CYBER STATECRAFT INITIATIVE

DFRLab

Atlantic Council
SCOWCROFT CENTER FOR STRATEGY AND SECURITY

ISSUE BRIEF

Targeting Ukraine Through Washington: Russian Election Interference, Ukraine, and the 2024 US Election

MARCH 2022 GAVIN WILDE AND JUSTIN SHERMAN

EXECUTIVE SUMMARY

The Russian government has launched an illegal, aggressive, large-scale invasion of Ukraine. In the leadup to war, the British government and the Joe Biden administration accused the Vladimir Putin regime of a plot to install a pro-Russian government in Ukraine, accompanied by information operations to provide a pretext for military incursion. These and other events remind that, for Putin, controlling Ukraine is a deep-seated desire—and, broadly speaking, one the United States must watch. In the aftermath of Moscow's wide-ranging attempts to influence the outcome of the 2016 US presidential election cycle, US officials and media trained their focus on the immediate impacts to electoral infrastructure, on potential conspiracy by US citizens, and on the methodology behind Russia's "active measures." The partisan fervor attending this focus—from the Robert Mueller investigation to the (first) impeachment trial of President Donald Trump—has obscured a common thread also woven throughout Moscow's assaults on the US political system over the past seven years: reversing Ukraine's drift away from Russia following the 2014 Maidan Revolution and discrediting the movement's backers in Kyiv and Washington. This issue brief describes Russia's interest in Ukraine as it interfered in past US elections, why the current state of play might shape interference in the 2024 US elections, and what policymakers must watch. It makes three core recommendations: implement the legislative reforms to foreign espionage, agents, and lobbying disclosure laws recommended in the Senate's bipartisan review of the 2016 election; watch the Putin regime's war on Ukraine and identify any new cyber and information tactics; and intensify the practice of public intelligence disclosures concerning Russian covert influence activities and Russian cyber and information operations.

INTRODUCTION

The Russian government has launched an illegal, aggressive, large-scale invasion of Ukraine. In the leadup to war, the British government and the Biden administration accused the Putin regime of a plot to install a pro-Russian government in Ukraine, accompanied by information operations to provide a pretext for military incursion.[1] "We have information that the Russian intelligence services maintain links with numerous former Ukrainian politicians," the London press release stated, noting that "the former Ukrainian MP Yevhen Murayev is being considered as a potential candidate." All of this comes alongside heightened Russian intelligence activity in Belarus and Ukraine, which reminds that, for Putin, controlling Ukraine is a deep-seated desire—and, broadly speaking, one the United States must watch.

History is a guide here. In the aftermath of Moscow's wide-ranging attempts to influence the outcome of the 2016 US presidential election cycle, US officials and media trained their focus on the immediate impacts to electoral infrastructure, on potential conspiracy by US citizens, and on the methodology behind Russia's "active measures." The partisan fervor attending this focus—from the Robert Mueller investigation to the (first) impeachment trial of President Donald Trump—has obscured a common thread also woven throughout Moscow's assaults on the US political system over the past seven years: reversing Ukraine's drift away from Russia following the 2014 Maidan Revolution and discrediting the movement's backers in Kyiv and Washington.

Most Western media coverage of the 2016 election focused on Moscow's efforts to exploit divisions in the United States, and for plenty of good reasons. In 2020, Kremlin-linked influence efforts were again cast primarily through bilateral and partisan prisms. Yet, as Moscow ratchets up military pressure to foreclose upon the westward tilt Ukraine's Maidan movement symbolized, US officials should recognize—drawing from the broad compendium of publicly available intelligence, law-enforcement, congressional, and investigative-journalist reviews—that Ukraine's trajectory has always been a centerpiece of Russian interference in US elections. Doing so should guide US policymakers' observations of what is happening now in Ukraine—and their preparations for what promises to be a climactic 2024 US election cycle.

This brief makes three core recommendations:

- Implement the legislative reforms to foreign espionage, agents, and lobbying laws recommended in the Senate's bipartisan review of the 2016 election;
- Watch the Putin regime's war on Ukraine and identify any new Russian cyber and information tactics; and
- Continue to invest in public intelligence disclosures concerning Russian covert influence activities and Russian cyber and information operations, where possible.

1 "Kremlin Plan to Install Pro-Russian Leadership in Ukraine Exposed," UK Foreign, Commonwealth & Development Office, press release, January 22, 2022, https://www.gov.uk/government/news/kremlin-plan-to-install-pro-russian-leadership-in-ukraine-exposed; Julian E. Barnes, "U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion," *New York Times*, February 3, 2022, https://www.nytimes.com/2022/02/03/us/politics/russia-ukraine-invasion-pretext.html.

UKRAINE, THE INTERNET, AND MOSCOW'S STRATEGIC VIEW

Since its formal vote for independence on December 1, 1991—which every region (or oblast) favored, including those in the Donbas and Crimea—Ukraine has struggled to be seen as a fully sovereign state in the eyes of leaders in Moscow. For Boris Yeltsin, consolidating power over post-Soviet Russia and prevailing over his rival, Soviet Premier Mikhail Gorbachev, accepting Ukrainian independence was a necessary, if unpalatable, step. Both Yeltsin and his successor, Putin, used every bit of leverage at their disposal to essentially subordinate Ukraine to Moscow's whims—including via the Commonwealth of Independent States (CIS), in which Kyiv suspended participation in 2018, citing Russian aggression. The 1994 Budapest Memorandum—under which Ukraine relinquished the Soviet-era nuclear arsenal in its territory in return for security guarantees from Washington and Moscow—was as much an expression of trepidation about Russia's intentions as it was an altruistic step toward nonproliferation. Putin's later designs for a Eurasian Economic Union that included Ukraine, and the strategic value of the Black Sea port of Sevastopol for the Russian navy, served as ulterior motives for his claims that "Russians and Ukrainians [are] one people—a single whole."[2]

Moscow's efforts to exert control over its independent neighbor extended to the media space as well. Russia's 2009 State Security Strategy outlined a singular "common information sphere" to encompass the CIS and consolidate influence over the Russian-speaking communities of the entirety of the former Soviet space. By 2013, this drive was not confined to television programming, but extended to the Internet—including a then-obscure "troll farm" based in Saint Petersburg. As the Maidan unfolded in early 2014, online trolls were "just one part of a massive propaganda campaign the Kremlin [had] unleashed…Russian state TV endlessly assert[ed] that Kyiv's interim government [was] under the thumb of 'fascists' and 'neo-Nazis' intent on oppressing Russian-speaking Ukrainians and exert[ed] a mesmerizing hold on many in the country's southeast, where the channels [were] popular."[3]

In Ukraine, as elsewhere, the Internet and "cyber" broadly have played key roles in the Kremlin's approach to influence, sabotage, subversion, and conflict. As Chatham House's Keir Giles explains, "the Ukraine conflict has provided clear demonstrations of how Russia sees cyber activity as a subset, and sometimes facilitator, of the much broader domain of information warfare."[4] The Internet, as discussed later in this brief, has been a key vector of organization, mobilization, and information dissemination for Ukrainians working to build and improve their country's democracy. Simultaneously, the Kremlin has viewed Internet-entangled events in Ukraine (and elsewhere) with intense suspicion, and it has leveraged the Internet to try to shape those events as much as possible.

Moscow's conceptual approaches to the Internet are importantly different from those in the West, in several dimensions. The Russian government has long seen the Internet as both a threat to regime security and an ecosystem to be leveraged against Russia's enemies. When it saw free speech and mobilization via the Internet in the last two decades, it saw threats to the regime's ability to control the flows of information at home and abroad: from independent blog coverage of the Russo-Georgian War in 2008; to protests against Putin's election rigging and return to the presidency in 2011 and 2012, heavily organized on Russian platform VK; to Ukraine's Maidan Revolution in 2014 (discussed more below). Simultaneously, the Kremlin has leveraged—and Russian military doctrine has increasingly recognized—the Internet as a way to enhance and expand Russia's portfolio of political-warfare activities.[5] Distributed denial-of-service (DDoS) attacks that knocked Estonian government websites

2 "Article by Vladimir Putin 'On the Historical Unity of Russians and Ukrainians,'" President of Russia, July 12, 2021, http://en.kremlin.ru/events/president/news/66181.

3 Max Seddon, "Documents Show How Russia's Troll Army Hit America," *Buzzfeed News*, June 2, 2014, https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america.

4 Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, November 2016), https://www.ndc.nato.int/news/news.php?icode=995.

5 Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Washington, DC: Georgetown University Press, 2019).

offline, intrusions that turned off Ukraine's power grid, and military intelligence operations against investigations into the Skripal poisonings were all situations in which the Russian government used cyber means to pursue its political goals.[6] Western democracies have recently arrived at the idea that the Internet presents both serious opportunities and serious risks, but the Russian government has long realized and internalized this idea.[7]

To the Russian government, there is also far less distinction than in the United States and Europe between data and information. In other words, many Western countries make firm distinctions between ones and zeros readable by machines (data) and content readable by humans (information). Much Russian thinking does not quite make this same distinction, with the broad concept of "information security" encompassing not just firewalls, hacking, and other activities and technologies oriented around code—but also information flows generally, and the idea of social, political, and moral stability online (aka regime security). Thus, while the United States and other Western democracies often orient their analyses of Russian operations around distinctions between hacking into targets and spreading disinformation, for example, Moscow often views these tactics as under the same umbrella. It is precisely the point that DDoS attacks to knock websites offline, hack-and-leaks of government communications and political campaign documents, and disinformation spread through social media posts, RT broadcasts, and websites are blended at once.

Finally, there is much attention in the US policy and academic discourse on the idea of "cyber war" and whether certain actions in cyberspace do or do not constitute an act of war. While there are versions of these conversations in Russia, from the Kremlin's perspective, there is immense benefit in the fact that many cyber operations are perceived as below the threshold of armed conflict. It fits into a long history of Russian "active measures" or political warfare, including leveraging assassinations, propaganda, disinformation, front groups, nonstate proxies, and even the funding of terrorism to attack, kill, or silence critics and to subvert, sabotage, and influence for the state's benefit. The Russian government also perceives much value in operating in this "gray zone" because it frequently sees Western countries responding relatively weakly, or not at all, to these gray zone measures.

SECOND SECOND CHANCES

Significant portions of Moscow's current thinking—and, subsequently, its information operations conducted against US elections—stem from incremental movements toward democratic reform and European integration in Ukraine, which have solidified Putin's commitment to reasserting influence over the country. Simultaneously, these movements catalyzed the Kremlin's paranoia about the Internet as a US tool of influence and global power projection.

In 2004, a protest-fueled revote on Ukraine's fraud-riven presidential election swept a reform-oriented administration into power in Kyiv. This dramatic turn was dubbed the Orange Revolution, noting the color of the banner under which reformists rallied.[8] The loss by Moscow's preferred candidate, Viktor Yanukovych—whose initial claims of victory were widely disputed—left his party and the oligarchs who backed it looking for ways to reclaim the initiative. For outside assistance, they turned to a US political consultant named Paul Manafort. Already well connected via his ties to Kremlin-linked metals tycoon Oleg Deripaska, Manafort proved an asset to Yanukovych's ultimate re-ascension to the Ukrainian presidency in 2010 (a decisive blow to what little reformist momentum remained—or so many thought).[9]

Yanukovych's presidency was marred by corruption and incompetence, personified by a circle of party bosses and oligarchs who held sway over the country's economy through rent extraction; their ties to the Kremlin lent Moscow significant sway over the country's political future. By late February 2014, however, long-simmering popular dissatisfaction with these

6 Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC, April 27, 2017, https://www.bbc.com/news/39655415; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Luke Harding, "How Russian Spies Bungled Cyber-Attack on Weapons Watchdog," *Guardian*, October 4, 2018, https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog.

7 For more on these issues and this history, see: Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars for the Internet* (New York: PublicAffairs, 2015); Julien Nocetti, *"Digital Kremlin": Power and the Internet in Russia* (Paris: Institut Français des Relations Internationales [French Institute of International Relations], 2011), https://www.ifri.org/sites/default/files/atoms/files/ifrinocettirussianwebengmars2011.pdf.

8 Peter Dickinson, *How Ukraine's Orange Revolution Shaped Twenty-First Century Geopolitics, Atlantic Council*, November 22, 2020, https://www.atlanticcouncil.org/blogs/ukrainealert/how-ukraines-orange-revolution-shaped-twenty-first-century-geopolitics/.

9 Anton Troianovski, "'Whatever He Wants': Inside the Region Russian Oligarch Oleg Deripaska Runs Like a Personal Fiefdom," *Washington Post*, February 15, 2019, https://www.washingtonpost.com/world/europe/whatever-he-wants-inside-the-region-russian-oligarch-oleg-deripaska-runs-like-a-personal-fiefdom/2019/02/15/c00f7e10-1e61-11e9-a759-2b8541bbbe20_story.html; Josh Kovensky, "In Manafort's World, Everyone Had a Price," *Kyiv Post*, October 12, 2018, https://www.kyivpost.com/ukraine-politics/in-manaforts-world-everyone-had-a-price.html.

dynamics reached a boiling point. Yanukovych's reversal of a long-anticipated association agreement with the European Union (EU) sparked a mass revolt, only further inflamed by his orders to security services to massacre peaceful protesters.

The information environment had changed drastically since the Orange Revolution. In 2014, Ukrainians used Internet technologies to assist with organizing protests, including a widely viewed EuroMaidan Facebook page and the Twitter accounts @EuroMaydan and @EuroMaydan_eng (the English version).[10] The heavy use of US Internet platforms only deepened Putin's suspicion—accelerated during the Arab Spring—that Facebook, Twitter, and the like were merely tools of US power projection, used to undermine Russia and its near-abroad interests.

Yanukovych ultimately fled, taking exile in Russia. From a safe remove, he likely pondered how contacts like Manafort might once again prove useful. Manafort's fortunes at that moment, however, were grim. His business ventures in Ukraine, bankrolled by Deripaska, had not panned out. Continually hounded by one of Deripaska's deputies—a former Russian operative and arms dealer named Viktor Boyarkin—Manafort likewise pondered his next move.[11] Absent a financial windfall, he needed something he might barter to satisfy the debt.

Meanwhile, Moscow's burgeoning online disinformation efforts—which had initially focused on delegitimizing Russian oppositionists—turned their sights on the post-revolution government in Kyiv.[12] As General Phil Breedlove told the 2014 NATO Wales Summit regarding Ukraine, "Russia is waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[13] Indeed, as the first Special Counsel Robert Mueller's report on Russia's 2016 election interference would later note, it was 2014 when the infamous Internet Research Agency began focusing on the United States.[14] Legitimate-looking "news" outlets serving as fronts for Russian security services laundered narratives designed to smear and discredit newly-elected Ukrainian President Petro Poroshenko and his administration, and the Barack Obama administration which supported them—foremost then Vice President Joe Biden.[15] For example, in summer 2015, an obscure website featuring foreign affairs commentary of dubious provenance—called "South Front," and later revealed to be a front for the Russian Federal Security Service (FSB)—ran a think piece under the byline of (an otherwise unpublished) Kalvin Burris, alleging that "the CIA had its hands all over" the Maidan Revolution.[16] The piece highlighted the appointment of Biden's son, Hunter, to the board of Ukrainian energy concern Burisma. Thus, the early seeds of an influence campaign were planted.

The eighteen months following the Maidan Revolution would prove fateful. Russian forces would annex Ukraine's Crimean Peninsula and back separatists in its easternmost enclaves. They would down a civilian airliner, killing nearly three hundred. The United States and EU would unleash punitive sanctions on Russian officials and entities. The ruble would crash. A Western-leaning government would enact major reforms in Kyiv—including cementing Ukraine's split from Russia in political, religious, linguistic, and cultural terms. And the 2016 US presidential election cycle would begin to take shape.

---

10 Tetyana Bohdanova, "How Internet Tools Turned Ukraine's #Euromaidan Protests into a Movement," Global Voices, December 9, 2013, https://globalvoices.org/2013/12/09/how-internet-tools-turned-euromaidan-protests-into-a-movement/.

11 Simon Shuter, "Exclusive: Russian Ex-Spy Pressured Manafort Over Debts to an Oligarch," *Time*, December 29, 2018, https://time.com/5490169/paul-manafort-victor-boyarkin-debts/.

12 Ben Nimmo and Aric Toler, *The Russians Who Exposed Russia's Trolls, Atlantic Council*, March 8, 2018, https://medium.com/dfrlab/the-russians-who-exposed-russias-trolls-72db132e3cd1.

13 Peter Pomerantsev, "Russia and the Menace of Unreality," *Atlantic*, September 9, 2014, https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

14 Robert S. Mueller, III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election: Volume I of II," US Department of Justice, March 2019, 4, 19, https://www.justice.gov/archives/sco/file/1373816/download.

15 "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem," US Department of State, August 2020, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf; Matt Spetalnick, "Biden's Role on Ukraine Underscores Risks for his Political Future," Reuters, March 11, 2014, https://www.reuters.com/article/us-ukraine-crisis-biden-analysis/bidens-role-on-ukraine-underscores-risks-for-his-political-future-idUKBREA2A1XX20140311.

16 "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," US Department of the Treasury, press release, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0126; Kalvin Burris, "Understanding Obama Foreign Policy," SouthFront, July 5, 2015, https://southfront.org/pdf.php?hash=248&code=fdd0689b93c7a2c5bac776a236969a42.

AN INSIDER, A PLAN, A PLATFORM

Russian investigative journalist Andrei Soldatov notes, "[a] distinguishing feature of Russia's intelligence services is their lack of interest in mass movements and the activity on the street in favor of a total focus on the corrupt elites holding power. This is based on the old idea that 'if we control the shah, we control the country.'"[17] With options now limited in Kyiv, entrepreneurial actors were on the hunt for access, influence, and leverage.

By early 2016, a twist of fate had improved Manafort's lot. Having been tapped as chief strategist on the campaign of then candidate Donald Trump, he saw an opportunity to make amends with his creditor. He asked one of his longtime employees, Konstantin Kilimnik, a Russian national with close ties to Yanukovych and his circle—as well as to Russian intelligence, per the FBI—whether Deripaska had been made aware of this newfound role.[18] Even more importantly, Manafort wanted to know "how do we use [it] to get whole?"[19]

While pursuing shuttle diplomacy between debtor and creditor, the opportunity to "make whole" another patron—Yanukovych—was not lost on Kilimnik, judging from Mueller's report. After a matter of months, Kilimnik met with Manafort in New York City with a message from the exiled former president in hand: candidate Trump should endorse a "backdoor" plan to ensure Moscow's control over eastern Ukraine—Yanukovych's home turf. In return, Yanukovych would ensure Trump an audience "at the very top level" in Moscow.

By the time of the Republican National Convention in summer 2016, serious discussions were ongoing about the level of support for Ukraine in the party platform, while Manafort directed internal campaign polling data be relayed to Kilimnik, who, according to subsequent US sanctions findings, passed it along to Russian intelligence.20 Its onward use from that point remains an open question. Among others, the data could be used to: profile individuals the Russian intelligence services could approach, intimidate, blackmail, or coerce; profile individuals the Kremlin might coopt; and micro-target online advertisements related to the election, Russia, and other issues (like Ukraine).[21]

2020: A NEW OPPORTUNITY

Extensive investigations into the span of Russian state-backed efforts targeting the 2016 elections detail that Kilimnik's scheme was but one of several linked to Russian intelligence services and their range of assets—both human and technical. However, his specific line of effort was doomed before it got off the ground. Increasing media scrutiny of Manafort's foreign entanglements resulted in his ouster from the Trump campaign mere months after his entry; Russia intrigue would dog the president's entire tenure in office; Washington's policy of military and political aid to Ukraine would intensify; peace talks to defuse military clashes in Russia-backed separatist enclaves in eastern Ukraine stalled; and a reform-minded political novice, Volodymyr Zelensky, rose to the presidency in Kyiv. Kilimnik evidently determined to regroup and plan for the next big opening.

> "As for the conflict in Ukraine and what's happening there, everyone believes and knows that the people of Ukraine didn't organize this, the people of Ukraine are against this. They're intimidated, forced to follow that path. Organized by the United States."
>
> *Nikolai Patrushev, Secretary of the Russian Security Council, former Director of the FSB (1998–2008), speaking at a February 2022 Russian Federation Security Council meeting*[22]

17 Andrei Soldatov, "The True Role of the FSB in the Ukrainian Crisis," *Moscow Times*, April 15, 2014, https://www.themoscowtimes.com/2014/04/15/the-true-role-of-the-fsb-in-the-ukrainian-crisis-a33985.

18 Jeremy Stahl, "Mueller's Report Sure Makes It Look Like Paul Manafort Was Working with the Russians," *Slate*, April 18, 2019, https://slate.com/news-and-politics/2019/04/mueller-report-paul-manafort.html.

19 Aaron Blake, "'How Do We Use [This] to Get Whole?': The Most Intriguing New Paul Manafort-Russia Email," *Washington Post*, September 20, 2017, https://www.washingtonpost.com/news/the-fix/wp/2017/09/20/paul-manaforts-ominous-email-to-an-aide-how-do-we-use-this-to-get-whole/.

20 Justin Hendrix, "US Treasury Provides Missing Link: Manafort's Partner Gave Campaign Polling Data to Kremlin in 2016," Just Security, April 15, 2021, https://www.justsecurity.org/75766/us-treasury-provides-missing-link-manaforts-partner-gave-campaign-polling-data-to-kremlin-in-2016/.

21 See, e.g., on microtargeting and open data: *Data Brokerage and Threats to U.S. Privacy and Security*, Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth, hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector" (December 7, 2021) (testimony of Justin Sherman), https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf.

22 Svitlana Slipchenko, Valeriia Stepaniuk, and Khrystyna Telehonenko, "Putin's Council of Lies. An Analysis of a Russian Federation Security Council Meeting," *Vox Ukraine*, February 23, 2022, https://voxukraine.org/en/putins-council-of-lies-an-analysis-of-a-meeting-of-the-russian-federation-security-council/.

Reversing the Maidan movement's years of momentum toward integration with the trans-Atlantic community would not be easy. Decisively rendering it illegitimate, and thus reversible, in the eyes of both Ukrainians and Americans would require substantial backing and a support network. When Ukrainians took to the streets in 2013–2014, protesting and ultimately ousting Yanukovych from power, Western media saw one picture: self-motivated citizens organizing, partly via the power of the Internet and social media, to topple dictatorship. The Kremlin saw no such independence. Putin, for a multitude of reasons—including his time in the KGB and his advisers' Cold War-entrenched mindset—does not view opposition movements as legitimate, instead believing they must be the work of a foreign power.[23] The 2010–2012 Arab Spring exacerbated the paranoia of this worldview; to the Kremlin, citizens organizing on regional microblogs, Twitter, and other websites was not a "Twitter revolution" but Washington's hand at work in the shadows, through US social media platforms. Russian protests against Putin's election rigging and return to the presidency in 2011–2012 were likewise met with conspiratorial accusations from Putin that the United States had spent hundreds of millions of dollars to sow protests.[24] When the Maidan movement began in late 2013, relying significantly on the Internet to organize, this only solidified Putin's view of the Internet.[25] Even more so, the global and open Internet became a threat to the Kremlin's interests and a weapon for it to wield against its enemies.

Parochial power struggles and score-settling in Kyiv—both among and between Maidan and pro-Russian factions—had reached fever pitch by 2019. Among the belligerents was Andriy Derkach, a Ukrainian parliamentarian, graduate of the KGB (later FSB) academy, and son of Ukraine's one-time intelligence chief, with family-business ties to Deripaska. According to the US intelligence community, he would also take his cues from the upper echelons of the Kremlin.[26]

Under that purview, Kilimnik, Derkach, and a network connected to the FSB set out to sow discord in bilateral relations between Washington and Kyiv, as well as unsubstantiated allegations of wrongdoing by Maidan-era Ukrainian leadership and the Obama administration, using the 2020 election cycle as a platform. Once again, a US adviser with access to Trump, Rudy Giuliani, served to chum the water.[27] This time, however, he brought the added benefit of media savvy.

Derkach supplied a steady stream of allegations of corruption between the Poroshenko and Obama administrations, offering spurious evidence that hardly supported his vast claims. Among his offerings were leaked recordings of conversations between then Vice President Biden and then Ukrainian President Poroshenko, which to investigators looked suspiciously like they were intercepted by Russian intelligence.[28] A slickly produced "documentary"—portions of which were aired by a fringe US cable-news outlet, OAN—also

23 Mitchell Binding, "What Is 'Technology of The Color Revolutions': Why It Occupies Such a Prominent Place in Russian Threat Perceptions—Analysis," *Eurasia Review,* November 25, 2019, https://www.eurasiareview.com/25112019-what-is-technology-of-the-color-revolutions-why-it-occupies-such-a-prominent-place-in-russian-threat-perceptions-analysis/.

24 Steve Gutterman and Gleb Bryanski, "Putin Says U.S. Stoked Russian Protests," Reuters, December 8, 2011, https://www.reuters.com/article/us-russia/putin-says-u-s-stoked-russian-protests-idUSTRE7B610S20111208.

25 Bohdanova, "How Internet Tools Turned Ukraine's #Euromaidan Protests."

26 "Foreign Threats to the 2020 US Federal Elections," Office of the Director of National Intelligence, March 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

27 Philip Bump, "Whom Rudy Giuliani Is Talking to, What He's Doing—and What Comes Next," *Washington Post*, December 11, 2019, https://www.washingtonpost.com/politics/2019/12/11/what-rudy-giuliani-is-up/.

28 Victor Tregubov, "Why the 'Derkach Tapes' Look Like a Russian Special Op," *Kyiv Post*, September 9, 2020, https://www.kyivpost.com/article/opinion/op-ed/victor-tregubov-why-the-derkach-tapes-look-like-a-russian-special-op.html.

made a range of unfounded claims about the Biden family.[29] Despite Derkach and his circle being exposed and sanctioned by the US Treasury Department for this activity, and their claims being debunked by Ukrainian authorities, several of the narratives were seized upon and propagated by sitting members of Congress and President Trump himself.[30]

Behind the scenes, per US Treasury sanctions filings in 2020, stood the Russian FSB.[31] Putatively a domestic agency, the FSB nevertheless maintained primacy over the Ukraine portfolio, having prevailed over the other Russian intelligence services as they competed over remits of the defunct Soviet KGB.[32] Under Yanukovych, the Ukrainian security services had reportedly "functioned as regional FSB subsidiaries."[33] The FSB's technical surveillance apparatus likely extended throughout the country.[34] When mass protests broke out in November 2013, Russian hackers—whether under the FSB's purview or under its nose—defaced and knocked offline websites critical of Yanukovych.[35] Senior FSB official Sergey Beseda's visit to Kyiv amidst the Maidan protests in 2014 was widely believed to have been the catalyst for Yanukovych's decision to use lethal force against protesters. Yanukovych's ouster was followed by the lustration of Russia-friendly figures from ruling circles in Kyiv, depriving Moscow of high-level insight into, and leverage against, Ukrainian leadership.[36]

The determination of the Yanukovych circle and the FSB to reclaim the political capital lost in connection with the Maidan—the former in Kyiv, the latter with the Kremlin—only intensified. Moscow simultaneously became more and more interested in shaping international policy toward Ukraine, and especially in the United States. As of early 2022, the same cast of characters appears to remain actively engaged in plotting further US election interference.[37]

2024: ANTICIPATING MOSCOW'S MOVES

US policymakers watching further Russian aggression in Ukraine must remember the importance of the Maidan Revolution in the mind of the Kremlin—as London's recent announcement made clear. The Russian government's operations against the 2024 US election cycle will most likely have a considerable Ukraine focus in their narrative. The specifics depend on the next several months, but the Kremlin will seek to exploit the situation no matter the outcome: if Russia aggresses further in Ukraine and Biden does nothing, for example, or if Russia aggresses further and Biden does respond, the Kremlin will weaponize that in its narrative. Ukraine will remain a primary focus in Putin's mind through 2024, and it will very likely be a part of the US election debate.[38]

---

29 Dan Friedman, "Giuliani Allies Were Part of a 'Russia-Linked Foreign Influence Network,' the US Government Says," *Mother Jones*, January 11, 2021, https://www.motherjones.com/politics/2021/01/giuliani-allies-were-part-of-russia-linked-foreign-influence-network-us-government-says/.

30 "Treasury Sanctions Russia-Linked Election Interference Actors," US Department of the Treasury, press release, September 10, 2020, https://home.treasury.gov/news/press-releases/sm1118; Daryna Krasnolutska, Kateryna Choursina, and Stephanie Baker, "Ukraine Prosecutor Says No Evidence of Wrongdoing by Bidens," Bloomberg, May 16, 2019, https://www.bloomberg.com/news/articles/2019-05-16/ukraine-prosecutor-says-no-evidence-of-wrongdoing-by-bidens; Vicky Ward, "Exclusive: Giuliani Associate Willing to Tell Congress Nunes Met with Ex-Ukrainian Official to Get Dirt on Biden," CNN, November 23, 2019, https://www.cnn.com/2019/11/22/politics/nunes-vienna-trip-ukrainian-prosecutor-biden/index.html; Elise Viebeck and Dalton Bennett, "Sen. Johnson, Ally of Trump and Ukraine, Surfaces in Crucial Episodes in the Saga," *Washington Post*, October 28, 2019, https://www.washingtonpost.com/politics/sen-johnson-ally-of-trump-and-ukraine-surfaces-in-crucial-episodes-in-the-saga/2019/10/28/40b9e44c-f684-11e9-8cf0-4cc99f74d127_story.html; Scott Shane, "How a Fringe Theory About Ukraine Took Root in the White House," *New York Times*, October 3, 2019, https://www.nytimes.com/2019/10/03/us/politics/trump-ukraine-conspiracy.html.

31 Mark Galeotti, "The Spies Who Love Putin," *Atlantic*, January 17, 2017, https://www.theatlantic.com/international/archive/2017/01/fsb-kgb-putin/513272/.

32 "Департамент оперативной информации (ДОИ) [Department of Operational Information]," Agentura.ru, last accessed February 14, 2022, https://agentura.ru/profile/federalnaja-sluzhba-bezopasnosti-rossii-fsb/departament-operativnoj-informacii-doi/; Mark Galeotti, "Putin's Hydra: Inside Russia's Intelligence Services," European Council on Foreign Relations, May 2016, https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf.

33 "Юлия Самсонова, «Агенты влияния. Кто управлял Службой безопасности Украины»," Focus.ua, July 3, 2015, https://focus.ua/politics/332609.

34 Alina Polyakova, "Russia Is Teaching the World to Spy," *New York Times*, December 5, 2019, https://www.nytimes.com/2019/12/05/opinion/russia-hacking.html.

35 Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression Against Ukraine*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf.

36 Andrei Soldatov, "The True Role of the FSB in the Ukrainian Crisis," *Moscow Times,* April 15, 2014, https://www.themoscowtimes.com/2014/04/15/the-true-role-of-the-fsb-in-the-ukrainian-crisis-a33985.

37 "Treasury Sanctions Russian-Backed Actors Responsible for Destabilization Activities in Ukraine," US Department of the Treasury, press release, January 20, 2022, https://home.treasury.gov/news/press-releases/jy0562.

38 Julia Davis, "How Tucker Carlson Is Boosting Russia's New Propaganda War," *Daily Beast*, December 30, 2021, https://www.thedailybeast.com/how-tucker-carlson-is-boosting-russias-new-propaganda-war.

The human and bureaucratic architecture of past interference, and efforts to promote Moscow's interests toward Ukraine broadly, also matter for how US policymakers should watch and prepare for the conduct of potential Russian operations in the 2024 cycle. Moscow's 2016, 2018, and 2020 information-operation campaigns primarily relied on state organizations (like the Main Intelligence Directorate (GRU), Russian military intelligence) and state-funded front organizations (like the Internet Research Agency, funded and run by Putin's "chef" Yevgeny Prigozhin). These organizations seldom worked alone, but in tandem with a network of state, state-backed, state-recruited, and otherwise state-linked actors to amplify existing tensions—from Kremlin front companies to security-service cutouts to entrepreneurial oligarchs leveraging ties with insiders (à la Manafort and Giuliani). The Kremlin has even begun outsourcing its troll farms overseas.[39] In similar form, operations in 2024 are likely to leverage this network of proxies for maximum confusion, overlap, and (implausible) deniability.

Much has improved on the US domestic front since 2016 and since 2020, including because of greater press awareness of disinformation and hack-and-leak operations, greater investment in election machine cybersecurity, and the Cybersecurity and Infrastructure Security Agency's work to coordinate election defense across local, state, and federal levels. In many key ways, the United States has built up its defenses against these operations: Cyber Command deploys "Hunt Forward" missions overseas to look for election threats; leaders have taken to preemptively inoculating the public against tactics like "hack-and-leak" operations or forgeries designed to stoke chaos and amplify divisions.[40]

However, the tactics deployed by Moscow and the Yanukovych circle demonstrate key gaps that remain. This brief makes three core recommendations.

- **Recommendation:** Implement the legislative and regulatory reforms recommended in the Senate review of 2016 election interference, which was endorsed on a bipartisan basis. "Unclear laws regarding foreign advocacy, flawed assumptions about what intelligence activity looks like…and the freedom of expression at the root of our democratic society became an opportunity for Russian influence to hide in plain sight."[41] Congress should update legislation on foreign espionage, agents, and lobbying—most of which is rooted in post-war and Cold War-era thinking—to pre-posture for 2024.[42] In tandem, the US intelligence community should update its cyber and intelligence tradecraft to account for increased Kremlin use of dark money, obscure financial webs, and money laundering, as well as the Kremlin's growing use of proxy groups and individuals in third countries to interfere in the US election process.

- **Recommendation:** Watch the Putin regime's war on Ukraine and begin to identify any new Russian cyber and information tactics. There is an immense risk of policymakers fighting the last war: still relying on 2016 as the model for "Russian election interference" and, in that vein, assuming that information operations targeting the US election process will be just about the United States itself. The 2020 election cycle demonstrated that the time-tested "active measures" tradecraft of the KGB era is still effective. The US intelligence community should closely observe developments in the Russia-Ukraine war to understand if the Russian government is leveraging any new cyber or information tactics, operations, or strategies. Already, for example, the Putin regime has enlisted the Alexander Lukashenko regime in Belarus to launch cyber and information operations against Ukrainian military and civilian targets, and this Kremlin use of Belarusian state hackers may not end with the current war.[43] Further, the

39 Taylor Hatmaker, "Russian Trolls are Outsourcing to Africa to Stoke US Racial Tensions," TechCrunch, March 12, 2020, https://techcrunch.com/2020/03/12/twitter-facebook-disinformation-africa-ghana-nigeria-ira-russia/.

40 Shannon Vavra, "Cyber Command Deploys Abroad to Fend off Foreign Hacking Ahead of the 2020 Election," *CyberScoop*, August 25, 2020, https://www.cyberscoop.com/2020-presidential-election-cyber-command-nakasone-deployed-protect-interference-hacking/; Nicole Perlroth and Matthew Rosenberg, "Russians Hacked Ukrainian Gas Company at Center of Impeachment," *New York Times*, January 13, 2020, https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html; Kevin Collier, "Russia-Connected Group Pushed Fake Documents Aimed at Political Flashpoints, Researchers Say," NBC News, April 8, 2020, https://www.nbcnews.com/tech/security/russia-connected-group-pushes-fake-documents-aimed-political-flashpoints-researchers-n1178996.

41 "Volume 5: Counterintelligence Threats and Vulnerabilities," US Senate Select Committee on Intelligence, August 2020, https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

42 Eric Tucker, "FBI, US Agencies Look Beyond Indictments in Cybercrime Fight," *Federal Times*, January 19, 2022, https://www.federaltimes.com/management/2022/01/19/fbi-us-agencies-look-beyond-indictments-in-cybercrime-fight/.

43 Justin Sherman, "The Cyber Conflict Isn't Limited to Ukraine," *Barron's*, March 4, 2022, https://www.barrons.com/articles/the-cyber-conflict-isnt-limited-to-ukraine-51646405827.

US government should try to learn lessons from Ukrainian, NATO, and other informational responses to Russian state disinformation and propaganda during the conflict; those lessons may be helpful in preparing for the 2024 US election cycle.

- **Recommendation:** Continue and intensify the practice of public intelligence disclosures concerning Russian covert influence activities and Russian cyber and information operations, where possible. The US, UK, and Ukrainian governments, among others, publicized several intelligence findings in recent weeks, especially in the leadup to Putin's illegal attack on Ukraine, to expose Russian activities. This drew attention to the Russian government's activities, worked to undermine Russian deniability (for example, concerning the use of undercover Russian Foreign Intelligence Service (SVR) operatives or private military companies like the Wagner Group), and also provided information to social media and civil society organizations in the process. The US intelligence community should continue this pattern and build on its 2016, 2018, and 2020 election track records to keep exposing Russian election interference efforts where it is possible to protect sources and methods in the process.

Recent history clearly highlights the Ukraine theme in Russian election influence efforts, where (shaping) US policy toward Ukraine was of great interest to the Kremlin. Further, that Moscow apparently did not interfere in 2020 on the scale it did in 2016 does not necessitate a lack of activity in 2024. And Russia's possible further aggression in Ukraine underscores that nation's center-stage position in Putin's foreign policy outlook. Particularly if Russia escalates the situation and a prolonged kinetic conflict unfolds, the Russian government's tactics may become more aggressive. If the United States levies sanctions against Russia because of its actions in Ukraine, that could likewise become a central theme of Russian election interference—even if not rhetorically targeting the sanctions, working to stoke divisions or advance ideas or political careers that would reverse or weaken them. The same goes for a scenario in which the United States works with allies in Europe to impose a wider array of sanctions against the Putin regime.

The through lines from Ukraine's revolutions to Russian assaults on US democracy are clear, and demonstrate that the drivers of Moscow's election interference efforts are not confined to bilateral relations; they are also in service of regional objectives. Their trajectory—spurred on by current military tensions—points to a tumultuous 2024 election cycle. For the White House, Capitol Hill, and the interagency, now is the time to prepare.

ACKNOWLEDGMENTS

The authors would like to thank Trey Herr, Liv Rowley, Shelby Magid, and Emma Schroeder for their comments on earlier versions of this document.

ABOUT THE AUTHORS

Gavin Wilde is a managing consultant at Krebs Stamos Group 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.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org