CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

JANUARY 2023

No Water's Edge: Russia's Information War and Regime Security

Gavin Wilde and Justin Sherman

No Water's Edge: Russia's Information War and Regime Security

Gavin Wilde and Justin Sherman

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Summary 1

The Soviet Era and the “Hidden Hand” 1

After the Fall: The Compensatory Myth 4

Russian Information Doctrine Under Putin 6

Ukraine Tips the Scales 13

Conclusion 15

About the Authors 17

Notes 19

Carnegie Endowment for International Peace 25

Summary

To the extent that any unified theory of Russian information warfare actually exists, its core tenet might well be that regime security has historically been indivisible from information warfare in Russian strategic thought. Rather than an aggressive or expansionist expression of Moscow's foreign policy, the Kremlin's so-called information war should primarily be viewed through a domestic and regime security prism—it's as much a counterinsurgency as an expeditionary strategy, less an escalation than a projection. Analysts and decisionmakers should therefore avoid reflexively casting the United States and the West as Russia's primary antagonists in its information war, as doing so risks reinforcing these insecurities and exaggerating Moscow's degree of power in the information ecosystem.

The Soviet Era and the "Hidden Hand"

U.S. diplomat George Kennan, in his famous 1947 article "The Sources of Soviet Conduct," suggested an interesting duality to the idea of information threats to the state—that they serve simultaneously destabilizing and legitimizing functions. Kennan wrote that "it lies in the nature of the mental world of the Soviet leaders, as well as in the character of their ideology, that no opposition to them can be officially recognized as having any merit or justification whatsoever. Such opposition can flow, in theory, only from the hostile and incorrigible forces of dying capitalism."

He then wrote, however, that:

> “As long as remnants of capitalism were officially recognized as existing in Russia, it was possible to place on them, as an internal element, part of the blame for the maintenance of a dictatorial form of society. But as these remnants were liquidated, little by little, this justification fell away; and when it was indicated officially that they had been finally destroyed, it disappeared altogether. And this fact created one of the most basic of the compulsions which came to act upon the Soviet regime: since capitalism no longer existed in Russia and since it could not be admitted that there could be serious or widespread opposition to the Kremlin springing spontaneously from the liberated masses under its authority, it became necessary to justify the retention of the dictatorship by stressing the menace of capitalism abroad.”[1]

In accordance with that worldview, Kennan said, “all internal opposition forces in Russia have consistently been portrayed as the agents of foreign forces of reaction antagonistic to Soviet power.” At once, Kennan seemed to be suggesting that Soviet portrayals of foreign information threats were genuine—Communist Party officials did, in fact, believe that any information countering state narratives was a foreign attack—and that branding antiregime narratives as foreign threats was also an effective instrumentalist move by the Soviet leadership. The symbiosis of “information war” and regime security thus persists as an existential Gordian knot within the Kremlin.

A retired Russian colonel and military expert later asserted that Russia has rarely been defeated militarily by its opponents, except when they used information and psychological effects to defeat it “from within.”[2] Far from routine bluster, this line of thought is rife throughout Soviet doctrine and practice, which long recognized the importance of information in domestic security and control, armed conflict abroad, and broader geopolitical competition. The dynamics outlined in this paper are symptomatic of a recurring cycle in Moscow’s perception of security and its conception of information: the theories and technologies initially designed to control events within its borders are consequently unleashed to shape those beyond it.

Even in the pre-Soviet era, the czarist security force (Okhrana) viewed its remit as “securing the ruling elite and its ideological path.” It operated on the assumption that “internal threats invariably sprang from foreign plots,” according to professor Kevin Riehle of the National Intelligence University.[3] Much of the faith that Soviet leaders later imbued upon information warfare stems from the notion of individual and social malleability inherent to Leninist thought.

Upon overthrowing the czar in the October Revolution of 1917, the ideological leaders of the Bolshevik movement took upon themselves the task of molding the “new Soviet man.” As Leon Trotsky wrote, “Experiments in social education . . . will take place to a degree which has not been dreamed of before. Communist life will not be formed blindly . . . but will be built consciously, will be tested by thought, will be directed and corrected . . . social construction and psycho-physical self-education will become two aspects of one and the same process."[4] Concurrently, Vladimir Lenin "attached to propaganda the highest priority, attributing to it his regime's ability to survive against overwhelming odds. Its prerequisite was complete control over all sources of information," according to historian Richard Pipes.[5] Consequently, over the ensuing decades, so-called propaganda was not confined merely to party messaging and regime-friendly news reporting—it infused everything from education to the arts, sculpture and painting, literature and dance.[6] Dissidents and objectors to this top-down, reality-building endeavor by the Communist Party were driven underground, exiled, or worse.

Later, as advanced technologies began to capture both U.S. and Russian imagination during the atomic age, Soviet intellectuals were seized with the prospects of cybernetics—the study of the control and feedback in complex systems, particularly those involving humans and machines—and its potential social, economic, and military applications. Echoing Lenin's assertion that governance is inherently a science, Soviet admiral Aksel Berg propounded on the promise of the new discipline in the early 1960s: "There are no unknowable phenomena, only unknown ones; likewise, there are no uncontrollable processes, only those in which the complexity of the task is not yet matched by the methods and means for its solution. Cybernetics broadens the range of controllable processes; this is its essence and its major merit." Despite "increasingly gaining prestige as the main theoretical idea of the 'technology' of managing society," the discipline ultimately fell from favor over the course of the next decade—having been overladen with Communist philosophy, misappropriated by the sprawling Soviet *nomenklatura*, and extended into too many competing disciplines.[7]

This systemic rejection of any notion that a network might emerge organically and unsanctioned was emblematic of Moscow's future approach to information and technology writ large.[8] Moreover, the tendency to apply a mechanistic rubric to the complexities of human development and cognition soon permeated Soviet war planning, as military theorists developed an indigenous analog to the dominant Western "game theory" of interstate conflict. As a 1937 article in the state-run newspaper, *Pravda*, stated: "We know that engines do not stop by themselves, machine tools do not break down on their own, boilers do not explode on their own. Someone's hand is hidden behind these events."[9] Incidentally, this sentiment enabled Soviet leaders to abdicate responsibility for major failures, both economic and military.

The sentiment also found resonance in Soviet warfighting doctrine. Concealment (*maskirovka* in Russian) was thought to lend a degree of control over an adversary by inducing them to take an action—of their own volition, at least in their mind—which had in fact been carefully orchestrated in advance. This Soviet theory, dubbed "reflexive control," is defined as "influenc[ing] the opponent's perception of the situation or his goals or his doctrine, and at the same time conceal[ing] from him the fact that one *is* influencing him."[10] For example, many Russians consider U.S. president Ronald Reagan's Strategic Defense Initiative to have been a masterful use of reflexive control, as the Soviet Union was "tricked" into attempting to keep up with U.S. space-based weapons, pouring resources into countermeasures at a time when the Soviet economy could least afford them.[11] The idea drew on Marxist-Leninist notions—that everything in the world is scientifically understandable and governed by laws of behavior (which, in turn, can be systematically manipulated).[12]

The natural (and compounding) byproducts of such a theory are a hubristic faith in one's own ability to control events and the conspiratorial paranoia of assuming the same capability in the adversary. For example, Russian researchers more recently viewed the overlapping advent of social media and eruption of popular revolutions since the 2000s as a more-than-coincidental form of managed chaos: "[Western] elites understand that by controlling the flow of information, managing its submission to the media, it is possible to influence the course of social processes."[13] Such accusations can be at least partially considered projection on Moscow's part, as the Soviet-era active measures program set the standard for political subversion abroad—in aspiration, if not in practice. The covert tradecraft designed to sculpt foreign public and leadership perceptions through whatever means necessary—proxies, agents, frauds, and even incitement to violence—was perfected by the Committee for State Security (KGB). The agency's First Chief Directorate, in charge of all foreign operations, had a dedicated department for spreading disinformation—including antisemitic, racially charged narratives designed to exacerbate sociopolitical fissures in targeted countries. However inconspicuous its name, Department D was considered by KGB leadership as vanguard of "the most effective form of active measures . . . integrated actions that took on a proactive, offensive, and long-term character."[14]

For example, when the KGB suspected Russian dissident writer Aleksandr Solzhenitsyn of conducting subversive activity from exile in Zurich in the mid-1970s, the organization dedicated enormous, but largely wasted, efforts—entailing no fewer than twenty discrete operations spanning three directorates—to discredit him and infiltrate his circle. The domestically rooted impetus for such a ham-fisted, futile effort was clear in then KGB chair (and later Soviet premier) Yury Andropov's concern about "counter-revolutionary elements" from without, which might "seek to fan the flames" of nationalism, dissent, and ideological subversion.[15] In the KGB era, as in the digital age, the distinction between aggressive expansionism and reactionary reprisal can be difficult to parse.

After the Fall: The Compensatory Myth

Dedication to information warfare did not die with the Soviet Union's 1991 collapse. Rather, mid- and late-1990s Russian debates about security in the information sphere appeared to center around internal instability, former Soviet republics' growing integration with the

West, and a deep desire on the part of many officials, as well as many Russians, to reassert an idea of Russian national unity and greatness. Much of Moscow's thinking about security in the so-called information age found roots in the search for explanatory power amid the disorienting and tumultuous post-collapse period.[16] In its worst expressions, strategic culture gravitated toward the "compensatory myth," as Russian pollster Lev Gudkov calls it, of a glorious past disrupted by external forces, a scapegoat for governing failures, and a means to legitimize increasingly repressive measures.[17]

These conceptualizations of information and security were varied. In 1995, former Russian navy admiral Vladimir Pirumov wrote an article stressing the importance of making "information security" a vital component of Russian national security.[18] Russian army general Makhmut Akhmetovich Gareyev argued that states initiating war do not want protracted conflict and that information and other revolutions in military affairs can enable quick and decisive victory. He also wrote that information warfare could be used indirectly, to end conflicts before they become kinetic.[19] Russian colonel Sergey Modestov and general-major Nikolay Turko, by contrast, suggested that information warfare was changing the very nature of the threat to Russian national security itself.[20]

Timothy Thomas, an analyst for the U.S. military, put it succinctly in 1997: "Russian military theorists have always been particularly sensitive to the enemy's ability to control, through either propaganda or the manipulation of information, the psyche of Russian soldiers. They consider the concept of 'moral-psychological' preparation of the soldier to be a Russian principle of war."[21] Yet, in the wake of the Soviet Union's collapse, "Russian sociologists consider[ed] the populace and the armed forces to be psychologically unstable and extremely vulnerable to foreign based and foreign-run information operations. The requirement to counteract the information-psychological capability of the enemy [became] even more important."[22]

This was not a purely intellectual exercise. Information's power to tangibly shape international relations and Russia's international standing remained top of mind. After the Russian military brutally suppressed a 1994 rebellion in Chechnya (the First Chechen War)[23]—killing thousands of civilians[24]—information about the human rights abuses and indiscriminate deaths contributed to then U.S. president Bill Clinton's administration toughening its line on the Kremlin.[25] (This was not absolute and did not last a while, either; Clinton was quick in April 1996 to downplay the war and echo Yeltsin's depiction of the conflict when trying to resolve an arms control dispute.[26]) Damage to Yeltsin's public perception domestically, stemming from press reporting and Chechen accounts of Russian military violence, was likewise noticed by Russian officials (and blamed on the media).[27] Shortly after the war's end, for instance, a May 1996 article in the *Moskovskiy Komsomolets* newspaper said the Russian military might return to "propaganda" units to control information.[28] Emil Pain, a Moscow State University professor and Russian president Boris Yeltsin's former adviser on ethnonational relations, would later write that "after the first Chechen War, the Russian military concluded that it had lost the information war to the Chechen resistance."[29]

By the turn of the century, Russian military thought grappled with the rapid advances in computer network operations in wartime and increasingly networked societies in peacetime. Drawing somewhat from China's equal and complementary emphasis on both the technological and psychological evolutions in interstate conflict, Moscow eventually adopted "information confrontation" (*informatsionnoye protivoborstvo*, also translated as "information struggle") as a guiding paradigm for the digital age.[30] Often used interchangeably with information warfare, it likewise became institutionalized within both the military and the KGB's successor agencies. Concurrently, the Kremlin cracked down on independent media, consolidated and later reorganized its state-run media holdings, and spent lavishly to make outlets like RT and Sputnik household names in post-Soviet propaganda with a modern twist.[31] The assumption baked in at each step was the idea that genuine public engagement in political (and geopolitical) affairs was merely a thin veneer for adversarial "social programming."[32]

The transition from the Soviet heyday of propaganda and active measures to the current era of digital subversion did not take place in a vacuum. Each step along this path, evolving into what Russia scholar Robert Horvath describes as "preventive counter-revolution,"[33] was guided by meticulously documented strategy.

Russian Information Doctrine Under Putin

Since Vladimir Putin's ascension to the Russian presidency in December 1999, there has been no single, cohesive doctrine for information warfare. Instead, the Russian government has published a series of information security doctrines, foreign policy concepts, military doctrines, and other policy and strategy documents that both set strategic and operational priorities for the Russian information apparatus and, collectively, lay out how the Kremlin thinks about information and the internet—and competition and conflict within that space. The components of Russian thinking in the Putin era illustrate a comprehensive view of information security that goes far beyond the technical. It reflects an increasingly paranoid belief that external actors are weaponizing the modern information space to threaten Russian interests abroad and undermine the security of the regime at home. The very notion of information security as encompassing social and cultural stability, regime security, and technical and traditional measures to cement control over information speaks to the sweeping nature of this worldview.

Putin's Inaugural Information Security, Foreign Policy, and Military Doctrines

The 2000 Information Security Doctrine of the Russian Federation declared that "the national security of the Russian Federation substantially depends on the level of information security, and with technical progress this dependence is bound to increase."[34] It defined information security as "the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state."[35] It then described seven external sources of threat to Russian information security. On top of naming international competition for information technology, terrorism, world powers' growing technological edge over Russia, and foreign reconnaissance, the doctrine also listed:

- "Activities of foreign political, economic, military, intelligence, and information entities, directed against the interests of the Russian Federation in the information sphere";[36]

- "The striving of a number of countries toward dominance and the infringement of Russia's interests in the world information space and to oust it from external and domestic information markets";[37] and

- "Development by a number of states of information war concepts that provide for creating means for dangerous attack on the information spheres of other countries of the world, disturbing the normal functioning of their information and telecommunications systems, breaching the security of their information resources, and gaining unsanctioned access to them."[38]

Critically, Russian government references to so-called information security do not mirror the modern, Western understanding of information security—which refers generally to the confidentiality, integrity, and availability of systems, networks, and data.[39] Likewise, references to "information security breaches" do not correspond to the contemporary Western understanding (of undermining encryption or getting past a firewall). Instead, the Russian government's discussion of information security broadly encompasses the regime's interests in the information sphere, including regime security and the state's control over information flows and public opinion. This is the "sovereignty" to which Moscow refers in "cyber sovereignty." Relatedly, breaches of information security, in the Russian government's conception, include threats to encryption and technical defenses, but also include—and perhaps principally emphasize—undesirable content or information. The last of the Information Security Doctrine's "external threats" speaks particularly to this point. Indeed, the document expresses a fear of information undermining the regime: "the precariousness of citizens' rights to information access, and information manipulation evoke a negative reaction among people, which in a number of cases leads to a destabilization of the social and political situation in society."[40]

The 2000 Foreign Policy Concept of the Russian Federation reflected similar thinking about the role of information in Russian diplomacy and international standing. "While the military power [sic] still retains significance in international relations among states," it stated, "an ever greater role is being played by economic, political, scientific and technological, ecological, and information factors."[41] It added, "the major breakthrough in a number of key areas of scientific and technological progress leading to the formation of a single, worldwide information environment, the deepening and diversification of international economic ties add a global nature to interdependence of states."[42] Alongside discussions of United Nations Security Council influence, nuclear war risk, and other issues, the Foreign Policy Concept specifically called attention to external information dependence—specifically to reinforce Russia's foreign policy, culture, economic interests, and impact on public opinion.[43]

In the context of Putin's July 2000 address to the Federal Assembly, the concept appears to have been developed from a position and perception of weakness on the part of the Kremlin. Putin's speech "underlined Russia's economic backwardness in relation to the advanced western states," as one analyst put it—with Putin warning that "the growing rift between the leading states and Russia is pushing us towards becoming a third world country."[44]

Released the same year, the 2000 Military Doctrine of the Russian Federation included similar themes of information conflict. Of the eight main factors described as determining the "military-political situation" of the day, one was "the exacerbation of information confrontation" unleashed by unspecified, expansionist international forces using nontraditional means to destabilize the geopolitical landscape.[45] The doctrine listed as a main external threat to Russia "hostile information (information-technical, information-psychological) operations that damage the military security of the Russian Federation and its allies."[46] Main internal threats to Russia included "an attempted violent overthrow of the constitutional order," efforts by "extremist nationalist, religious, separatist, and terrorist movements" to destabilize Russia's "domestic political situation," and "the planning, preparation, and implementation of operations aimed at disrupting the functioning of federal organs of state power and attacking state, economic, or military facilities, or facilities related to vital services or the information infrastructure."[47] In peacetime, according to the doctrine, one key element of "safeguarding military security" was "maintenance of domestic political stability and protection of the constitutional system, integrity, and inviolability of the territory of the Russian Federation."[48] During a period of threat or armed conflict, the doctrine made clear, one of the military's central tasks is the "organization and coordinated implementation of armed, political, diplomatic, information, economic, and other forms of struggle."[49]

These three documents fit into a broader interrogation and rearticulation of what national security and national power meant to the Kremlin in a post-Soviet, twenty-first-century information age. To the Putin regime, this principally included leveraging information and communication technologies to project Russian influence globally, safeguarding information systems within the country from kinetic attack, and ensuring it maintained control over domestic information flows and stability. For all that some Russian security service personnel were closely watching the global internet's spread with concern, many Kremlin officials were not bringing the same high-level attention to the online space. Others were still fixated on controlling narratives in the press and especially on television.[50] It would be years before the Russian government began cracking down on the internet, unlike counterparts in China.

While the primary beneficiary of the KGB legacy was the Federal Security Service (or FSB, of which Putin briefly served as director),[51] no single agency adopted the explicit charge over what once fell to the KGB's Fifth Chief Directorate: quelling domestic political dissent.[52] As opposition figures like Alexei Navalny took to online platforms to organize and expose incompetence and corruption in the late 2000s, the Kremlin outsourced to putatively private actors the job of drowning out and disputing their findings.[53] By 2013, one of Putin's associates, Yevgeniy Prigozhin, was bankrolling an entire operation—known variously as the "Russian troll farm" or the Internet Research Agency—that aimed to undermine and disrupt these opposition bloggers.[54] This tradecraft would, of course, later be turned outward against Ukraine, NATO, and the United States. Meanwhile, the military and security services variously arrayed themselves to engage in information confrontation, notably:

- The General Staff Main Directorate (GRU), Russia's military intelligence agency—which has at least one unit (54777, the 72nd Special Service Center, or GRITs) dedicated to psychological, disinformation, and influence operations abroad—leverages front organizations, proxies, and online sock-puppet accounts to advance or refute specific narratives.[55]

- The Russian Foreign Intelligence Service (SVR), successor to the KGB First Chief Directorate, has a directorate dedicated to so-called active measures: Directorate MS.[56] This unit similarly employs front organizations to amplify and propagate specific narratives.[57]

- The Russian military's Information Operations Troops (VIO) was initially touted by Russian Defense Minister Sergei Shoigu in 2017, noting its Soviet-era counterpropaganda pedigree.[58]

- The FSB, in addition to its domestic surveillance and censorship remits, appears to have some degree of organizational focus on digital information manipulation abroad.[59] In particular, the Center for Information Security (TsIB), also known as Center 18, is reported to run point for the agency on social media-based operations.[60]

Whereas the old KGB model sought, at least in part, to clear a path for Kremlin-advantageous narratives to prevail on the international stage, the Putin-era model appears designed primarily to subject that same stage to the tragedy of the commons—so polluted by contradiction and distortion that none prevail at all.[61] Such a strategy is indeed a hallmark of any aspiring totalitarian regime, which "moves ahead less on the conviction of its members than on the confusion of its opponents."[62] It also reflects Russia's friction-filled reality of operationalizing information warfare ideas, where a few dominant security organs—with a history of turf wars and infighting—execute overlapping, uncoordinated operations while a web of media outlets flood the zone with information that might be redundant, or even contradictory.

Later Doctrines and Concepts

Moscow developed and released numerous such doctrines, concepts, and policy documents in the ensuing years. Among them were the 2008 Foreign Policy Concept, the 2010 Military Doctrine, the 2014 Military Doctrine, the 2015 National Security Strategy, the 2016 Foreign Policy Concept, the 2016 Information Security Doctrine, and the 2021 National Security Strategy. Each of these documents expounded on the idea of information security as integral to national security and foreign policy—alongside an increasing emphasis on foreign powers using information to undermine Russia domestically.

Keeping in line with the Kremlin's growing focus on using all matters of state power, including nonmilitary means, to protect security, the 2015 National Security Strategy asserted that a main threat to the Russian state and public security is "activities connected with the use of information and communication technologies to disseminate and promote the ideology of fascism, extremism, terrorism, and separatism, and to endanger the civil peace and political and social stability in society."[63] Notably, this use of the term "fascism" was novel in Putin-era strategy documents, but it was predictable in the context of the narratives Moscow was advancing at the time regarding developments in Ukraine (more on that later). Equally important is the distinct way Moscow perceives the term relative to the West—less as "a set of abstract principles related to the nature of a political regime and its mass indoctrination techniques" than as an encroaching external force, victory over which has served as a primary legitimizing principle for the Kremlin's domestic authority since the end of World War II.[64]

The 2016 Information Security Doctrine, signed that December, superseded the earlier doctrine from 2000. This one defined information security more expansively, adding in explicit mention to "internal and external information threats" against Russia.[65] It stated that "foreign countries are building up their information technology capacities to influence the information infrastructure in pursuing military operations."[66] Beyond this supposed military activity, per se, it also said:

> "Intelligence services of certain States are increasingly using information and psychological tools with a view toward destabilizing the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other States. Religious, ethnic, human rights organizations, and other organizations, as well as separate groups of people, are involved in these activities and information technologies are extensively used towards this end."[67]

Notably, the doctrine then stated the importance of improving the competitiveness of Russian technology companies, eliminating dependence on foreign technology, and developing a "competitive domestic electronic component base."[68] It said the Russian government must counter the use of information technologies to forcibly change the constitutional order and violate the territorial integrity of the Russian Federation.[69] It then added that another key state activity is “suppressing the activity detrimental to the national security of the Russian Federation, carried out by special services and organizations of foreign States as well as by individuals using technical means and information technologies,”[70] seemingly a nod to domestic information control and political repression in general. Fear of foreign plots was a consistent theme.

Most recently, the 2021 National Security Strategy ratcheted up the Kremlin’s explicit paranoia even further,[71] stating that Russia’s enemies include foreign tech companies “spreading unverified information” and that a “distorted view of historical facts, as well as events taking place in the Russian Federation and in the world, are imposed on Internet users for political reasons.”[72] It said that “the use of information and communication technologies is expanding to interfere in the internal affairs of states, undermine their sovereignty, and violate [their] territorial integrity.”[73] Further, it added, “information and psychological sabotage and the ‘westernization’ of culture reinforce the threat of the Russian Federation losing its cultural sovereignty.”[74] The strategy also stated that foreign technology increases Russia’s vulnerability to foreign influence—and that in response, the Russian government should improve “information security” at home, bring “reliable information about the Russian Federation’s domestic and foreign policy to the Russian and international community” (presumably through enhanced overt propaganda), and ensure Russia advances “the development of forces and means of information confrontation” (presumably via military and intelligence means).[75]

Suspicion, Isolation, and Autarky

Information warfare becomes an even more encompassing concept online, where information is flowing constantly. The Kremlin has long seen the internet as both a threat to regime security and a weapon to be used against Russia’s enemies. Or, as Sergei Ivanov, former chief of the Russian Presidential Administration, once elegantly put it, “the Internet is a stick that has two ends: it can do good service but it can also be a real garbage place.”[76]

Since 2008, Moscow has released two successive strategies to cultivate Russia’s “information society.” Nominally intended to spur indigenous digital development and technological innovation, these documents have instead primarily served to legitimize increasingly rigid censorship and surveillance measures.[77] These strategies were complemented by a raft of legislation over the ensuing decade designed to impose “sovereignty” over the infrastructure, content, and data traversing Russia’s “information space.” While nowhere near as sophisticated (or effective) as China’s so-called Great Firewall, upon which it draws inspiration, Moscow’s RuNet is the culmination of these efforts.[78]

Around 2012, when Putin returned to the presidency amid large-scale protests he believed were engineered by the United States, Moscow began introducing numerous new restrictions on the internet within Russia, from a law undermining bloggers’ anonymity to a data localization law mandating that companies store copies of data regarding Russian citizens within Russia. These controls operated alongside the FSB's legal intercept system, the System of Operational-Investigative Measures (SORM), which was initially designed in the mid-1990s for surveillance of telephony and later updated for email and deep-packet inspection of online traffic.[79]

In 2019, Putin signed a sovereign internet law calling for the government to make the internet in Russia isolatable from the global one at the flick of a switch. The law's incredibly aspirational components—like centralizing state control of a diffuse internet architecture and creating a custom domain name system (DNS, essentially the internet's phone book for traffic) in Russia—quickly hit stumbling blocks as bureaucratic and technical hurdles impeded progress.[80] Moscow is still far from its objective. The internet in Russia is far less centralized than in China, where Beijing already controlled the four primary internet backbones in the 1990s when it focused more on expanding internet control.[81] This makes the process of mapping and then filtering and controlling the internet much more difficult for the Russian government, as the infrastructure is diffuse and many providers underpin the overall network.[82] (Illuminating this problem, the sovereign internet law in 2019 included a requirement for the government to create a central repository of all the autonomous system numbers (ASNs) in Russia, the smaller networks of which constitute the internet—suggesting the government has not even comprehensively understood and tracked the internet infrastructure in its own country.)[83]

Due to a relative historical lack of investment in technical filtering capabilities, relatively delayed high-level Kremlin attention to the internet (until around the time of the 2008 Russo-Georgian War and the Arab Spring), and emphasis on traditional coercion rather than technology as the primary means of control, Moscow has lagged behind China in controlling the internet at home. Beijing's efforts, by contrast, began in the 1990s and ramped up heavily during the early 2000s, concurrent with greater investments in internet traffic filtering capabilities and drawing on an immense base of technical talent.

Nevertheless, the Kremlin has continued to gradually cement its grip over the online space in Russia, including through traditional offline coercive measures like confusing and inconsistently enforced speech laws, threats of arrest, security service harassment, and police brutality at protests. Its recent blocking and throttling of some foreign websites, like Twitter and the BBC,[84] also conveys that its filtering capacity has improved since the botched, two-year attempt to block encrypted messaging app Telegram from 2018 to 2020.[85] Roskomnadzor, Russia's internet and media censor, has also taken on a surveillance role: recently leaked documents show the agency compiling dossiers on regime critics for handover to security services, tracking online activity from hundreds of people and organizations, and performing other intelligence-type activities.[86]

The fears of overreliance on Western tech implicit in Putin's 2000 address to the Federal Assembly appear to have come full circle nearly twenty-two years later. After Western firms made their exodus from the Russian market in the aftermath of Moscow's full-fledged invasion of Ukraine, Putin expressed relief, calling the move "a blessing in disguise."[87]

Ukraine Tips the Scales

Throughout the entirety of Putin's reign, the Russian government, senior Russian officials, and leading Russian foreign policy and military thinkers have all written about both internal and external threats to the regime.[88] In March 2000, after the Russian Duma (the lower house of parliament) refused to challenge former president Boris Yeltsin's immunity, then foreign minister Igor Ivanov called Western media reports of Yeltsin's corruption a "real information war" against Russia. Ivanov told Russia's Foreign Ministry Council on Science and Culture that Western media was looking to "draw an extremely negative, one-sided picture of modern Russia . . . and not only of the state, but also of society as a whole." He continued, "it is difficult to evade the impression that there is a definite scheme behind such actions—by blackening Russia, pushing it into secondary roles and depriving it of an independent voice in world affairs. We will not allow this to happen any more than we will let ourselves roll into primitive anti-Westernism or self-isolation."[89]

While the first two Putin terms and Dmitry Medvedev's presidency certainly entailed a rejection of the 1990s, they had not yet embraced a "wholesale adoption of ideological and allegorical thinking," according to scholar Eliot Borenstein. "Even as the country's media lost most of its independence from the state, the government's interventions in the culture were limited. But when Putin returned to the presidency for a third term in 2012 . . . Russia was now under siege by the combined efforts of Europe and the United States to isolate the country strategically and ruin it culturally. Conspiracy, which had been slowly moving out of the margins, was now mainstream."[90]

There were a number of catalysts for this shift. After organic Russian protests to Putin's election-rigging in the fall of 2011 and return to the presidency in the spring of 2012, organized in part on social media through Facebook and Russia's VK, Putin said that then U.S. secretary of state Hillary Clinton "set the tone for some opposition activists, gave them a signal, they heard this signal and started active work" and said that "hundreds of millions of dollars are being invested in this work."[91] The Russian government then published its Concept for the Security of Society of the Russian Federation, which declared that "one of the main sources of threats to the security of society is the extremist activities of nationalist, religious, ethnic, and other organizations and structures aiming to ruin the unity and territorial integrity of the Russian Federation, and to destabilize the domestic political and social situation in the country."[92] All of this occurred around other Kremlin concerns about the internet, catalyzed by the Arab Spring movements in 2011,[93] the Snowden leaks in 2013,[94] the Panama Papers leak in 2016,[95] and even the day-to-day internet disruptions to the regime in Russia, as citizens documented police searches and brutality online.[96] Real challenges to the regime melded with paranoia, conspiratorial thinking, and a strong desire to cement control over information—yielding a fixation on information warfare increasingly waged online.

The 2013–2014 Ukraine crisis proved to be a major inflection point, as the Kremlin's grip on the domestic information space tightened and its information campaigns were increasingly aimed at much more complex geopolitical developments—ultimately to include U.S. presidential elections. The Maidan Revolution in Ukraine either sparked an uptick in conspiratorialism from Moscow or merely brought latent impulses fully out into the open. Kremlin-linked online mercenaries and traditional propaganda outlets turned from focusing on domestic oppositionists to branding Ukraine's post-Maidan leaders as "fascists" being weaponized by the United States and its allies against Moscow.[97]

Over time, such feverish narratives were internalized: "For the first time in seventeen years top-ranking politicians, including Putin, himself, started to regularly voice [such] notions in public. . . . Projecting Russia's important standing in the world, via anti-Russian conspiracy theories and modern technologies, is, certainly, an elegant way of trying to restore its status as a great power."[98] Putin especially has, in many ways, become quite skilled at spinning facts on the ground to create an imagined notion of foreign information threats to Russia's domestic stability. The "art of the offensive defense," as former U.S. national security official and Russia expert Fiona Hill calls it, has become part and parcel of Russian foreign policy—and of Kremlin messaging toward social movements in Russia's so-called near abroad.[99]

What results is Putin's portrayal of a vast foreign threat to Russia—a product of citizens taking to the streets, as well as imagined foreign intelligence activity that stoked the protest movement in the first place. Much of Moscow's subsequent interference and information operations in the U.S. presidential elections of 2016 and 2020 were driven as much by a desire to delegitimize the Maidan movement and its supporters in Washington as by any purely bilateral calculations.[100] While Putin certainly views relations with the United States in zero-sum terms, the implications of Ukraine's organic shift westward were unacceptably ominous for the staying power of Putinism. Thus, the Kremlin's inability (or unwillingness) to contend with the idea that the Orange Revolution in 2004 and the toppling of former Ukrainian president Viktor Yanukovych's regime in 2014 were anything but the fruits of a foreign plot were evident in its catastrophic underestimation of Ukraine's resiliency to covert, cyber, and later conventional assaults on its sovereignty.

By early 2022, as a renewed Russian invasion appeared imminent, journalism about the regime's war on Ukraine, Western intelligence disclosures, and firsthand accounts by Ukrainians themselves were frequently dubbed "Russophobia" by Russian officials, "blasphemous and unfounded allegations . . . part of information war [sic] against Russia."[101] A mere nine months later, Putin stood on Red Square to commemorate the illegal annexation of four Ukrainian territories, partially occupied by force, proclaiming: "We will defend our land with all the powers and means at our disposal. . . . The battlefield to which fate and history have called us is the battlefield for our people, for great historical Russia, for future generations, our children, grandchildren and great-grandchildren."[102]

Conclusion

Moscow's fixation on regime security and the interaction between domestic and foreign policy has been continually highlighted across the past decades and currently continues apace. To offer just a few examples:

- Defense Minister Shoygu said in March 2015, "The day has come when we all have to admit that a word, a camera, a photo, the internet, and information in general have become yet another type of weapons [sic], yet another component of the armed forces. . . . This is a weapon that was involved in various events in our country in different years, both in our defeats and in our victories."[103]

- Chief of the General Staff Valery Gerasimov said in December 2019, "Unprecedented political, economic, and information pressure is being applied to countries trying to pursue an independent policy, among them Russia," which means that "under these circumstances, we cannot rule out a possibility of crises, which may run out of control and develop into a large-scale military conflict."[104]

- Dmitri Trenin, a prominent Russian voice on foreign policy and security issues, wrote in July 2022, "Ultimately, the main field of the ongoing battle is located inside the country . . . [we] must start with ourselves, with an awareness of who we are, where we come from, and what we strive for, based on our values and interests."[105]

As Moscow's disastrous war on Ukraine drags on, tensions among the elite are beginning to emerge. The Putin regime looks weakened and internally incoherent—it is grasping for an alternative to the unfriendly, objective realities it faces. Insofar as the Kremlin continues to insist upon a view of information as foremost a battlefield for regime solvency, analysts and policymakers should:

Accept that Moscow's insecurities about the information environment, however profoundly misguided, are nevertheless genuine and deeply entrenched. While the belief that the U.S.-led West is concertedly deploying covert information operations to destabilize Russia and its neighbors may be mere cynical posturing in some circles, it is foundational canon in the Kremlin inner circle. Both overt messaging and covert activities should be conducted advisedly—they will be perceived and portrayed accordingly by Russia. Disabusing Moscow of this notion, meanwhile, is likely to be a generational project that is unlikely to bear fruit under a Putin (or Putinist) regime.

Perceive and portray Russian information operations less as expressions of strength on the international stage and more as signals of vulnerability on the domestic front. Reflexively casting the United States and the West as the primary focal points (or antagonists) of Russian activity in the information space risks legitimizing Moscow's framing and lending more credit to Russia's strategic thought and prowess on the international stage than is likely warranted.

Continue to explore the relationship between Russian information operations abroad and Russian government insecurity at home. This area is ripe for further research and policy analysis. Using history as a guide, the entities and tradecraft Moscow uses to subjugate the information environment in Russia—particularly as failures in the war on Ukraine threaten to spur fissures online[106]—can likely serve as an early-warning mechanism for how they will eventually be operationalized abroad.

The thinking captured in Russian strategy documents indicates that Russian information warfare is foremost an egocentric expression of systemic self-preservation. To conclude otherwise is to inflate Moscow's sense of dominance over the information ecosystem and lend too much credence to a regime that struggles to keep its domestic insecurity from expanding beyond the water's edge.

About the Authors

Gavin Wilde is a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace, where he applies his expertise on Russia and information warfare to examine the strategic challenges posed by cyber and influence operations, propaganda, and emerging technologies.

Justin Sherman is the founder and CEO of Global Cyber Strategies, a DC-based research and advisory firm; a senior fellow at Duke's Sanford School of Public Policy; and a nonresident fellow at the Atlantic Council. He was previously a fellow at Stanford's U.S.-Russia Forum, where he participated in Track II dialogues with Russian counterparts on international security issues.

Acknowledgments

The authors are grateful for contributions of both time and expertise by the Carnegie Endowment's own George Perkovich and Eric Ciaramella.

Notes

[1] George F. Kennan, "The Sources of Soviet Conduct," *Foreign Affairs*, 1947, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct.

[2] Ольга Божьева, "Мураховский рассказал, чем может удивить новая российская военная доктрина," *Московский Комсомолец*, https://www.mk.ru/politics/2021/04/03/murakhovskiy-rasskazal-chem-mozhet-udivit-novaya-rossiyskaya-voennaya-doktrina.html.

[3] Kevin P. Riehle, *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present*, First (Bethesda, Maryland: National Intelligence University Press, 2022), https://www.scuolafilosofica.com/10883/kgb-gru-fsb-russian-intelligence-history-and-present.

[4] Leon Trotsky, *Literature and Revolution* (1924), 8. https://www.marxists.org/archive/trotsky/1924/lit_revo/ch08.htm.

[5] Richard Pipes, *A Concise History of the Russian Revolution* (Knopf, 1995), 305.

[6] Britannica, T. Editors of Encyclopaedia (2022, July 25). *Socialist Realism*. *Encyclopedia Britannica*. https://www.britannica.com/art/Socialist-Realism.

[7] Slava Gerovitch, *From Newspeak to Cyberspeak: A History of Soviet Cybernetics* (Cambridge, MA: MIT Press, 2004), 254-286.

[8] Andrei Soldatov, Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York, NY: Public Affairs, 2015), chapter 1.

[9] Gabor Rittersporn, *Anguish, Anger, and Folkways in Soviet Russia* (Pittsburgh, PA: University of Pittsburgh Press, 2014), 34.

[10] Vladimir Lefebvre, *Algebra Konflikta* (Russia, 1968).

[11] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military" in *Journal of Slavic Military Studies* (Taylor & Francis, 2004), 17: 237–256.

[12] Diane Chotikul, *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study* (Monterey: Naval Postgraduate School, July 1986), 13.

[13] Владимир Карякин, "Наступила эпоха следующего поколения войн – информационно-сетевых," *Новая Газета*, http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html.

[14] Thomas Rid, *The Secret History of Disinformation and Political Warfare* (New York, NY: Farrar, Straus, and Giroux, 2020), 130–131, 133.

[15] Christopher M. Andrew, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York, NY: Basic Books, 1999), 311, 319–321.

[16] Serguei Oushakine, "'Stop the Invasion!': Money, Patriotism, and Conspiracy in Russia," Social Research 76, no. 1, (Spring 2009): 71–116, https://scholar.princeton.edu/sites/default/files/oushakine/files/490-stop_the_invasion_money_patriotism_and_conspiracy_in_russia.pdf.

[17] Anton Barbashin (@ABarbashin), "Lev Gudkov: The Putin regime is a reaction to the failure to build a democratic, legal society, a normal country. Hence the malice, aggression, appeal to the great past as a compensatory myth.," Twitter post, August 14, 2022, 3:29 p.m., https://twitter.com/abarbashin/status/1558898536888033280.

[18] U.S. Foreign Military Studies Office, *The Russian Military and the Revolution in Military Affairs: A Case of the Oracle of Delphi or Cassandra?*, Jacob W. Kipp (Fort Leavenworth: Foreign Military Studies Office, June 1995), 27.

[19] U.S. Foreign Military Studies Office, *Confronting the RMA in Russia*, Jacob W. Kipp (Fort Leavenworth: Foreign Military Studies Office, June 1997), 4–5.

[20] Ibid., 8.

[21] U.S. Foreign Military Studies Office, *Russian Information-Psychological Actions: Implications for U.S. PSYOP*, Timothy L. Thomas (Fort Leavenworth: Foreign Military Studies Office, Winter 1997), 2.

[22] Ibid.

[23] Andrew Higgins, "The War That Continues to Shape Russia, 25 Years Later," *New York Times*, December 10, 2019, https://www.nytimes.com/2019/12/10/world/europe/photos-chechen-war-russia.html.

[24] See, for example, "Russia: Chechen War," World Peace Foundation at Tufts University, August 7, 2015, https://sites.tufts.edu/atrocityendings/2015/08/07/russia-1st-chechen-war.

[25] Toby Trister Gati, *Putin's Russia* (Washington, D.C.: Center for Strategic & International Studies, March 2000), https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0001qus_russia.pdf, 40.

[26] David Hoffman and John F. Harris, "Clinton, Yeltsin Gloss Over Chechen War," *Washington Post*, April 22, 1996, https://www.washingtonpost.com/history/2020/06/26/russian-election-interference-meddling.

[27] Jason Clinton Vaughn, *Russian Public Opinion and the Two Chechen Wars, 1994-1996 and 1999-2002: Formation and Evolution* (London: University College London, 2007), https://discovery.ucl.ac.uk/id/eprint/1445136/1/U592450.pdf, 191.

[28] *Russian Information-Psychological Actions*, 10.

[29] U.S. Foreign Military Studies Office, Emil Pain, translated by Robert R. Love, *The Second Chechen War: The Information Component* (Fort Leavenworth: Foreign Military Studies Office, July-August 2000), 8.

[30] Joe Cheravitch, *The Role of Russia's Military in Information Confrontation* (Washington, D.C.: Center for Naval Analyses, June 2021), 3.

[31] United States Department of State Global Engagement Center, "Report: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem," January 20, 2022, https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem.

[32] Dmitry Gusev et al., *Ears Wagging the Donkey: Modern Social Programming* (St. Petersburg, Russia: Izdatelskiy Dom Piter, 2006).

[33] Robert Horvath, *Putin's Preventive Counter-Revolution: Post-Soviet Authoritarianism and the Spectre of Velvet Revolution* (London, UK: Taylor & Francis, 2013).

[34] Russian Federation, *Information Security Doctrine of the Russian Federation*, 2000, https://base.garant.ru/182535, 1.

[35] Ibid.

[36] Ibid., 7.

[37] Ibid.

[38] Ibid.

[39] It also does not mirror a Western, nontechnological understanding of "information security," either; for example, if "information security" can also be understood as protecting state secrets, including "measures to frustrate foreign espionage" internally and "measures to protect military and diplomatic communications against foreign interception and exploitation," Russia's notion is still broader and encompasses the likes of press reporting and public perception. On the information security point, see: Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), https://people.exeter.ac.uk/mm394/Michael%20Herman%20Intelligence%20Power%20in%20Peace%20and%20War%20%201996.pdf, 165.

[40] *Information Security Doctrine of the Russian Federation*, 2000, 9.

[41] Russian Federation, *Foreign Policy Concept of the Russian Federation*, 2000, https://www.ng.ru/world/2000-07-11/1_concept.html.

[42] Ibid.

[43] Ibid.

[44] UK Conflict Studies Research Center, *Russian Foreign Policy 2000: The Near Abroad*, M. A. Smith (Shrivenham: Conflict Studies Research Center, December 2000), https://www.files.ethz.ch/isn/96793/00_Dec.pdf, 1.

[45] Russian Federation, *Military Doctrine of the Russian Federation*, 2000, https://www.ng.ru/politics/2000-04-22/5_doktrina.html.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Arkady Ostrovsky, *The Invention of Russia: The Rise of Putin and the Age of Fake News* (New York, NY: Penguin Books, 2015), 7–8.

[51] Mark Galeotti, "Putin's Hydra: Inside Russia›s Intelligence Services," European Council on Foreign Relations (ECFR), 2016, https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf.

[52] Amy Knight, *The KGB – Police and Politics in the Soviet Union* (Winchester, MA: Allen & Unwin, Inc., 1988), chapter 6.

[53] U.S. Treasury Department, "Treasury Targets Assets of Russian Financier who Attempted to Influence 2018 U.S. Elections," Press Release, September 30, 2019, https://home.treasury.gov/news/press-releases/sm787.

[54] Илья Клишин, "Максимальный Ретвит: Лайки на Запад," *Ведомости*, 21 Мая 2014, https://www.vedomosti.ru/newspaper/articles/2014/05/21/lajki-na-zapad.

[55] Anton Troianovski and Ellen Nakashima, "How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West," *Washington Post*, December 28, 2018, https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

[56] Kevin Riehle, *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present* (Bethesda, MD: National Intelligence University, 2022), 63–64.

[57] U.S. Treasury Department, "Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections," Press Release, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0126.

[58] РИА Новости, "Шойгу рассказал о задачах войск информационных операций," РИА Новости, 22 Февраля 2017, https://ria.ru/20170222/1488617708.html.

59 “Russian Intelligence Controlled Platforms, Chinese Sanctions Disinformation and More,” Disinfowatch, April 16, 2021, https://disinfowatch.org/disinfodigest-russian-intelligence-controlled-platforms-chinese-sanctions-disinformation-and-more.

60 “Fronton: A Botnet for Creation, Command, and Control of Coordinated Inauthentic Behavior,” Nisos, May 19, 2022, https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/fronton-report.pdf.

61 Ben Nimmo, “Anatomy of an Info-War: How Russia’s Propaganda Machine Works, and How to Counter It,” May 19, 2015, https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it.

62 Suzanne Labin, United States Senate, “Committee on the Judiciary. Subcommittee to Investigate the Administration of the Internal Security Act and Other Internal Security Laws” (Washington, DC: U.S. Government Printing Office, 1960), 2.

63 Russian Federation, *National Security Strategy of the Russian Federation*, 2015, https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf.

64 Marlene Laruelle, *Is Russia Fascist? Unravelling Propaganda East and West* (Ithaca, NY: Cornell University Press, 2021), 28.

65 Russian Federation, *Information Security Doctrine of the Russian Federation*, 2016, https://publicintelligence.net/ru-information-security-2016.

66 Ibid.

67 Ibid.

68 Ibid.

69 Ibid.

70 Ibid.

71 Russian Federation, *National Security Strategy of the Russian Federation*, March 2021, http://publication.pravo.gov.ru/Document/View/0001202107030001.

72 “What You Need to Know About Russia’s 2021 National Security Strategy,” Meduza, July 5, 2021, https://meduza.io/en/feature/2021/07/05/what-you-need-to-know-about-russia-s-2021-national-security-strategy.

73 Ibid.

74 Graeme P. Herd, *Understanding Russia’s Strategic Behavior: Imperial Strategic Culture and Putin’s Operational Role* (London: Routledge, 2022), 74.

75 “What You Need to Know About Russia’s 2021 National Security Strategy,” Meduza.

76 Andrey Vandenko, “Sergey Ivanov: Don’t Think the Kremlin Always Decides Everything, Sometimes It Doesn’t,” TASS, accessed August 24, 2022, https://tass.com/top-officials/829778.

77 Sergey Sukhanin, “Russia Adopts New Strategy for Development of Information Society,” Eurasia Daily Monitor, Jamestown Foundation, May 16, 2017, https://jamestown.org/program/russia-adopts-new-strategy-development-information-society.

78 Justin Sherman, *Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior* (Washington, DC: Atlantic Council, July 12, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior.

79 Zack Whittaker, “Documents Reveal How Russia Wiretaps Phone Companies,” TechCrunch, September 18, 2019, https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance.

80 Alena Epifanova, *Deciphering Russia’s “Sovereign Internet Law”: Tightening Control and Accelerating the Splinternet* (Berlin: German Council on Foreign Relations, January 2020), https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf.

81 Justin Sherman, “China’s War for Control of Global Internet Governance: The Chinese Government’s Campaign to Influence and Control the ITU” (July 2022): 10, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4174453.

[82] See, for example, Polina Kolozaridi and Dmitry Muravyov, "Contextualizing Sovereignty: A Critical Review of Competing Explanations of the Internet Governance in the (So-Called) Russian Case," *First Monday* 26, no. 5 (May 2021), https://doi.org/10.5210/fm.v26i5.11687.

[83] Ilona Stadnik, "Control by Infrastructure: Political Ambitions Meet Technical Implementations in RuNet," *First Monday* 26, no. 5 (April 2021), https://doi.org/10.5210/fm.v26i5.11693.

[84] Dan Milmo, "Russia Blocks Access to Facebook and Twitter," *The Guardian*, March 4, 2022, https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter. See also Simon Migliano and Samuel Woodhams, "Websites Blocked in Russia Since Ukraine Invasion," top10vpn.com, March 2, 2022, https://www.top10vpn.com/research/websites-blocked-in-russia.

[85] Diwen Xue et al., "Throttling of Twitter in Russia," Censored Planet, April 6, 2021, https://censoredplanet.org/throttling; Dylan Myles-Primakoff and Justin Sherman, "Russia Can't Afford to Block Twitter—Yet," *Foreign Policy*, April 30, 2021, https://foreignpolicy.com/2021/04/30/russia-block-twitter-telegram-online-censorship; Matt Burgess, "This is Why Russia's Attempts to Block Telegram Have Failed," *WIRED* UK, April 20, 2018, https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google; and Justin Sherman, "What's Behind Russia's Decision to Ditch Its Ban on Telegram?," Atlantic Council, June 26, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/whats-behind-russias-decision-to-ditch-its-ban-on-telegram.

[86] Paul Mozur, Adam Satariano, Aaron Krolik, and Aliza Aufrichtig, "'They Are Watching': Inside Russia's Vast Surveillance State," *New York Times*, September 22, 2022, https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html.

[87] Riya Baibhawi, "'Blessing in Disguise': Putin Says Exit of Companies Will Help Russia End Dependency on Foreign Technologies," *Republic World,* July 21, 2022, https://www.republicworld.com/world-news/russia-ukraine-crisis/putin-says-exit-of-companies-will-help-russia-end-dependency-on-foreign-technologies-articleshow.html.

[88] And "to the Russian Federation," though in practice, national security was often equated with regime security.

[89] David Hoffman, "Yeltsin's Immunity Upheld by Duma Vote," *Washington Post*, March 30, 2000, https://www.washingtonpost.com/wp-srv/WPcap/2000-03/30/090r-033000-idx.html.

[90] Eliot Borenstein, *Plots Against Russia: Conspiracy and Fantasy After Socialism* (Cornell University Press, 2019), 27.

[91] 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.

[92] Swedish Defense Research Agency. *War by Non-Military Means: Understanding Russian Information Warfare*, FOI-R–4065–SE, Ulrik Franke (Stockholm: Defense Research Agency, March 2015), 15.

[93] For a capturing of this view, see: "Exporting Revolution," RT, February 1, 2012, https://www.rt.com/usa/revolution-activists-world-people-297.

[94] Andrei Soldatov and Irina Borogan, "How Edward Snowden Inadvertently Helped Vladimir Putin's Internet Crackdown," *BuzzFeed News*, September 2, 2015, https://www.buzzfeednews.com/article/andreisoldatov/how-edward-snowden-inadvertenly-helped-vladimir-putins-inter.

[95] "Russia's Putin: Panama Papers Are a 'Provocation,'" Reuters, April 14, 2016, https://www.reuters.com/article/us-russia-putin-panamapapers/russias-putin-panama-papers-are-a-provocation-idUSKCN0XB16D; Adam Taylor, "Putin Saw the Panama Papers as a Personal Attack and May Have Wanted Revenge, Russian Authors Say," *Washington Post*, August 28, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/08/28/putin-saw-the-panama-papers-as-a-personal-attack-and-may-have-wanted-revenge-russian-authors-say.

[96] Swedish Defense Research Agency, *Russian Politics and the Internet in 2012*, FOI-R–3590–SE, Ulrik Franke and Carolina Vendil Pallin (Stockholm: Defense Research Agency, December 2012), 44.

97 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.

98 Ilya Yablokov, *Fortress Russia: Conspiracy Theories in Post-Soviet Russia* (Medford: MA; Polity, 2018), 183–184.

99 Fiona Hill, "Mr. Putin and the Art of the Offensive Defense: Approaches to Foreign Policy (Part Two)," Brookings Institution, March 16, 2014, https://www.brookings.edu/articles/mr-putin-and-the-art-of-the-offensive-defense-approaches-to-foreign-policy-part-two.

100 Gavin Wilde and Justin Sherman, *Targeting Ukraine Through Washington: Russian Election Interference, Ukraine, and the 2024 US Election* (Washington, DC: Atlantic Council, March 14, 2022), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/targeting-ukraine-through-washington.

101 "Russian Envoy Says 'Leaks' of Russian Operation in Ukraine Are Part of Information War," TASS, February 4, 2022, https://tass.com/politics/1398427.

102 "Putin's Speech on Annexation: What Exactly Did He Say?," Al Jazeera, accessed October 3, 2022, https://www.aljazeera.com/news/2022/9/30/russia-ukraine-war-putins-annexation-speech-what-did-he-say.

103 "Shoigu: Information Becomes Another Armed Forces Component," Interfax, March 28, 2015, https://interfax.com/newsroom/top-stories/37293.

104 "Russian General Staff Chief Sees No Prerequisite for Massive War," Interfax, December 18, 2019, https://interfax.com/newsroom/top-stories/18119.

105 Dmitri Trenin, "How Russia Must Reinvent Itself to Defeat the West's 'Hybrid War,'" Russian International Affairs Council, July 11, 2022, https://russiancouncil.ru/en/analytics-and-comments/comments/how-russia-must-reinvent-itself-to-defeat-the-west-s-hybrid-war.

106 Leonid Bershidsky, "Putin's War Hawks Are No Longer in Step," *Washington Post*, October 5, 2022, https://www.washingtonpost.com/business/putins-war-hawks-are-no-longer-in-step/2022/10/05/6371bb58-446b-11ed-be17-89cbe6b8c0a5_story.html.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org