Changing the Kremlin’s Election Interference Calculus

Justin Sherman

To cite this article: Justin Sherman (2022) Changing the Kremlin’s Election Interference Calculus, The Washington Quarterly, 45:1, 112-131, DOI: 10.1080/0163660X.2022.2058186

To link to this article: https://doi.org/10.1080/0163660X.2022.2058186

Published online: 25 Apr 2022.
Since the Russian government’s interference in the 2016 US presidential election, much has changed: dozens of public and private studies have detailed Russia’s playbook of operations; the intelligence community has become more transparent in publicly reporting on the issue; the US has imposed sanctions on dozens of Russian actors involved in the disinformation ecosystem; and technology platforms have spent millions of dollars on misinformation task forces and content guidelines. Yet one thing remains markedly unchanged: election interference is still an incredibly low-cost, high-gain mechanism of influence for the Russian government. The Kremlin has strong incentives to interfere in US elections again. And with Vladimir Putin’s illegal, aggressive, and large-scale war on Ukraine, it is clear that the Putin regime will continue to target other countries it sees as its enemies with wide-ranging means of attack, influence, sabotage, and subversion.

Russian state and state-backed interference in 2016 took many forms, including hacking and leaking campaign documents, building relationships with Trump campaign officials, and spreading disinformation and stoking division on US social media platforms. It is an open empirical question whether those social media posts actually swayed Americans’ voting decisions, and if so, how. The same question could be asked about the media coverage of the leaked Clinton campaign documents, though resulting press coverage was highly critical of Hillary Clinton. Yet assessing modern Russian and even Soviet disinformation purely on this definition of effectiveness misses the
point: these operations are meant primarily to sow and heighten confusion and chaos. For the Kremlin, spending a few million dollars to stoke division during a US election cycle, prompt innumerable news stories on Russian election interference, and generate rhetorical ammunition for Russian President Vladimir Putin’s strongman image (particularly at home) is a great return on investment. The costs are low, and the gains are high.

With Putin seemingly ever-more intent on international aggression, there is an opportunity for the Biden administration to step back and reassess US policy approaches to Russian election interference. Formulating US strategy entirely based on what occurred in 2016 will only doom the US to failure; Russian tactics are always evolving, and even recent information operations on Facebook have seen Russian actors using deepfakes and other new techniques to avoid detection. Repeating the same old responses, like continued sanctions on Russian disinformation groups, does not constitute a comprehensive and effective plan either; these measures have plainly not changed Putin’s calculus to date. Perhaps worst of all, both approaches—focusing too much on 2016 and repeating the same old policy responses—are reactive rather than proactive.

The United States is not going to fundamentally change Putin’s view of the internet and modern information conflict. But Washington should still try to shape Moscow’s election interference calculus to the extent possible. To have a better chance at doing so, the US must look forward and focus on altering the Kremlin’s incentives and ability to act. The first step is understanding the scale and scope of Russian disinformation campaigns and election interference operations, and reflecting on why steps already taken—mainly, sanctions and vague discussions of red lines in cyberspace—likely have not greatly shifted the Kremlin’s incentives to interfere again. Then, policymakers need to focus on a three-pronged strategy that involves continuous intelligence disclosures to undermine Russian deniability and operations; a widespread investment in the public and private sectors on deterrence by denial; and a narrowly tailored diplomatic effort to bolster international norms against election interference and better draw concrete red lines in cyberspace around election infrastructure. Only by arriving at a comprehensive, cohesive, and coherent strategy oriented around Kremlin decision-making can the US hope to have a better chance at shifting the Putin regime’s election interference calculus.

Focusing too much on 2016 and repeating the same policy responses is reactive, not proactive.
Russian Interference Didn’t End in 2016

Moscow’s interference in the 2016 US election is well documented, but what happened after is much less so. The Office of the Director of National Intelligence found in February 2018 that “the 2018 US mid-term elections are a potential target for Russian influence operations.” In April of that same year, Facebook suspended 70 accounts, 138 pages, and 65 Instagram accounts, each controlled by the Internet Research Agency but mostly targeted at Russian speakers in Russia and surrounding countries (i.e., Azerbaijan, Uzbekistan, Ukraine, etc.). By July, however, Facebook reported that it had uncovered dozens of pages and profiles, many linked to Russia, that were created to reach US citizens ahead of the 2018 midterms. In August, it removed hundreds more Russian-originating accounts that were targeting US (and UK) users. That same summer, in a similar move designed to counter ongoing inauthentic behavior, Twitter suspended more than 70 million fake accounts, some of which were tied to Russia (the exact number remains unclear), and deleted 200,000 tweets from Russian proxies.

Then, in October 2018, the Department of Justice charged a Russian national for conspiring “to interfere in the US political system, including the 2018 midterm election.” The sealed charges detailed her management of funds for “Project Lakhta,” the overarching effort funded by Russian billionaire and Putin confidante Yevgeny Prigozhin that encompassed the Internet Research Agency. Project Lakhta had reportedly been using virtual private networks to obscure actors’ locations, creating thousands of accounts on social media platforms and through email, and advocating “for the election or electoral defeat of particular candidates” in both 2016 and 2018, among other actions. The Justice Department stated that the operation internally described the Project’s function as “information warfare” against the United States. Halfway through the Trump administration, the Russian government was still interfering in the US electoral system, a testament to its operations’ broad goal of heightening confusion and division.

On Election Day 2018 itself, independent media later reported, US Cyber Command knocked the Internet Research Agency’s building off the internet to disrupt its trolling—apparently still ongoing—toward the US midterms. Unnamed officials described the operation as a warning to Russia; one unnamed official said it was a way to “throw a little curveball, inject a little friction, sow confusion.” This action was also widely viewed as part of the Defense Department’s recent doctrinal shift towards the concept of active defense in cyberspace—responding to a direct threat in real-time by “kicking the knife out of the hand” of the attackers, so to speak.
In 2020, the Russian government continued to interfere in US politics. “Russia’s intelligence services, Ukraine-linked individuals with ties to Russian intelligence and their networks, and Russian state media, trolls, and online proxies” all targeted the 2020 presidential election in one form or another, according to the Office of the Director of National Intelligence. This targeting included the now-familiar tactics of trying to shape public perception of candidates, undermine confidence in US election processes, and exploit divisions among the US public. Putin described these published US intelligence findings as a “provocation” in December 2020, saying he hoped that then-president-elect Biden would stop engaging in “speculation to tarnish relations between our two countries.” While much attention was paid to the fact that these operations were not as widespread in 2020 as in 2016, Moscow nonetheless continued to interfere, and used a network of state and proxy organizations to that end.

There is still plenty of indication that these activities are low-cost for the Kremlin. While Russian oligarch Yevgeny Prigozhin reportedly budgeted over $35 million from January 2016 to January 2018 for running Project Lakhta’s foreign influence activities, this is pocket change for a billionaire. Far from deterred from further investment, Prigozhin (and, in this case, the Kremlin) has also showcased a readiness to spend more. Justice Department figures indicate that Project Lakhta funds to run information operations may have been allocated at a higher rate in 2018 than in years prior (reportedly over $35 million from January 2016 to June 2018, and more than $10 million alone from January 2018 to June 2018). A 2020 CNN investigation and a 2021 report from the Office of the Director of National Intelligence disclosed that the Kremlin was funding election interference operations based out of Ghana, Nigeria, and Mexico, an expansion of US-targeting troll farms far beyond St. Petersburg. Much of the reporting detailed a similar setup to the Internet Research Agency, the latter of which was a low-cost and efficient enterprise; Internet Research Agency trolls were reportedly paid less than $1,000 a month to run fraudulent online profiles. Further, Kremlin strategists have not had to pour many resources into reworking strategy and procedure for these far-flung outposts: social media platforms have not fundamentally changed their business models since 2016. It is still relatively easy and financially inexpensive for the Kremlin to create false social media accounts to amplify divisive content and spread disinformation.
Moving Beyond the Same Old Responses

Following each major episode of Russian state interference in the American electoral system, the US government response has largely been the same: imposing sanctions and reiterating that such actions violate “red lines” in cyberspace. Neither of these responses has greatly changed the Kremlin’s incentives to interfere again. Sanctions have clearly failed to stop the Putin regime, strategically and operationally, from interfering in elections in the US and beyond. “Red lines” dialogues have similarly failed, in part because the US government often does not go into greater detail on what those red lines are or what will happen when Russia crosses them. Understanding the shortcomings in the current approach will help craft responses that may more effectively alter Kremlin behavior and thereby move the US toward a three-pronged strategy of continuous intelligence disclosures, robust investment in deterrence by denial, and clearly articulated, concrete red lines in cyberspace negotiations.

Imposing Sanctions

The literature on economic sanctions is wide-ranging and reflects continued debates as to their efficacy. With respect to US sanctions on Russia and Russia-linked entities, some call sanctions little more than a signal of displeasure, while others say they will sow discord within elite ranks, break Putin’s contract with the Russian people, or prevent future Russian aggression.19 Others question how much US and other sanctions have actually hurt Russian economic growth,20 including whether that economic pain may hurt the US in the long run by “harming Russians and fueling Putin’s narrative that the West seeks to keep Russia down.”21 However, their opponents argue that sanctioning Russian businesses and individuals for election interference may also help communicate the US position on their unacceptability to the Putin regime.22

The main US response has been sanctions, and Moscow has continued interfering anyway.

Yet, the fact remains that the main US government response to Russian election interference has been sanctions—and that Moscow has continued interfering anyway. The United States has opted for economic and diplomatic sanctions over and over again in recent years. In December 2016, the Obama administration expelled thirty-five Russian diplomats, closed two Russian compounds, and sanctioned two Russian intelligence agencies, four intelligence officers, and three companies that supported hacking operations against the 2016 election.23 The Senate imposed more sanctions in 2017 and
established a review process for any potential Trump-led attempts to weaken or eliminate them. In March 2018, the White House sanctioned nineteen more Russian individuals and five more Russian entities (including the Internet Research Agency) for election interference. The Treasury Department imposed yet more sanctions in December 2018, targeting fifteen Russian intelligence officers and four entities involved in the same influence campaigns. The list goes on.

There is certainly a complicated debate on these sanctions’ long-term effects, and this is not to suggest that they are pointless if used as one part of a multifaceted approach. (Though even if morally important, their current strategic utility vis-à-vis Russia may be limited.) But in the short run, they did not shift Moscow’s calculus on troll farms and election influence and interference operations: the Russian state kept interfering in US politics even amidst a barrage of sanctions. Sanctions levied by the US (especially by the Trump administration) did not create adequate leverage against the Putin regime. It’s even worth noting that some analysts wonder if sanctions work as a deterrent mechanism against Putin at all; Russian-American journalist and intellectual Masha Gessen has referred to the US and other Western countries as acting with delusion on sanctions—always thinking that more of the same will deter Putin the next time around.

**Articulating Vague Red Lines**

Following his June 2021 summit with Putin, President Biden said he had raised a list of sixteen sectors (not publicly specified, though quite possibly the US list of critical infrastructure sectors) that the US wants to see off-limits to Russian cyberattacks. Election infrastructure—whether voting machines, registration databases, or other targets—might very well be on the list (though it is not one of the federal government’s sixteen critical infrastructure sectors). This reflects a continued tendency to respond to Russian election interference by emphasizing its unacceptability and violation of US red lines in cyberspace.

Nonetheless, there is no strong international norm against interfering in democratic elections, and former President Trump’s continued lying about Russian election interference undermined US diplomats’ chances at promoting one. There are conflicting views about if and how election interference should be included in the United Nations’ cyber norms-development process. For now, there is no such comprehensive treatment of these issues in UN cyber norms reports. It is also unclear how election interference sits in international law, and in the United States’ unwillingness to publicly confront its history of covert election interference (e.g., during the Cold War), among other factors, the US has failed to move toward a modern norm against it.
All of this amounts to an international environment in which there is no strong norm against election interference.

The best chance the US had at directly articulating its own red lines on election interference may have been cybersecurity dialogues with Russia immediately following the 2016 influence campaigns. But the Trump administration gutted the US diplomatic apparatus, including sidelining its cadre of experienced cyber diplomats, and weakened the US ability to continue strategic stability and red line talks with Russian counterparts. The Trump White House also consistently lied about Russia’s documented interference in 2016 and undercut, attacked, fired, or otherwise sidelined those raising the issue. Moscow continued interfering all the while. To boot, much of the US conversation on red lines remains vague; there continues to be a persistent belief in the value of strategic ambiguity in cyberspace, and American officials may be reluctant to give Russia specific do-not-cross mandates as a result.

The Russian government is not the only foreign actor interfering in American elections—according to a recent Office of Director of National Intelligence report, the Iranian government did so in 2020 through an influence campaign—but Moscow is certainly the most active. This prolificity necessitates a new, three-pronged US strategy to change the Russian government’s behavior: continued intelligence disclosures, deterrence by denial, and bolstering US red lines in cyberspace. Intelligence disclosures would build on a now-established track record of exposing Russian covert activities to undermine deniability, build political consensus to respond, and better enable civil society organizations to act. Deterrence by denial would prevent the Russian government from so easily carrying out different election interference operations altogether. And bolstering US red lines in cyberspace would move the conversation with Russia toward specific do-not-cross positions with articulation of clear consequences.

**Spotlight Through Exposure**

The Biden administration, and the US government more generally, must dispense with its fixation on sanctions to supposedly deter the Putin regime through punitive means. Instead, the US must focus its efforts on continuous, near-real-time intelligence disclosures to expose Russian disinformation and election interference activities. Putin and his inner circle simply do not view election interference through the same lens as American policymakers; while US officials often talk of Russian interference as an act of “escalation,” the Kremlin already believes the United States to be interfering in Russian politics and in the politics of countries in Russia’s so-called near-abroad. While the US need not (and
should not) legitimate this worldview, it can recognize its strategic importance to the Kremlin—where US sanctions are (a) an expected cost and (b) possibly playing into the Kremlin’s view of escalation—and instead focus on exposing Russian election interference efforts.

Intelligence exposures of Russian interference have been fruitful thus far. For example, the US government publicized intelligence in February, ostensibly obtained shortly before it was released, exposing a Russian plan to fabricate a video to create a false pretext for launching a war on Ukraine.34 This and other exposures undermined Russian deniability—global press coverage and political condemnation were widespread—and they prepared publics and civil society organizations, from citizens to social media platforms, for possible Russian disinformation in that vein. The US government should invest more in public exposures to undermine Russian deniability, hinder the Russian government’s effectiveness in the process, and empower election defense coalition-building with civil society, industry, and foreign partners.

National security professionals frequently speak of Russian election interference in terms denoting “aggression” or even “escalation” in the digital domain.35 While perhaps intended to underscore the scope and severity of the interference and its resulting harm to US national security and democracy, such framings should not be taken to suggest that Russian actors view it the same way. On the contrary, Putin and his Kremlin circle already see Russia as embroiled in an information conflict with the West—and have for at least a decade now. The recent ODNI report itself notes that “Moscow almost certainly views meddling in US elections as an equitable response to perceived actions by Washington,” and that “Russian officials are probably willing to accept some risk in conducting influence operations targeting the US—including against US elections—because they believe Washington meddles similarly in Russia and other countries and that such efforts are endemic to geostrategic competition.”36

Many factors play into this belief system, including Putin’s KGB-shaped mindset, the legacy of KGB Department A “active measures,” widespread conspiratorial thinking in the Russian security services, fear of “color revolutions” that swept across former Soviet Republics beginning in 2003, the Arab Spring in 2010-2012, protests against Putin’s election rigging and return to the presidency in 2011-2012, and a perception that internet openness and the “internet freedom” agenda are little more than US means to influence world politics.37 The Russian government routinely extracts propaganda value out of discussing
supposed US covert influence, such as when officials exploit problems in the
democratic technology sphere to justify Moscow’s pursuit of internet control.\textsuperscript{38} But these comments—most famously, Putin calling the internet a “CIA project” in 2014—also reflect a genuine perception that the US works to digitally interfere in Russian politics.\textsuperscript{39} Putin, for example, stated in advance of the 2021 Russian “election” that the Kremlin was preparing for inevitable foreign attempts to interfere.\textsuperscript{40} Election interference, in the Kremlin’s eyes, thus does not put the Russian government on any kind of aggressive footing with Washington. Instead, the Kremlin perceives election interference as simply doing as all governments, including Washington, do to advance their interests (even if that is not the case).\textsuperscript{41}

The US need not give credence to this worldview to recognize its importance to the Kremlin’s cost-benefit calculus on election interference. If the Kremlin views all countries as engaging in this activity, and views it as essential to advancing the regime’s objectives, there is strong incentive for the Russian government to engage in it. And Moscow’s cyber sophistication as well as the US’s information-sphere vulnerabilities lend Moscow the capability and opportunity to do so. Instead of a question of desirability, the Kremlin’s pursuit of election interference becomes one of necessity and cost, which as discussed is incredibly low: a few million dollars spent on running the Internet Research Agency (part of “Project Lakhta”) and less than $150,000 spent on Facebook ads in a single election cycle is more than worth the value of destabilizing the US electoral system.\textsuperscript{42}

In part, this is why sanctions have arguably failed to shape the Kremlin’s thinking around and conducting of election interference in the United States. The Putin regime expects US sanctions as a matter of routine in response to its aggressive overseas actions, from assassinations to election-related hacks to invasions. Yevgeny Prigozhin and others involved in Internet Research Agency-type efforts can easily move money around to keep running their operations. Moreover, sanctions, to be effective, must be paired with a clear path for the Kremlin to get them lifted—and US vagueness on what does and does not constitute interference and red lines (discussed more in the next section) makes drawing that path harder.\textsuperscript{43}

Yet, intelligence exposures of Russian election interference activities have been remarkably effective. Reports from the US intelligence community, as well as the Mueller report and the five-volume report from the Senate Intelligence Committee, are widely considered to be
the authoritative sources on Russian election interference in 2016, 2018, and 2020.\textsuperscript{44} As former Principal Deputy Director of National Intelligence Sue Gordon has said, “one of the best ways to protect against influence is to actually tell people that the potential is there.”\textsuperscript{45} Even more broadly, there has been a notable shift in the US government’s thinking in the lead-up to Russia’s massive reinvasion of Ukraine: disclosing Russian covert, proxy, and influence activities as a way to undermine deniability and build domestic and international political consensus in responding. The disclosures also helped bolster other aspects of the strategy discussed in this article such as identifying to journalists, civil society organizations, and social media platforms that Russian authorities may fabricate videos of violence in Ukraine as a false pretext for attack.\textsuperscript{46}

The administration should invest more resources in tracking, and where possible exposing, Russian election interference efforts—such as identifying Russian government information and cyber operations as well as associated front organizations. This includes continuing to support the Office of the Director of National Intelligence in releasing public, declassified assessments of Russian election interference, and continuing to support intelligence and law enforcement agencies in tracking these activities. While there is often valid concern about exposing sources and methods of intelligence collection, the US intelligence community should keep exploring ways to shine lights on Russian interference efforts while protecting sources and undermining the Kremlin’s deniability. On top of that, the administration should also work with allies and partners to publish similar intelligence disclosures about Russian activities in other countries (e.g., new Internet Research Agency facilities in Ghana and Nigeria) and to systematize intelligence processes for sharing information about Russian election interference efforts globally. The more the Kremlin moves its operations outside Russia (whether to Eastern European or Western Africa), the more international intelligence cooperation will be essential to tracking, attributing, and publicly exposing those activities.

**Deter by Denial**

The second main component of shaping Russian election interference behavior should be deterrence by denial. Principally, this should be led by the private sector, as much of the US media and information ecosystem is not controlled by the government. But the US government should act in a few select areas: namely, denial through cyberspace and bolstering American democracy at home. The US government can also work with the private sector and civil society to more effectively incentivize suspending Russian information operations from social media platforms.
Deterrence by denial focuses on limiting an actor’s ability to carry out an action, or at least greatly minimizing the likelihood they can do it successfully. While investments in deterrence by punishment, as discussed, have failed to substantially alter the Kremlin’s decision calculus by imposing economic costs, investing in deterrence by denial would better prevent the Russian government from successfully carrying out election interference operations in the first place. Of course, it is impossible to stop literally everything Moscow tries. But a focus on denial matters in a modern information and internet space where governments, companies, and civil society organizations do not adequately invest in preventing the exploitation of cybersecurity vulnerabilities, legal and regulatory loopholes, and institutional weak points.

In much of deterrence by denial, the US government should take a backseat to the private sector. For example, television and radio media should not air disinformation about elections, even if spread by domestic actors, instead cutting away from politicians’ broadcasts that demonstrably lie about foreign manipulation of election precincts’ vote counts. The media more broadly should place greater scrutiny on election-related claims that are not backed up by sufficient evidence, and they should take care to note when and where statements are “disputed.” News outlets should have rigorous internal processes in place for reporting on hacked-and-leaked materials, as that information may be a means of interfering in the electoral process. And technology firms, for their part, should pursue creating new online platforms which are not as fundamentally oriented around low-cost micro-targeting—the leveraging of massive data troves to run highly targeted advertisements and content to individuals.

But the US government can still make Russian election interference harder. US Cyber Command should continue monitoring and, where necessary, disrupting active foreign operations to spread large volumes of disinformation on American social media platforms around elections. The Cybersecurity and Infrastructure Security Agency should continue its outreach programs to state and local election officials to boost the security of election infrastructure and communicate with the public about signs, or lack thereof, of digital election interference. Congress should increase the budget for CISA to conduct these activities as well as revise dangerous campaign finance laws that leave the United States vulnerable to malign domestic and foreign corporate and government influence. The US government should also recognize the value of civil society organizations that track and expose Russian election interference campaigns, both in acting as independent entities to monitor foreign election interference and in providing tactically useful information for government and/or private sector efforts to directly impede Russian operations.

Perhaps most importantly, if the United States wants to protect the integrity of its election processes and systems, it needs to bolster the strength and resilience of
American democracy at home. This includes a continuous, widespread effort to defend American democracy from anti-democratic forces within the United States. Republican Party efforts to effectively take away the voting rights of millions of people of color weaken American democracy, as do many elected officials who continue spreading disinformation on television, in print, and online. Politicians who nominally support defenses against Russian disinformation while engaging in disinformation themselves, for instance, both exacerbate the problem and undermine efforts to bolster the resilience of American democracy.

As a recent letter signed by dozens of American scholars of democracy wrote, “the most effective remedy for these anti-democratic laws at the state level is federal action to protect equal access of all citizens to the ballot and to guarantee free and fair elections.” Congress must guarantee and protect the equal right of all Americans to vote. The US executive branch must also change its rhetoric about threats to democracy from foreign powers to encompass threats to democracy from anywhere; part of addressing anti-democracy threats is first acknowledging how pervasive and dangerous they are in the United States and then working to stop them. Doing all this will bolster US democracy. It will also, in the process, make it more difficult for the Kremlin to conduct its election interference operations, such as those exploiting US racial divides to discourage Black communities from voting. And such policies could target overlap areas as well, such as American conservative media figures who parrot the Kremlin’s blatantly false disinformation talking points.

**Bolster Norms and Clearly Draw Red Lines**

The third and final component of a new strategy on Russian election interference should be to bolster norms against election interference operations and much more clearly articulating US red lines to Moscow. Until now, a lack of clear norms against election interference and a mixed record of articulating concrete red lines to the Kremlin have undermined efforts to shape Russian state behavior.

Following Biden’s June 2021 meeting with Putin, he told reporters that he named sixteen critical sectors the US wanted to see off-limits to destructive cyberattacks. While a full list was not provided to the public, it is possible that election infrastructure may have been covered by it. Nonetheless, to create an international norm against interfering in other countries’ election systems, the United States has to first publicly confront its long history of interfering in
other countries’ elections (e.g., during the Cold War), and vocally shift its position today to one of noninterference in other states’ elections.\textsuperscript{52} If an international norm against election interference is to have any chance of success, it will require American backing. The White House should start by making its own public commitments against this practice and encouraging allies and partners to do the same.

In direct conversations with the Russian government, the US executive branch should also clearly articulate its concrete red lines vis-à-vis elections. This process of identifying red lines and subsequently articulating them, however, will face multiple challenges. Election infrastructure is arguably not limited to electronic voting machines and voter registration databases. Media organizations, political campaigns, and watchdog groups all have digital infrastructure which, if compromised during an election season, can be used to sow discord and undermine election integrity (or public perceptions of it). And between 2016 and 2020, the Russian government targeted all of these entities. In 2016 alone, Russian state and state-backed actors hacked electronic voting machines (though reportedly did not change any vote counts), hacked into voter registration files in two Florida counties (though reportedly did not change any records), hacked and leaked emails from the Democratic National Committee, hacked the Republican National Committee but did not leak any documents, and stole US identities to make fraudulent online accounts.\textsuperscript{53} Poor security across many of these organizations—media companies, political campaigns, watchdog groups, and so on—leaves them vulnerable to hacks. It is feasible that Russian state or state-backed actors will hack these targets as part of future election influence campaigns.

American policymakers must therefore narrow the scope of their red-line-drawing efforts with Moscow. Many of these efforts should try to prohibit specific types of cyber activities against elections, rather than focusing on every possible hack of a target by every potential actor. This is because many of the organizations targeted in previous US elections are also targets in which many countries have legitimate espionage interest—and internationally accepted reasons to hack. For instance, political campaigns (and their email servers, document drives, and other digital systems) are a potentially valuable source of intelligence for governments looking to better understand the election landscape in a foreign country, including candidates’ personal beliefs, policy positions, financial backers, campaign strategy, engagement with opponents, and potential future staff. Hacking political campaigns to steal this information for purely espionage purposes would sit well within established international practice. Certainly, these hacks damage US national security, and campaigns have a long way to go toward better cybersecurity. But political campaigns and other entities critical to the US election process can all be legitimately targeted by governments for
espionage reasons—and it is fair to assume the United States engages in this kind of intelligence-gathering overseas as well. It is unrealistic to expect Moscow to even consider complete prohibitions on hacking those targets.

On this basis, the GRU, Russia’s military intelligence organization, did not violate any international norms per se when it hacked the Democratic National Committee in 2016 and read its emails. It was the subsequent, covert leaking of those materials online, to fuel the “simulation of scandal” and generate media criticism of Hillary Clinton, that was outside the norm and constituted a serious interference in the US electoral process. This is an important reason why US red line-drawing efforts with Russia must focus narrowly on specific types of cyber activities against specific types of targets. In this case, a prohibition on intelligence agencies conducting traditional espionage against political campaigns is completely unrealistic; it would be a total waste of time and resources to pursue. The prohibition, in this example, should instead focus on state actors leaking hacked materials and/or planting materials, real or forged, into US press coverage of an election.

All of that said, there may be some targets that the US wants to prohibit as a hacking target altogether—e.g., electronic voting machines. This is a case where policymakers may consider broadening their norm-building and red-line-drawing efforts. But getting the Russian government to agree to any kind of prohibition on certain kinds of cyber operations will be difficult, compounded by the state’s reliance on a web of cyber actors, leveraged with varying degrees of state backing, to conduct operations on its behalf. Hacking is a key part of the Kremlin’s foreign influence strategy, its modern intelligence operations, and its military activity; it is relatively low-cost, and blurred lines between state and non-state operations provide the Kremlin with a degree of deniability (even if implausible).

Biden administration officials should narrowly scope their red lines on election interference when communicating them to the Kremlin, focusing on specific types of activities conducted against specific types of targets. While these efforts have been ongoing, the key is to move away from a fixation on so-called strategic ambiguity in cyberspace, and to make the red lines much more concrete: working to draw the kinds of clear, tangible red lines that Russian negotiators can understand (and which play into Russian security service understandings of force). Talking about red lines includes discussing what happens beyond economic sanctions when the other country crosses them—and officials should not expose American cyber capabilities when articulating those red lines. But even general references to the ability to hit a particular Russian target in a particular way if the Kremlin takes a given action against US elections would still be far more effective than a vague reference to what Moscow should consider off-limits. It goes without saying that there is no guarantee of any change in
behavior from the Russian government. But pushing for the Kremlin to respect narrow, concrete red lines—with more specificity than the US articulates now—would still give the US a better chance at shaping Russian behavior than going in with broad lists of off-limit sectors and vague reference to possible repercussions.

**The key is to move away from strategic ambiguity in cyberspace**

**A Better Defense of Democracy**

For all the discussion in Washington of “deterring election interference,” the Russian government has continued running influence campaigns against US elections since 2016, despite US officials’ repeated condemnations and the numerous sanctions imposed on Russia. Election interference still remains low-cost and high-return for the Putin regime, which has strong incentives to interfere again in and throughout the upcoming 2022 midterm election campaigns as well as the presidential election in 2024. All the while, US democracy is becoming more fragile—as domestic actors work to undermine the idea of a country in which every American has a truly equal right to vote.

The United States needs to forge a new strategy on Russian election interference. Pursuing the same old response will not reshape the Putin regime’s behavior. Washington also cannot stay reactive—waiting for Russian activity to flare in order to respond—but instead must become proactive in combating foreign government efforts to influence the American electoral process. This three-pronged strategy of continuous intelligence exposures of Russian operations, comprehensive investment in deterrence by denial, and promotion of narrowly tailored, concrete US red lines will not solve everything. But the United States must change its strategies and at the very least make a concerted attempt to shape the Kremlin’s behavior—or doom itself to enduring the same interference that has been plaguing the country for close to a decade.

**Notes**


15. U.S. Department of Justice, “Russian National Charged with Interfering in U.S. Political System.”


40. “Putin says Kremlin knows foreign countries will interfere in Russia’s 2021 election, insists Moscow will be ready to resist,” RT, December 17, 2020, https://www.rt.com/russia/509962-putin-kremlin-foreign-interference-election/.


43. See, e.g., Newlin and Mankoff, “U.S. Sanctions against Russia.”

44. With thanks to Cara Dienst for discussion of this point.


52. See, e.g., Knake, Banning Covert Foreign Election Interference.

