 905,000 likes and 313,000 retweets". While it is impossible to draw a direct causal link between Russian messaging and the evolution of US political debate, it was around this time when some members of Congress began to question the purpose of providing military assistance to Ukraine, often highlighting the economic consequences for Americans. Regardless, Russian state-sponsored messaging to Americans and Europeans alike was designed to undermine continued support for Ukraine by emphasizing how doing so would have economic repercussions for the West.

Hamilton 2.0 Dashboard

ASD's Hamilton 2.0 Dashboard offers a comprehensive analysis of the narratives and topics propagated by Russian, PRC, and Iranian government officials and state-backed media. This dashboard covers a range of platforms, including Telegram, YouTube, Facebook, Instagram, state-sponsored news websites, and official press releases from respective ministries of foreign affairs.

Russia uses other tools that reinforce key objectives of its information operations. In the United States, Moscow's cyber operations have targeted electoral infrastructure—not just voting systems but online voter rolls and official state election websites as well—to exacerbate many Americans' distrust in the integrity of US elections. Russian state-affiliated hackers have also increasingly employed cyber tools like ransomware to paralyze businesses and key social services like hospitals, map vulnerabilities in American critical infrastructure, and harass and intimidate key voices in civil society that Russia perceives as hostile to its interests.

With the 2024 presidential election on the horizon, Russia remains the threat actor that most concerns US government officials. In May, Director of National Intelligence Avril Haines told the Senate Select Committee on Intelligence that "Russia remains the most active threat to our elections. The Russian government's goals in such influence operations tend to include eroding trust in [US] democratic institutions, exacerbating sociopolitical divisions in the United States, and denigrating Western support to Ukraine." Russia may not wage the type of all-encompassing interference operation in 2024 that it did during the 2016 presidential election. But with a shift in US policy in Ukraine potentially on the ballot this election and with heightened polarization dividing Americans on any number of issues, Russian-backed efforts to interfere have already surfaced. One example is the US Department of Justice's recent indictment alleging that Russian state media employees funneled nearly $10 million to a US content creation company to target American voters and promote Moscow's interests, in what is likely only a small part of a much wider set of Russian threats.

Russia's interference campaigns across Europe have also been deliberate, corrosive, and increasingly sophisticated. The war in Ukraine has served as a major accelerant of Moscow's interference objectives, conducting operations that have spanned nearly the whole of Europe. The full-scale invasion was accompanied by "disinformation of an unparalleled malice and magnitude", as the 2022 report from the European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE), starkly described.

Only in the past few months of 2024, a spate of cash-for-influence, sabotage, election interference, and espionage cases has surfaced in Europe. In March, Germany's Defense Minister Boris Pistorius claimed that Russia leaked a 38-minute audio recording it had intercepted in which four top German military officers discussed support for Ukraine, as part of an "information war". In the same month, collaboration among authorities in several European countries revealed a Russian-backed propaganda network financing a double operation of disinformation and interference across the continent. According to reports, the network used the pro-Russia website "Voice of Europe" as a vehicle to pay politicians from across the EU, including members of the European Parliament, to disseminate pro-Kremlin narratives about Ukraine and influence public opinion before the European Parliament elections in June. This was followed by serious allegations in Germany that the far-right Alternative für Deutschland (AfD) party's top two candidates for the European elections had nefarious links to Russia and/or the PRC.

In May, NATO expressed deep concerns over "hostile" Russian activity across the continent, pointing to hybrid operations that had affected Czechia, Estonia, Germany, Latvia, Lithuania, Poland, and the United Kingdom. Similarly, European intelligence agencies offered alarming assessments over what they saw as Russian preparations of violent sabotage acts across the continent, including covert bombings, arson, and attacks on infrastructure. This followed arrests in Germany on suspicion of plotting attacks on US military facilities and other targets on behalf of Moscow, Swedish authorities' investigation of possible sabotage linkages behind a number of railway derailments in the country, and an Estonian internal security services' allegation that Russian agents were recruiting local citizens to attack government targets.

Beyond undermining democracy in countries across the transatlantic community, Russia has employed similar hybrid tactics either in service of its own interests or to compete with the West in many parts of the "Global Majority", including sub-Saharan Africa, the Middle East and North Africa, and Latin America. In these regions, particularly in Africa, the Wagner Group, formerly led by the now-deceased Yevgeny Prigozhin, has provided military support to Moscow-aligned dictators and autocrats, fomented suppression of political opposition, and conducted information operations in conjunction with both. Russia's vast propaganda machine, particularly Sputnik and RT, produces and provides content for resource-starved local media organizations in vulnerable regions, while RT stories are repackaged and republished on suspicious networks of spoof local news sites purporting to be authentic American or European voices. Targeting Latin America, RT en Español is arguably RT's most successful brand, significantly outperforming

RT's flagship English-language channel on a variety of social media platforms. It is also among the most followed Spanish-language media pages on Facebook, often besting other international outlets like Telemundo and CNN en Español. This global propaganda apparatus gives the Kremlin an important channel to unleash information operations that undercut the West in key regions around the world.

Information Integrity Organization Map and Resources

Developed for the Summit for Democracy's Information Integrity cohort, co-led with the governments of Canada and Latvia, ASD's Information Integrity Map offers a comprehensive view of organizations worldwide dedicated to fostering a healthier information space. Featuring 531 organizations across 113 countries, the map reflects the vast majority of initiatives and resources aimed at upholding information integrity globally, categorizing these efforts into four key areas: fact checking and verification, media literacy and training, research and monitoring, and policy and standards.

The People's Republic of China

The PRC, led by the ruling Chinese Communist Party (CCP), has become a more aggressive and assertive actor against democratic targets globally. Its campaign to meddle in the 2024 Taiwanese presidential election—an attempt to influence policy and electoral outcomes and entrench the One China policy on both sides of the Taiwan Strait—is indicative of the tools and tactics the CCP is now willing and able to employ in the interference domain. Indeed, PRC state-sponsored actors co-opted political and business elites and levied economic sanctions and threats of economic reprisals, as well as executed other gray-zone tactics to influence voter behavior, even if it is worth noting that the CCP's preferred candidate still lost. Elsewhere, the PRC has increasingly targeted its perceived critics, businesses, and politicians beyond its borders, and strengthened its covert police presence overseas as well.

In the United States, the PRC's operations have included targeting state and local politicians as a vector of influence for steering policies that align with Beijing's preferences. A US National Counterintelligence and Security Center report from 2022 describes how PRC state-affiliated actors exploit partnerships, such as the "Sister Cities" network, create economic dependencies with business leaders, instruct state legislators to introduce PRC-friendly legislation, and intimidate perceived enemies.

The PRC has not had much success targeting and co-opting national politicians in the United States like it has had in countries such as Australia, nor has it been a major player in trying to destabilize US presidential elections thus far. The Office of the Director of National Intelligence concluded in July that the PRC "does not plan to influence the outcome of the US presidential election." However, the assessment did not exclude the possibility that the PRC would try to malign candidates further down the ballot, a tactic it adopted during the 2022 midterm cycle. Indeed, during the midterms, PRC state-sponsored actors targeted candidates for Congress from both US political parties, relying on TikTok in particular as a platform for spreading CCP messaging about American candidates and political issues to a larger and broader American audience. Furthermore, a former aide to New York Governor Kathy Hochul and former Governor Andrew Cuomo was recently indicted for secretly acting as an agent of the PRC's government in exchange for millions of dollars in compensation and gifts, demonstrating an increasing PRC interest in US state politics.

The PRC's interference operations in Canada offer an important window into its attempts to shape specific electoral outcomes. There, PRC-affiliated actors targeted the Chinese-Canadian diaspora with a particular focus on denigrating support for Conservative Party candidates, some of whom the PRC perceived as hostile to Beijing's interests and some of whom were of ethnic Chinese origin. Mandarin-language newspapers and WeChat, the popular Chinese social messaging app, were important conduits reportedly used to target the diaspora. An independent inquiry into PRC interference in Canadian elections commissioned by the Canadian government found a "reasonable possibility" that the PRC's interference cost a Conservative Party candidate a seat in the 2021 parliamentary election.

In an example of interference operations often being "party-agnostic", the previous Canadian government's special rapporteur on foreign interference, David Johnson, concluded that in 2019, the PRC consulate in Toronto contributed to "irregularities" in the Liberal Party nomination process in an Ontario parliamentary district. Allegedly, PRC-linked actors helped fund buses to deliver Chinese students to the polls to secure the Liberal Party nomination for Member of Parliament (MP) Han Dong, who was viewed as more sympathetic to pro-PRC positions. The Canadian government inquiry could not substantiate allegations that MP Dong was aware of a PRC role in the campaign. The Canadian government inquiry also concluded that in the 2019 election cycle, PRC-affiliated actors used Canada-based proxies "to exclude 'political candidates perceived as anti-China from attending' local election-related events" and claimed that two transfers of $250,000 Canadian dollars from PRC officials in Canada were "possibly" used to facilitate foreign interference operations.

In Europe, the PRC has heightened its efforts to acquire vital economic assets, penetrate critical infrastructure, and steal sensitive technologies and cutting-edge technological know-how. The General Intelligence and Security Service of the Netherlands published a report in 2023 clearly warning that the PRC eyes and targets high-tech companies, knowledge institutions, and scientists through "legitimate investments, corporate takeovers, and academic cooperation, as well as illegitimate (digital) espionage, insiders, covert investments and illegal exports". Similar findings have been incorporated in several other EU member states' official assessments of security challenges. In its 2024 annual report, Norway's intelligence agency, for example, warned that PRC "intelligence services operate all over Europe. Their activities include political intelligence and industrial espionage, and cyberspace is the main gateway."

Critically, as a series of recent scandals demonstrated, the PRC's foreign interference activities have shown an increasing penchant for attempting to influence democratic processes in Europe. At the G20 summit in India in September 2023, former UK Prime Minister Rishi Sunak raised his concerns to his PRC counterpart about PRC interference in the United Kingdom's democracy following the arrest of a parliamentary researcher with links to several senior Tory lawmakers on suspicion of spying for the CCP. A few months later, the British government formally accused PRC state-affiliated actors for conducting a series of cyberattacks targeting the country's elections watchdog and UK lawmakers.

In April 2024, a close adviser to Maximilian Krah, now a sitting member of the European Parliament from Germany and then the AfD's top candidate for the EU election, was arrested on suspicions of spying for the PRC, raising alarms over influence-seeking campaigns. And earlier this year, the US Department of Justice issued an indictment alleging that PRC-backed hackers had targeted a number of European politicians to gather sensitive data over the past few years. One related case was a social media disinformation operation that targeted then-Chair of the European Parliament's Special Committees on Foreign Interference Raphaël Glucksmann, who was informed in mid-April that PRC-linked accounts had been accusing him of being a US Trojan horse in Europe.

A Greater Degree of Alignment

Finally, strategic and deliberate Sino-Russian cooperation on interference operations remains a topic of speculation, though the deepening of bilateral ties since Russia's full-scale invasion of Ukraine has likely led to some convergence in objectives and tactics. As indicated above, Beijing and Moscow share a goal in denigrating democracy as a model of governance and undermining the resilience of democratic institutions in countries that challenge them. Both have an interest in challenging the liberal democratic international order. In the final communiqué of NATO's 75th anniversary summit this summer, NATO allies expressed "profound concern" over the "strategic partnership between Russia and the PRC and their mutually reinforcing attempts to undercut and reshape the rules-based international order".

The war in Ukraine provides a very direct illustration of this dynamic. ASD's deep dive into Russian and PRC information operations during the first 11 months of the armed conflict demonstrated that PRC "messaging around the war in Ukraine […] prioritized defending [PRC] interests over Russia's; though, both countries' interests are so strongly intertwined, at least in terms of undermining the West, that it is often difficult to distinguish between the two."

Focusing on war messaging in particular, our analysis found that while the PRC was cautious not to publicly endorse Russia's war of choice, it nonetheless openly supported and promoted Kremlin-friendly and anti-West narratives about the war. For example, immediately after the invasion, PRC "state media outlets adopted Russia's sanitized language to describe the war, obfuscating the severity of Moscow's actions by labeling the invasion as a 'special operation', an 'issue', or a 'situation'. Mentions of 'war' or 'invasion' were largely reserved for whataboutism arguments directed at past US wars and interventions, most notably in the Middle East." Similar trends were observed throughout the surveyed period of the first 11 months of the war, in which PRC "diplomatic and state-affiliated media accounts on [X] mentioned the United States more than twice as often as Russia in tweets mentioning 'war'." PRC state media also regularly hosted and amplified several current and former Russian state media commentators, allowing pro-Kremlin voices to reach an even wider global audience. Ukrainian voices were given far less prominence in comparison. Our data found that between February 24, 2022 and January 23, 2023, for example, PRC diplomatic and state media accounts on X quoted Russian Foreign Minister Sergei Lavrov three times more than his then Ukrainian counterpart, Dmytro Kuleba, and PRC diplomats were roughly eight times more likely to quote Russia's president than Ukraine's.

2. New Threat Actors Are Proliferating

New State Actors

Democracy is eroding at a global level. Like Russia and the PRC, other nation states have increasingly capitalized on vulnerabilities in the democratic order worldwide, concluding that interference operations are low-cost, relatively low-risk pathways to exert influence abroad. Even back in 2020, the Oxford Internet Institute's Global Inventory of Organized Social Media Manipulation found "evidence of 81 countries using social media to spread computational propaganda and disinformation about politics."

Corruption has been at the heart of many nation states' interference campaigns across the transatlantic community, including the notorious "Qatargate" scandal in the European Parliament in late 2022. In one of the biggest graft scandals in the EU in decades, a years-long corruption investigation led to high-profile arrests based on allegations that Qatar, Morocco, and Mauritania sought to buy influence in the European Parliament to promote their interests. Meanwhile, in the United States, former Chairman of the US Senate Foreign Relations Committee Bob Menendez was found guilty of accepting bribes on behalf of—and acting as a foreign agent of—the Egyptian government.

A 2022 classified US intelligence report detailed how the United Arab Emirates (UAE) went to extensive efforts, licitly and illicitly, to influence US foreign policy. Their tactics were numerous and often involved domestic proxies in the United States. The report includes allegations that the UAE hired former US intelligence and military officials to hack into computer systems to target politicians, dissidents, journalists, and corporations. It also highlights how the UAE funneled money into friendly US think tanks to produce policy reports favorable to UAE interests, while masking the origin of the funding. ASD's "Covert Foreign Money" report also documents the extent to which the UAE and other nation states exploited loopholes in US policy and the country's legislative framework to interfere in US democracy. For example, the UAE used US-based straw donors to funnel campaign contributions to Hillary Clinton's 2016 presidential campaign and to Donald Trump's 2016 inaugural committee, ultimately causing political action committees affiliated with Clinton to "unwittingly file false [Federal Elections Commission] reports".

Iran has also systematically engaged in interference operations and is perceived as a rising threat in this domain. According to Microsoft's Threat Analysis Center's report on interference in the 2020 US presidential election, Iran "launched several cyber-enabled influence operations that impersonated American extremists … and attempted to sow discord among US voters and incite violence against US government officials." Since then, Tehran has sharpened its methods. In an August 2024 bulletin, the same center described Iran's tactics for interfering in the 2024 US presidential election cycle, detailing Iranian information operations that often mirrored methods Russia employs. Captured in more detail in a follow-up report, Iranian state-affiliated actors were found to have created fake US local news sites and used artificial intelligence (AI) tools to plagiarize content from US media sources. Like Russia, these operations targeted Americans on the left and right of the political spectrum, demonstrating that Iran too has an overarching interest in general instability in the United States.

Like Russia and the PRC, Iran has also exploited sensitive political topics in the United States, including the Israel-Hamas war and cultural flashpoints like racial and gender issues, to amplify societal divisions and promote pro-Iranian views. Analyzing how state-affiliated accounts from these three countries covered the first month of the Israel-Hamas war across multiple social media platforms, an ASD report found that Iranian messengers used the war to enhance their country's own global standing and promote its influence within and beyond its borders.

In perhaps its most notorious interference attempt in 2024, Iran was purportedly behind an attempted "hack-and -leak" operation against the Trump campaign in August. Politico and the New York Times each received an anonymous email containing internal campaign documents, including vetting documents for Trump's vice-presidential selection, US Senator JD Vance. Neither outlet published the content of the documents, a responsible decision by the two newsrooms to avoid facilitating the leak of information obtained through nefarious means and abetting a foreign state-sponsored interference operation. The Trump campaign attributed the hack to Iran, which the US Office of the Director of National Intelligence (ODNI) ultimately corroborated. The ODNI also confirmed Iran has "sought access to individuals with direct access to the [p]residential campaigns of both political parties".

Domestic Actors

Perhaps even more troubling than the explosion of nation states conducting foreign interference operations has been the proliferation of domestic actors within established democracies who have sought to undermine trust in democratic institutions and sow doubt in the integrity of elections. Though some of this domestic activity inherently falls outside the definition of "foreign interference", domestic proxies can and do serve—wittingly or unwittingly—as enablers of foreign state-sponsored operations.

The trend of domestic actors undermining democracy at home has been most acutely felt in the United States, where sitting politicians, candidates for office, and influential figures on traditional and social media have perpetuated falsehoods about election procedures and election results, further polarizing an already fractured body politic.

The United States avoided worst-case scenarios during the 2022 midterm elections. Most candidates for state and national office who ran on a platform of election denialism lost their races and conceded peacefully, and election-related violence and mass voter intimidation did not occur. However, almost a third of the US electorate still falsely believes that the 2020 presidential election was stolen, a conviction rooted in disinformation and arguments that have no evidence to support them. Election officials and poll workers still face serious threats of violence and conspiracy theories about the rigging of elections are pervasive. Tellingly, in 2023 alone, state legislators in 38 US states introduced bills that would make it easier for state governments to overturn election results and make election administration more cumbersome and partisan.

In Europe, widespread election denialism might not have taken root in the same way as in the United States, but the continent suffers from other domestic threats that facilitate foreign interference. Politicians have, at times, served as proxies or enablers of foreign authoritarian state actors, including by amplifying foreign propaganda. Russia's war in Ukraine serves yet again as an illustrative example of this trend. As a 2023 report by the European Council on

Foreign Relations about the Italian political scene stressed, the country has "several major political parties whose leaders have vocally queried and pushed back against measures that aim to curtail Russia's ability to continue to attack Ukraine. … [T]hey disseminate pro-Russian and anti-Ukrainian narratives in four main ways: openly supporting pro-Kremlin narratives; allowing to go unchallenged false information about the war, on sanctions, and energy; ignoring information on the war, sanctions, and energy; and propagating false information relating to the war."

Far more concerningly, the European reality of the last few years has been marked by political forces and leaders who have themselves used an illiberal playbook to weaken the rule of law and democratic institutions from within. The current government in Hungary under Viktor Orbán and the Polish government led by the Law and Justice party from 2015 to 2023 both stand out as key, but not singular, examples of this dynamic. Both gained and retained power through democratic means, but their governments focused overwhelmingly on centralizing their power by fueling polarization, weakening the practical separation of powers, and co-opting the media landscape. Unsurprisingly, these actions had a chilling effect on both countries' democratic health, a trend that continues in Hungary but could be bucked in Poland after the outcome of the last parliamentary election in October 2023. In the United States, the Project 2025 plan driving many of the policy ideas that could shape a second Trump administration adopts elements of the illiberal playbook, notably the desire to capture and politicize state institutions like the Department of Justice. (Trump and his campaign have attempted to distance themselves from Project 2025).

Finally, private-sector actors, motivated predominantly by profit, have become agents of interference operations in democracies. Revelations about different governments reportedly using sophisticated hacking software such as Pegasus, an extremely powerful piece of spyware developed by an Israeli company, for surveillance purposes have become commonplace over the past several years. There has also been a discernible rise in advertising, marketing, public relations, and other firms and contractors that are hired to manipulate information and promote falsehoods, amplify political messages, and meddle in elections at the behest of nation-state clients. Increasingly accessible and cheap technologies have lowered the barriers to entry for these private entities. Gone are the days when security services singularly dominated this field. Furthermore, relying on proxies in the private sector ostensibly creates plausible deniability for nation states to cover their tracks (except when they are caught, a long list that includes the Israeli government, which hired a political marketing firm to carry out information operations targeting US members of Congress and American citizens to shape views on the war in Gaza, as well as the US Department of Defense, which conducted a disinformation campaign in the Philippines to discredit Chinese-manufactured COVID-19 vaccines).

3. New Technologies Facilitate Operations to Undermine Democracy

The AI Era

To launch and sustain their interference offensives, authoritarian nation-state actors have increasingly exploited the global digital and cyber landscape for their strategic advantage, particularly the sudden, spectacular surge of AI-enabled technologies like generative AI. Boosted by these tremendous technological advances, including in "deep learning" techniques, machine translation and large-language models, and computing power and chips that drive and train AI systems, bad actors are already harnessing AI for nefarious purposes, magnifying existing risks and creating new ones.

The ASD AI Election Security Handbook

In February 2024, ASD developed a handbook aimed at election officials in the United States, who face a new challenge in AI amid declining public trust in their work. The handbook seeks to assist election officials in understanding and addressing the potential vulnerabilities AI may introduce, aiming to safeguard the integrity of future elections.

AI-generated deepfakes—hyper-realistic inauthentic audio, image, or video content that complicates the distinction between what is real and what is not—have perhaps been the most public-facing facet of this trend. In countries as diverse as Argentina, Slovakia, the United States, and Bangladesh, among others, such manipulated content has already been deployed in electoral contexts to sow confusion and division, considerably raising the systemic risks of information manipulation and election interference.

Enabling not just the sophistication of inauthentic content, but also its proliferation, AI innovations are helping malign actors produce and spread manipulated information at an unprecedented scale. Any event on the global stage can be used as a hook to do so. In 2024 alone, networks of Russian-linked propaganda bots have deliberately fueled conspiracy theories ranging from the health of members of the British royal family all the way to the completely unsubstantiated allegation of Ukrainian involvement in a terrorist attack in Moscow. In many cases, these malign campaigns have been AI-driven, meaning that they relied on inexpensive tools like large language models to create constant flows of alluring messaging, as well as "armies" of automated accounts and profiles for maximum and optimum amplification.

The low-cost nature and easy availability of these tools on the internet has, in a way, democratized information manipulation as well. It is not just state security services using these tools nowadays to wage interference campaigns against democratic targets. The average citizen now has powerful tools to spread inauthentic content, with potential real-world implications. Even back in the 2016 US election campaign, in the absence of AI tools, teenagers in a small town in North Macedonia created and profited from a torrent of baseless yet highly popular web stories, including sensationalist and often false negative stories about then-presidential candidate Hillary Clinton, using relatively rudimentary technology. Now in 2024, one of the world's leading AI firms identified and disrupted online influence operations involving users in Russia, the PRC, Iran, and Israel who were using its AI tools to deceive and manipulate public opinion and political discourse. There have been meaningful efforts to leverage these very same technologies for good to detect and deter the spread of inauthentic content. Unfortunately, combating this activity has lagged behind its misuse.

Information Laundering

New technologies, including AI, have also facilitated the creation and dissemination of state-of-the-art information laundering campaigns, opening easier pathways for state-sponsored propaganda and mis- and disinformation to bypass restrictions and mask attribution to the content's nation-state origins. The laundering of Russian state-sponsored media is a prime example of how foreign state-sponsored content is repackaged for Western audiences. Employing a nexus of malicious websites, monetization mechanisms, and distribution networks and channels, Russia's aim of information laundering is not simply to better spread and amplify its propaganda, but also to obfuscate the Russian government's connection and circumvent existing restrictions in the West against Russian state content.

Unlike the United States, the EU has formally banned Russian state media, ostensibly making it more difficult for this content to surface in member states' information environments. ASD's research found that Kremlin propaganda still finds ways to get around EU restrictions. Focusing on Poland as a key case study, our analysis uncovered evidence that a small network of Polish news blogs—Lega Artis, News na Dziś, and Daily Blitz—could serve as "pathways for Russian state media and pro-Kremlin media to reach Polish audiences. These sites employ content laundering techniques, automatically reposting stories predominantly sourced from Rossiya Segodnya, a Russian state-owned media conglomerate, and Zero Hedge, a financial blog that has been accused of spreading Russian propaganda."

Using ASD's Information Laundromat tool, our research also highlighted additional pathways through which content from Russian state media website RT.com reaches audiences on both sides of the Atlantic and beyond. Querying hundreds of RT articles, the tool discovered hundreds of domains that republished articles that were identical or nearly identical to those that originated on RT.com. As our May 2024 report explained, "in some cases, these sites were transparent or quasi-transparent about sourcing content from RT; in others, the provenance of the content was opaque or seemingly intentionally masked. [But] [i]n all cases, these sites allowed Russian state media to reach a wider audience, including in the EU."

Our analysis showed that information laundering tactics include faux local news sites and "journalists" amplifying Kremlin propaganda. In several cases, such as the "San Francisco Telegraph" or the "Kigali Daily News", seemingly authentic but fake local news outlets sourced content from RT.com but often attributed the stories to fictitious local reporters with fake profiles. By enmeshing RT content with otherwise innocuous—and truthful—local news stories, these sites tried to enhance their credibility with their readership. Furthermore, our report also confirmed various cases in which restricted RT content was still allowed to proliferate on social media and user-generated video sites.

Looking at popular platforms such as Reddit and YouTube, we found that users were not only able to bypass the existing restrictions, but they were also able to disseminate RT content further by exploiting the "authoritativeness" of these platform domains to ensure such content surfaced in search results on Google and Bing, as well as their news searches.

The Information Laundromat

ASD's newest analytical tool is dedicated to exploring content laundering practices across the web. Launched in spring 2024, it is a lead generation tool used to determine if and how websites share architecture and content. Through its development and use, ASD and its research partners have already uncovered multiple instances and ways through which banned or restricted Russian media context manages to reach its audiences across the transatlantic space.

Other Technological Vectors Facilitating Foreign Interference Threats

The PRC has been especially adept at exploiting emerging technologies either to gain leverage over other countries or to weaken democracy in the process. This trend has been particularly acute in the "Global Majority". ASD published analysis describing how PRC state-owned and private companies weaponized the digital information stack, and its five distinct, yet mutually reinforcing, layers—network infrastructure, devices, applications, content, and governance—in the stacks of five countries in Southeast Asia, Sub-Saharan Africa, and the Caribbean. For instance, in Myanmar, a Huawei app has been used to scan the ID cards of anyone who buys a SIM card. It allows the tech giant with close connections to the CCP to build, and likely preserve access to, a database containing the identification information of an ever-growing share of the population. In Uganda, Huawei has deployed surveillance hardware across the country and aided Ugandan security forces in using it to track political opponents. The PRC is also inspiring and enabling techno-surveillance at a systemic level. Nigerian authorities met with the PRC's Cyberspace Administration in 2021 to explore the possibility of mimicking the country's "Great Firewall". That same year, in the immediate aftermath of the coup in Myanmar, media reported that Chinese technicians had helped the country's junta reinforce its control over the country's internet.

The supply and demand for these PRC technological products and services has not been limited to the "Global Majority". A 2024 Radio Free Europe/Radio Liberty survey of nine Central and Eastern European countries revealed that their respective governments have purchased "millions of Chinese-made surveillance cameras over the past five years, despite the devices' security vulnerabilities and the manufacturers' lax data practices and ties to the Chinese state". In many cases, these systems were found to be present and in use in critical infrastructure and sensitive sites, such as special police headquarters in Hungary and military bases in Romania.

Finally, more traditional technology-enabled offensives, such as cyberattacks, have continued to have far-reaching consequences on numerous facets of democratic life: politics, economies, citizens' data privacy, social services, critical infrastructure and so on. Indeed, ASD's Authoritarian Interference Tracker catalogs more than 100 representative examples of how Russian and PRC state-sponsored cyber operations across the transatlantic space have served to undermine democratic institutions or processes, such as faith in governments, critical infrastructure (including election systems), and civil society actors. The 2023 annual threat report by ENISA, the EU's agency for cybersecurity, presented a European cybersecurity landscape that has witnessed "a significant increase in both the variety and quantity of cyberattacks and their consequences". Juhan Lepassaar, ENISA's executive director, recently confirmed that the trend continues unabated in 2024: "The number of hacktivist attacks (against) European infrastructure—threat actors whose main aim is to cause disruption—has doubled from the fourth quarter of 2023 to the first quarter of 2024."

4. Authoritarian Money is Infiltrating Democracies More than Ever

Malign Financial Threats

Just as state-sponsored actors abuse anonymity and privacy protections to obscure attribution of their information operations, so too do they leverage with malign intent the financial secrecy provisions and vehicles that our laws permit to interfere in democratic elections, destabilize democratic societies, and undermine democratic institutions. Both in the United States and across Europe, Russia has been the primary exploiter of the West's permissive landscape that facilitates covert financing of individuals, parties, and institutions in democracies, although other countries are using these tactics as well. ASD's research into the topic as early as 2020 found that authoritarian regimes spent "more than $300 million interfering in democratic processes more than 100 times spanning 33 countries over the past decade." In 2023, the US Department of State also alleged that Russian state-sponsored actors alone covertly spent over $300 million funneling resources to political parties, officials, and politicians in more than two dozen countries since 2014.

An increasing number of reports and evidence attests to authoritarian regimes' use of money to increase their political leverage and influence. The same 2020 ASD Covert Foreign Money report found that "[b]roader than just money flowing through straw donors, shell companies, non-profits, and other conduits, [these flows of] malign finance include a range of support mechanisms innovated by authoritarian regimes to interfere in democracies, from intangible gifts to media assistance." The European Parliament's 2022 INGE report reflected many of these findings, going one step further by condemning and exposing several high-level former European politicians who, through elite capture and co-optation, had been actively promoting Russian or PRC state interests.

Authoritarian governments and their proxies also take advantage of domestic proxies in democracies to move money surreptitiously, masking links to a foreign state. This is a particularly acute problem in the United States, but also manifests in permissive European jurisdictions like the United Kingdom. ASD's "Regulating the Enablers" report from 2021 describes the many pathways facilitating the corrupting influence of foreign illicit money in the United States. Among others, the report cites real estate transactions, legal proxies, and private equity and hedge funds as vehicles for illicit foreign money. And while the examples involving Russian state-affiliated actors are numerous, the problem is certainly not limited to Russia. The report details how a US-based lawyer laundered $400 million from a Bulgarian cryptocurrency scam by creating fake private equity funds, while a Ukrainian billionaire paid millions in cash to purchase buildings in Midwestern American cities to launder money he stole from a Ukrainian retail bank. These cases are obviously criminal in nature, not tied to foreign interference. But they are indicative of the ease with which savvy foreign actors with ties to a nation state can move money into the United States.

Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies

In a report published in August 2020, it was revealed how authoritarian regimes, notably Russia and the PRC, have spent over $300 million to interfere in democratic processes across 33 countries in the past decade. The report identifies seven key policy gaps exploited by these activities and offers recommendations to close them, ensuring protection of domestic speech rights while advocating for stronger governmental coordination.

Economic Leverage

Foreign adversaries have also been increasingly brazen about the use of economic leverage as a vector of influence and coercion across the transatlantic space. As has been well established, since the very beginning of its war in Ukraine in 2014, Russia has increasingly weaponized European energy dependencies on Russian fossil fuels as an important lever of pressure. Yet the PRC has also been using its economic might to try to pressure other countries to act in ways that advance PRC interests—or face consequences if they do not. The last few years offer several relevant examples in the EU. The most illustrative concerns the 2021 dispute between the PRC and Lithuania in which Beijing launched sweeping retaliatory economic measures against the small Baltic state after Vilnius gave permission to Taiwan to open a de facto embassy there.

Applying economic pressure often takes place in subtler ways too, like threats from PRC officials, even if they do not always lead to drastic, real-world consequences as in the Lithuanian case. In 2020, when Germany considered restricting Huawei from the rollout of its 5G telecommunications networks, the PRC's ambassador to Germany warned that such a decision would bear consequences, including potential countermeasures against key German industries like automobile manufacturing. Similar reactions were observed in other European countries. In 2023, Italy's decision to leave the PRC's Belt and Road Initiative prompted the PRC's foreign policy establishment to issue a threat that the move would impact Italy's "image, credibility, and [bilateral] cooperation".

Russia and the PRC have also leveraged economic dependencies to target and infiltrate civil society institutions to influence public opinion in democracies. A research center on human rights at the Free University of Amsterdam, for example, received significant funding from entities affiliated with the PRC from 2018 to 2020. The center published several posts rejecting Western criticism of the PRC's human rights policy, and academics associated with the center cast doubt about whether discrimination of Uyghurs or other minorities even existed in Xinjiang. Former European Commission President Ursula Von der Leyen highlighted this case as an example of the PRC's interference in Europe in her 2022 State of the Union speech.

5. Destabilizing Democratic Societies Is a Key Authoritarian Objective

Civic concerns in democratic countries, including poor infrastructure conditions, surging inflation, and the cost-of-living crisis, often dominate political debate and understandably preoccupy citizens' attention. Add to the list sensitive—and sometimes explosive—topics like immigration, migration, and election integrity, and there are many issues that could trigger societal instability. The January 6 insurrection attempt in the United States, the Yellow Vests protests in France, and the 2024 anti-immigration protests in the United Kingdom are among the many instances of mass citizen action and protests in the West that have threatened societal stability in recent years.

Authoritarian nation-state actors try to exploit such sensitive issues and events to maximize strife and deepen divisions in democratic societies. Unsurprisingly, the information domain is a primary conduit for their activity. For example, ASD's Hamilton 2.0 Dashboard revealed that during the violent riots that took place during summer 2023 in France, key phrases like "police", "riots", and "Macron" were among the most frequently used in tweets by Russian state-affiliated accounts. Propagandists amplified messages calling the unrest a coup and comparing President Putin's handling of the Wagner rebellion with French President Emmanuel Macron's alleged mishandling of the riots. Similarly, former Russian President Dmitry Medvedev exploited the unrest by stating in French that "the money spent in vain on weapons for the gang of the drug addict Zelenskyy could have been useful to ordinary French people". These attempts to influence views in France were likely not overly successful, but they are indicative of how the Russian propaganda apparatus immediately seized on a critical inflection point in a key European country to attempt to fan the flames of instability when French citizens were rioting in the streets.

Authoritarian Interference Tracker

ASD's Authoritarian Interference Tracker documents the extensive efforts of the Russian and PRC governments to undermine democracy across more than 40 countries within the wider transatlantic space since 2000. The tracker identifies and groups incidents according to five primary tools used, including information manipulation, cyber operations, malign finance, and economic coercion. Civil society subversion is a key aspect of interference that is tracked, detailing more than 200 examples of relevant attempts and showcasing how expansive these efforts are.

It does not require a citizen movement or protest to persuade authoritarian actors to attempt to foment instability in a democratic country. Ahead of the 2024 Paris Olympic Games, there were reported attempts to suppress attendance and heighten security concerns around the city. A special Microsoft Threat Intelligence report released in June 2024 observed "a network of Russia-affiliated actors pursuing a range of malign influence campaigns against France, French President Emmanuel Marcon, the International Olympic Committee (IOC), and the Paris Games." Like tactics described in previous sections of this report, these actors often impersonated existing media outlets to mislead the public by disguising disinformation as coming from reputable sources. In one case, Russian influence actors, purporting to be the media outlet Euronews, falsely claimed that "Parisians were buying property insurance in anticipation of terrorism surrounding the Games", clearly trying to fuel a narrative of insecurity and instability. In a separate incident, Russian influence actors masqueraded as French broadcaster France24 to claim that a sizeable portion of tickets for Olympic events "had been returned due to fears of terrorism". Related cases abound and are systematically cataloged by ASD's Authoritarian Interference Tracker.

Beyond the information domain, operations aimed at destabilizing societies have also taken on kinetic dimensions. Following the Hamas attacks in Israel on October 7, 2023, French intelligence services expressed their strong suspicion that Russian state actors were behind a graffiti campaign in Paris in which Stars of David were painted around the city. Similarly, French authorities are investigating whether a similar vandalism attack on a Holocaust memorial was conducted on the order of Russian security services. This year, German and Czech authorities alleged that Russian security services planned sabotage and arson attacks in the two countries. In Germany, two German-Russian dual nationals allegedly plotted strikes against US military bases, among other sites, and a third-country national had plans to set fire to a bus depot in Czechia.

There have also been brazen assassination attempts. A Russian government plot to kill the CEO of German defense company Rheinmetall, a major supplier of arms for Ukraine, was fortunately foiled. The Kremlin's goal, besides revenge, was most likely to shake the German public's support for Ukraine's self-defense. The US government claimed it had intelligence linking the Iranian state to a plot to assassinate former President Trump, though it is worth noting that there is no link between this reported plot and the would-be assassin who actually attempted to kill the former president at a rally in Butler, Pennsylvania. The Iranian regime was no doubt bent on revenge against Trump after his administration proved to be particularly hawkish on Iran. Yet it likely wanted to shake Americans' confidence in the election and government institutions as well, and perhaps even fuel suspicions about a "deep state" hand in the assassination attempt. In the West, Russian assassination attempts have also been a key part of its transnational repression activities, or the pursuit of perceived enemies of the state beyond Russia's borders. Incidents include the murder of Chechen separatist commander Zelimkhan Khangoshvili in Berlin, Germany and the near-fatal poisoning of former Russian intelligence officer Sergei Skripal and his daughter Yulia in Salisbury, England. Here too, revenge fuels attempts to shake societal stability and confidence in public institutions and safety.

Conclusion

Authoritarian regimes have concluded that interference operations are, by and large, easy, cheap, and effective ways to attempt to undermine democracy beyond their borders. The trends and tactics described in this report paint a disturbing picture. Democracies now face threats from an increasing number of nation-state actors that are adapting their tactics to stay ahead of defenses, learning from one another, and exploiting technological advances. Equipped with sharper tools and greater confidence, they are waging more targeted campaigns at all levels of democratic politics and all sectors of democratic society.

If there is a bright side, it is that most democracies are at least somewhat more prepared to address these threats than ever before. In the United States, the federal government is better organized to track foreign threats to US democracy and elections than it was in 2016 or even in 2020. The US Intelligence Community now has a dedicated center for tracking foreign malign influence, drawing on civil service professionals with varied backgrounds. The federal government, particularly the Department of Homeland Security, provides resources to state and local officials to protect US election infrastructure from foreign interference campaigns. Some states, including Arizona, have been pioneers as well, recognizing the potential for foreign and other malign actors to use AI tools to destabilize election integrity and preparing early in the 2024 election cycle to defend against these threats.

Other countries have provided models for allies and partners either to adopt or consider when formulating a strategic response to foreign interference threats. Canada's government protocol to communicate election interference threats with the public has informed related procedures in other governments, including in the United States. The EU created a legislative model for addressing threats in the digital domain, most notably the much-touted AI Act, the first comprehensive set of horizontal regulations for the AI industry at a global level, and the Digital Services Act, the bloc's ambitious bid to regulate online platforms. The creation of specialized agencies, such as France's Viginum, to detect and protect against foreign digital interference, has been instrumental in attributing foreign interference operations to nation-state actors and raising public awareness about these threats. Meanwhile, the recently established FIMI Information Sharing and Analysis Centre announced by the European External Action Service could serve as a meaningful multi-sector body that allows key civil society representatives a platform for analyzing and exchanging critical threat information.

In other sectors of democracies, efforts to defend institutions, elections, and societies from foreign interference threats have been galvanized. Certain corporations have published detailed accounts of adversaries' tactics and attributed attacks to nation-state actors. In doing so, they have brought public attention to operations in specific ways that governments are sometimes reluctant to do. Other companies have taken down networks of malign activity on their platforms, shutting down avenues for foreign interference even if new ones inevitably materialize. The list of think tanks and NGOs involved in tracking foreign interference threats, policy development work, and resilience-building efforts in local communities has increased dramatically. Finally, the mainstream media has learned lessons from some of its previous shortcomings by reporting more responsibly on these threats and avoiding amplification of foreign nation-state interference activities. The US media's refusal to publish the contents of a purported Iranian “hack-and-leak” operation targeting the Trump campaign in August 2024 is one noteworthy example of responsible journalism on these contentious issues.

This is not to argue that there is no work left to be done. Many vulnerabilities in democracies continue to facilitate interference operations. Some governments are not organized to address these threats from an intelligence or policy standpoint in a holistic, coordinated manner. Politicization of the foreign interference issue also adversely affects countries’ ability to respond. In the United States, forging bipartisan consensus to shut down avenues of malign activity has been fraught and fought largely in the public eye, undermining Americans’ confidence in the US government and raising doubts about whether interference threats matter at all. But it has also been visible in Canada, where political infighting over a public inquiry into PRC-backed interference in previous election cycles has taken up more political and media oxygen than any serious policy discussion to defend against and deter future foreign interference operations.

Meanwhile, the information space continues to fragment into smaller communities spread across numerous platforms. Worse, many of the corporations that operate these platforms now choose to leave them unregulated in ways that invite foreign actors to ramp up their interference activity, or they loosely enforce corporate policies and terms of service that do little but slap a bandage on a metastasizing problem. Civil society remains committed to conducting the democracy-affirming work at the local level that is desperately needed to build societal resilience to foreign interference threats. Yet, in most cases, it remains underfunded and in some national environments, particularly the United States, organizations and individuals that track information operations have come under political scrutiny—and physical threats—for allegedly censoring conservative voices. Unjustifiable as many of those allegations are, they have had a chilling effect on the research community, as some initiatives have shut down entirely while others have seen funders walk away from them.

Finally, polarization in democratic societies exacerbates several of these challenges. Different segments of the public get their version of the truth from radically different news sources, and reaching consensus on facts is a tenuous exercise. These are problems that democratic societies have created themselves, but foreign nation-state actors readily exploit them to conduct foreign interference operations, amplifying discord and distrust in almost all aspects and layers of democratic life, including governments’ ability to govern, election officials’ intention to facilitate free and fair elections, and the media’s reliability in providing trustworthy information.

This report makes clear that a multiplying body of adversaries has every intention of continuing to conduct interference operations against our democracies. There has indeed been greater transatlantic resolve to understand the threat, better prepare for it, and take action to address it. But there is much work to be done across sectors of society to create more hardened and forward-looking defenses against—and resilience to—this rapidly evolving threat.

About the Alliance for Securing Democracy at GMF

The Alliance for Securing Democracy (ASD) at the German Marshall Fund of the United States is a non-partisan initiative that exposes, analyzes, and develops strategies to counter foreign information manipulation and interference in democracies. ASD leverages its data and expertise to provide sharp analysis and actionable recommendations to counter these threats to relevant public and private sector actors. With staff in Washington, D.C. and Brussels, ASD translates lessons learned from countries' experiences addressing foreign information manipulation and interference for key stakeholders on both sides of the Atlantic—and, increasingly, around the world. ASD also aims to be a force multiplier, partnering with likeminded organizations to strengthen resilience among democracy's most crucial asset—the citizenry.

securingdemocracy.gmfus.org

About the Authors

Vassilis Ntousas

Vassilis Ntousas is the senior manager and fellow for Europe for ASD at GMF, where he serves as the lead in-house expert on European foreign policy and European efforts to defend and advance democracy within and beyond European borders. Prior to joining the ASD, he was the Senior International Relations Policy Advisor at the Foundation for European Progressive Studies in Brussels, where he led the foundation's global research, advocacy, and strategic convening work. In 2019–2020, he held the Stavros Niarchos Foundation Academy fellowship at Chatham House. He is the author of several policy papers and regularly comments on global affairs for international media outlets. He is also the co-editor of two books published by Routledge, The European Union and China's Belt and Road: Impact, Engagement and Competition (2021) and EU Climate Diplomacy: Politics, Law and Negotiations (2018).

David Salvo

David Salvo is a senior fellow and co-managing director of ASD at GMF, where he has worked since 2017, previously as a resident fellow and later as a deputy director. An expert in Russian affairs, Salvo has been analyzing the Kremlin's authoritarian toolkit to undermine democracy at home and abroad throughout his career. He is the principal author of the ASD Policy Blueprint for Countering Authoritarian Interference in Democracies and regularly comments to US and international media outlets on issues such US-Russian relations, Russian foreign policy toward its near abroad, and foreign tactics and objectives to undermine democracy in the United States and Europe. Prior to joining GMF, Salvo was a foreign service officer in the US Department of State, serving most recently as the deputy secretary of state's policy advisor for Europe, Eurasia, and international security issues. He also advised senior-level State Department negotiators on the protracted conflicts in the South Caucasus, worked on US policy toward NATO and the Organization for Security and Cooperation in Europe, and served overseas in Russia and Bosnia and Herzegovina.

Disclaimer

The views expressed in GMF publications and commentary are the views of the author(s) alone.

As a non-partisan and independent research institution, The German Marshall Fund of the United States is committed to research integrity and transparency.

Acknowledgments

The authors would like to extend grateful thanks to Rita Barbosa Lobo and Louis Savoia for their inputs and support to the success of this project. Many thanks are also owed to Rachael Dean Wilson, Bret Schafer, Josh Rudolph, Etienne Soula, and Peter Benzoni for their thoughtful comments and suggestions.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of the Second World War, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

gmfus.org