Social Media Weaponization
The Biohazard of Russian Disinformation Campaigns

By Sarah Jacobs Gamberini

In a renewed era of Great Power competition, the United States is faced with adversaries engaging across multiple domains without the traditional distinctions of war and peace. America’s competitors are regularly operating below the threshold that would warrant a military response, including on the information battlefield. The blurred red lines that result from covert information operations waged by foreign actors on the Internet will force a change in how the United States operates and how its society consumes information.

Russia used tactics of influence and coercion long before social media allowed for nearly ubiquitous access to its targets and a prolific capability for controlling a narrative and manipulating the hearts and minds of a population on a range of sensitive societal issues, including public health.

Russia has a long history of seeking to project power and influence while playing with a technological and geopolitical handicap. Given its history and a geographic location with many bordering...
nations, it sees itself as constantly besieged from all sides, but particularly by the West. Since the nadir of Soviet dissolution, Russia has fought to rebalance power and contemporaneously reduce American influence. But without equivalent conventional military might, Russia has turned to other asymmetric advantages to compensate in its competition with the United States. Social media has provided a unique tool kit to manipulate narratives and amplify societal divisions in an effort to weaken the United States in ways previously unimaginable. While Russian weaponization of information is not new the intersection of Russian disinformation, public health crises, and vulnerability to bioevents presents new and troubling homeland and national security threats for the United States.

The United States is diverse, pluralistic, and democratic. These characteristics, its founding principles, are also its strengths as a nation. But to U.S. adversaries, including Russia, they are potential weaknesses to exploit. One strategic goal of Russia’s influence operations is to weaken the United States and its allies, which Russia views as operating too close to its sphere of influence, what it refers to as its “near abroad.”

Time and again, Russia has used familiar influence tactics to spread disinformation in an attempt to weaken U.S. democratic society and undermine America’s reputation on the world stage. From Russia’s interference in the 2016 Presidential election to spreading hoaxes during the 2020 global pandemic, Russia is exploiting America’s divisions with disinformation to amplify discord in the United States and undermine its institutions. As Russia targets issues of public health in this way, there will be tremendous implications for American citizens and the U.S. health system. The world is grappling with an “infodemic” as well as a pandemic, and both require a whole-of-society approach to be successfully addressed.

Russia Under Siege

Over centuries, Russia has experienced attacks from the Teutonic Knights, Napoleon, and Nazi Germany, and, since the end of the Cold War, encroachment from the United States and the North Atlantic Treaty Organization (NATO). It views the United States, NATO, and the European Union as committed to weakening Russia, eliminating its sphere of influence, and ensuring sustained U.S.-Western unipolar dominance. This assessment derives from a strong Russian belief that the United States broke its word that NATO would move “not one inch eastward,” as stated by then-U.S. Secretary of State James Baker in the aftermath of the Soviet dissolution. Russia touts the West’s “interference” during the Ukrainian revolution as further evidence that the United States and NATO are meddling too much in its area of influence. It views this infringement on what it perceives as its near abroad as an unacceptable affront.

Russia sees Western dominance manifested socially and culturally (for example, Western entertainment seeking to replace Russian culture, values, and language), politically (the West fomenting “color revolutions” in Russia and the former Soviet Union), and militarily (the United States geographically encircling Russia with NATO expansion and technologically ringing Russia with missile defenses and bases). Moreover, Russia has long feared it is behind the West in science and technology. Russia has, at times, achieved parity in certain defense platforms but generally struggles to keep pace, thus relying heavily on traditional weapons of mass destruction, such as its substantial nuclear arsenal, to offset U.S. conventional might. Russia similarly lags in technologies for civilian applications. Underlying all this are vast and troubling demographic and health challenges (a declining birth rate and high death rate from unnatural causes, including widespread alcoholism). These factors have led to Russia viewing itself in a constant state of besiegment and deficiency.

Much of what shapes and propels Russia’s worldview today is based on former Prime Minister Yevgeny Primakov’s doctrine that rejects the United States as a hegemon and seeks a multipolar world and the reestablishment of Russia as the main regional power in the former Soviet region. Since the end of the Cold War, Russia has had to be calculating and creative to balance its economic, military, and technological disadvantages to compete with the United States, maximizing less conventional tools of war, including covert operations within the information domain.

During the Cold War, the Soviet Union used active measures to influence nations in coercive ways distinct from espionage and counterintelligence. Active measures included disinformation, political influence operations, and controlling media and messaging with the goal of discrediting or influencing the West, which are echoed in Russia’s modern-day tactics. This type of warfare and other measures below the threshold of actual use of force have been variously referred to in the West as Russia’s asymmetric, gray zone, hybrid, or next-generation warfare. However, the term cross-domain warfare better reflects the current Russian method of shaping the security environment using an integrated approach of all military and nonmilitary devices to achieve its strategic goals.

In a response to the Arab Spring uprisings, which Russia believed to be incited by the West, General Valery Gerasimov (now chief of the General Staff) publicly discussed how to prevent similar uprisings in Russia. In his speech, Gerasimov cited control of information as central to victory. This speech, which has been overstated as a Russian military doctrine, did describe how Russia should operate simultaneously across multiple domains—military, political, cyber, and information warfare—to achieve strategic goals. In March 2019, Gerasimov spoke on the shift of warfare to the information sphere and labeled information technologies as “one of the most promising types of weapons” to be used covertly “not only against critically important infrastructural institutions, but also against the population of a country, directly influencing the condition of a state’s national security.” Information is but one aspect of cross-domain warfare. Another important facet of this Russian thinking is the belief that the customary distinction between
wartime and peacetime no longer exists. These blurred red lines have been demonstrated beyond speeches or doctrine, for instance in Russia’s employment of this malign activity below the U.S. threshold of armed conflict—little green men in Crimea and Eastern Ukraine, “unaffiliated” private military groups in Syria, use of Novichok (a Cold War-era chemical weapon first developed by the Soviet Union) in the United Kingdom, and numerous cyber attacks—and by the nature of cloaked activities, likely many more. Yet Russia has protected itself from military response because attribution and proportionality are thrown into question by their deniability and obfuscation.

Old Influence Operations Playbook, New Media Tools

Russia’s present leaders fear that U.S. advantages in information technology allow Washington and its allies to undermine Russian social, cultural, and political institutions as part of its broader campaign to ensure Western geopolitical dominance. The Kremlin sees information as a new type of weapon and views all forms of information, across all platforms, as potential sources of power to be weaponized. Russia believes that the West is using all forms of information technology against them—from persistent satellite television and the Internet bombarding Russian citizens with what it views as overtly anti-Russian messages to social media as tools for coordinating activists and provocateurs in uprisings in former Soviet republics. Finally, Russia sees U.S. space, intelligence, surveillance, and reconnaissance, as well as other information technology systems, as networked military capabilities designed to summarily dismantle any opponent slow to adapt.

Russia has responded to this threat of the information age in a number of ways. It is working to create a “Russia only” Internet with aspirations of creating a Russian equivalent of China’s “Great Firewall.” Russian news and propaganda (for example, the state-controlled television network RT and online “news” aggregators such as Sputnik) are beamed in to counter Western cable news. Additionally, until Russia has its own information operations military systems, it holds Western systems at risk both physically (for example, antispace capabilities) and with cyber attacks. Finally, the Russian government’s active Internet presence pervades the social media landscape using large numbers of Russian Web brigades, troll farms, and automated bots to disseminate propaganda and flood hashtags.
media machine is employed to great
effect to influence its adversaries and
their populations. Russian trolls utilize
the power of narratives online, focusing
on simple messages targeting a cohesive
group so that its message will then be
shared and further amplified by foreign
targets. They have a keen understanding
that strong emotions spread quickly on-
line and that, given the right prompting,
people love nothing more than arguing
and solidifying entrenched viewpoints.
As with Soviet active measures, Russia’s
goals in weaponizing social media are
to foment chaos, create distrust in U.S.
institutions, and target the preexisting
divisions in the country. All this makes
it harder for the United States to form
a unified response to counter Russia in
more traditional domains.

Misinformation and Disinformation Campaigns
Americans are regularly confronted with
fake news in many forms from both
domestic and foreign sources. There
is a spectrum of false content online,
from well-meaning friends on Facebook
thoughtlessly sharing misinformation
they assume to be true to more malev-
olent and targeted propaganda-like
content designed to intentionally
confuse and deceive. Therefore, it is
important to understand the difference
between the terms disinformation and
misinformation. Disinformation is the
malicious and intentional development
and propagation of false information,
while misinformation is the inadvertent
spreading of erroneous content. Russia
relies on both. A misinformation cam-
paign, for example, could be employed
maliciously by relying on unwitting
users to spread false information.

Bill Gates, when asked in 1995 about
false information spreading on the then-
new “Net,” stated that fake news would
be easy to debunk because there would
be more people checking the facts and
information would be spread from friend
to friend, a more trustworthy transaction.
But as we now know, it is this very aspect
of social media that allows for misinfor-
mation campaigns to succeed and for fake
news to flourish. Another core challenge
that makes online influence operations
so successful is that once information is
disseminated and consumed, it is hard
to retract it from people’s minds. The
tools that make social media so useful for
connecting, sharing, and organizing are
the same tools that allow malign actors
to take advantage and manipulate. This
fact—paired with a need for fast news
without waiting for validating research or
fact-checking, the ease of sharing on so-
cial media platforms, and the fact that the
most divisive topics are deeply emotional
(for example, public health and race
relations)—makes the United States the
perfect target of this type of social media
weapon.

Russia’s modus operandi for social
media exploitation is predictable: Identify
a contentious issue, employ bots and
trolls on various social media platforms to
spread divisive rhetoric, amplify debates,
and promote discord. One of the most
publicized influence operations by Russia
was its interference in the U.S. elections
in 2016. But Moscow’s efforts are
broader than elections and exist as part of
an ongoing deliberate campaign against
the U.S. public. As a diverse, pluralist so-
ciety, the existence of societal fissures for
target are numerous.

In 2019, leaked documents revealed
that Russia considered targeting one of
America’s deepest and oldest fault lines as
a nation: race. Documents showed Russia
considered training African-Americans in
combat and sabotage before returning
these individuals to the United States to
create a Pan-African state in the southern
United States, physically breaking apart
the country. The proposal, which was
never enacted, intended to “destabilize
the internal situation of the [United
States].” Russia recognizes that slav-
eroy and the resulting centuries-long
inequality is the original American sin
and the ultimate fissure to be exploited.
Russian influence operations were used
against African-Americans in advance of
the 2016 election, and more recently
Russia has exploited the Black Lives
Matter movement by flooding Twitter
hashtags—a technique used to dilute
legitimate related content, thus inhibiting
the social media platform as a means of
communication during protests. It is
important to note that Russia’s goal is
rarely to promote one side of any issue,
but to stir the pot and enflame ten-
sions—U.S. self-destruction would be
Russia’s ideal victory.

Russia’s information warfare tactics
are moving target, making them diffi-
cult to understand and counter. In June
2020, a large-scale, persistent 6-year-long
disinformation campaign out of Russia
was exposed. The campaign used new
methods for targeting the West and
Ukraine on issues ranging from denying
Russian doping in international sporting
events to the broader praising of Russia
and its government and highlighting U.S.
and NATO aggression and interference
in other countries. The campaign was
labeled “Secondary Infektion” as an
homage to Operation Infektion, a Cold
War callback to the 1980s disinforma-
tion campaign when the Soviet Union
employed malicious messaging to sell the
conspiracy theory that the U.S. military
created the AIDS virus as a tool of war.
Of particular interest in Russia’s methods
during Secondary Infektion was the large
number of “burner” accounts used for a
single misleading tweet and then aban-
don. As opposed to previous efforts
to build social media accounts with a fol-
lowing, credibility, and trust, this shows
Russia’s recognition of Americans’ media
illiteracy, inability to recognize fake news,
and unwillingness to research deeper than
a single tweet. Few people take the time
to seek the source of information, and so
far Russia has been proved correct in its
hypothesis. As much as can be under-
stood about Russia’s goals and methods,
the inexpensive and ubiquitous nature of
social media empowers disinformation
efforts to shift and flex to changes in
the social media algorithms as needed.
It could also release prolific amounts of
false and harmful information, which, if
only marginally successful, could have an
outsized impact.

Amplifying Public Health Debates
Russia clearly recognizes how to iden-
tify, exploit, and amplify U.S. political
tensions and the Nation’s racial wounds
Public health is another area of acute debate in the United States, and one that is ideal for Russian targeting. Public health issues are both personal and societal, and therefore any discussion of related topics is often full of emotion and an eagerness to quickly obtain information. Often, people are more trusting of health advice from friends, family, or influencers they trust than impersonal institutions. A National Institutes of Health study found that “in the [United States], eight in ten Internet users search for health information online, and 74 percent of these people use social media.” This makes public health issues such as COVID-19 or measles an ideal target for Russian social media weaponization. It is divisive and emotional, and could realistically physically weaken the United States.

The anti-vaccination (anti-vaxxers) movement espouses a belief that vaccinations are at best unnecessary and at worst cause physical harm, including autism and seizures. The movement is fueled by a deep mistrust of authority and the existence of echo chambers online that encourage the spread of misinformation quickly and among friends. All the fake news about vaccines is actually harder to counter due to their amazing success. Diseases such as measles are seen as relics of the past that have long been eradicated and do not touch modern U.S. society. However, the United States is experiencing the greatest number of measles cases since 1992 in parts of the country where a significant percentage of the population has opted out of vaccines. Vaccines are successful with herd immunity when, depending on how contagious the disease, a certain percentage of the society is vaccinated in order to protect a small number of the society who cannot get vaccines for various reasons (for example, children, pregnant women, and other vulnerable populations).

For a disease as contagious as measles, herd immunity occurs only if approximately 94 percent of a population is vaccinated; even a small change in vaccination numbers could bring back this disease, declared eliminated in the United States in 2000. The result of erroneous fear-mongering about vaccines is a society that is physically degraded by previously eliminated diseases. And now that the world grapples with the novel coronavirus causing COVID-19, large pockets of society are loathe to be told how to protect themselves and their communities. If Americans are rebelling against the science that underlies why masks and physical distancing are good preventative measures, it is foreseeable that there will be skepticism over a vaccine once it is available. The United States has been lulled into a false sense of security due to the very success of vaccines.
These public health crises would be atrocious enough without attempts by foreign adversaries to exacerbate them. The *Journal of Public Health* uncovered that the same Russian Internet Research Agency—led by Yevgeny Prigozhin (a close friend of Russian President Vladimir Putin) and indicted in Robert Mueller’s investigation report on Russian election interference—was also behind deploying bots and trolls to spread disinformation on vaccinations. In its analysis, the journal article notes that Russian bots and trolls tweeted an equal number of pro- and anti-vaccine tweets. The goal, it seems, was to stir the debate and bring people into their corners, further entrenching their own viewpoints. Russia’s goal is to amplify and normalize the debate and firmly cement divisions. The health repercussions that result from a normalized vaccination debate were unlikely Russia’s primary goal—merely a byproduct—but the fact that Russia could so callously degrade the health of U.S. citizens as a secondary effect of its influence operations is egregious. Given the ties to the Russian president, it presents further concerns about how this campaign may be endorsed by the state and what that means for how the United States responds. Deniability, however, is the crux of Putin’s success in this area.

Russia has similarly used its predictable tactics against the United States to stoke fear and chaos and to undercut the U.S. response during the COVID-19 pandemic. False narratives spread by Russian state media, trolls, and bots range from conspiracy theories that the virus was variously created by migrants, as a U.S. bioweapon, or to benefit the virus was brought to Wuhan by the U.S. Army during Olympics-style military games in 2019. This adds to concerns that Russia’s influence operations are attractive to other U.S. adversaries and will continue to be a prime method of attack from multiple actors.

These attacks on public health present a threat to homeland and national security. The anti-vaxxer movement risks increasing U.S. vulnerability to infectious diseases. Looking forward to how these same tactics may be used against a COVID-19 vaccine once it is available, we must consider the implications of maligning messaging about vaccines from both domestic and foreign sources. Beyond propagating doubt in U.S. institutions (for example, hospitals/testing and government organizations such as the Centers for Disease Control and Prevention), these campaigns result in doubt of basic science (for example, people not wearing masks and possibly not trusting a future vaccine). By amplifying public health debates and not advocating for one side, Russia has helped normalize a previously fringe discussion rejecting basic science underlying vaccines and disease prevention. U.S. health institutions are faced with a crisis of trust as scientific facts about these contagious diseases are degraded by both intentional and inadvertent lies.

There are longer term effects of amplifying the anti-vaxxer movement. Beyond the health and institutional concerns, there are also costs to the U.S. health system, as well as costs associated with quarantining. The movement is a distraction for healthcare professionals who are overburdened in this crisis as it is, and for local, state, and Federal governments that must devote time and resources to countering this false information. Furthermore, natural or intentional biothreats (including natural biothreats exacerbated by foreign adversary messaging) could potentially inhibit the military’s ability to project power abroad. The pandemic has shown how vulnerable forces are to contracting diseases such as COVID-19, and there is renewed awareness of this threat by our adversaries. The United States has also relied on the military to help with expanded hospital bed capacity at home, all of which stretches resources and in theory means fewer forces deployed.

If anti-vaxxers grow in number and/or influence, this could weaken the U.S. ability to respond to any type of biological threat—natural or human-made. Bioweapons of the future are less likely to be those agents historically weaponized and will likely target civilian populations. Biological agents have always been difficult to weaponize because of the quantity and dissemination needed to have widespread, mass impact. As the large-scale programs of the Cold War gave way to the terrorist threat, the biothreat scenario of a biological agent-filled test tube dropped in a subway has been overtaken by disturbing real-world pandemic scenarios.

Russia and other U.S. adversaries are certainly noting U.S. vulnerabilities in its response to the coronavirus. All this presents renewed concerns of a future biological weapon, the effects of which could be further enabled by information warfare. These indiscriminate information attacks on public health reveal how Russia will exploit any divisions within the United States, even to the point of wreaking public health havoc. These attacks on public health highlight the type of ruthless adversary the United States faces. At a certain point, the United States must contemplate whether this interference in its public health is a biothreat caused by a foreign adversary.

**Countering the Influence of Influence Operations**

Asymmetric warfare is being waged against the United States and its citizens daily across multiple platforms and with expanded notions of what constitutes acceptable warfare. Though the effects of Russia’s information operations on health matters are grave, we have not yet codified these societal attacks as warfare, and therefore they do not rise to the level of military response. The United States requires a comprehensive, whole-of-government solution to counter these actions as well as a whole-of-society awareness to be part
of the solution. Governments and companies could raise barriers to make the efforts harder, and people could be better informed on how to identify misinformation and disinformation, thereby making it less effective. The combined effects could lead to reducing Russia’s influence, if not deterring it altogether. The solution will be complex, at all levels of society, and it begins and ends with an informed public with high media literacy.

Government can help but cannot alone solve the problem of disinformation any more than it can solely solve public health challenges. The 2020 National Defense Authorization Act called for the Director of National Intelligence to create a Malign Foreign Influence Response Center to coordinate and integrate across the Intelligence Community on issues of foreign influence; as of this writing, this center has not yet been established as authorized.49 In the past, there has been work to counter Russian messaging in pockets of the U.S. Government, but it has often been limited to addressing overt propaganda rather than the low-level guerrilla exploitation of social media we face today. During the Cold War, the U.S. Active Measures Working Group was established not only to counter Soviet disinformation but also to sensitize societies to be able to recognize Russian interference for themselves.40 It would seem this type of whole-of-government commitment to countering disinformation would be timely to revive, perhaps in the form of the Malign Foreign Influence Response Center. Even so, it would not be enough on its own and certainly not with intelligence-only participation. The Department of State’s Global Engagement Center is doing its part to identify, expose, and counter disinformation, but without higher visibility by U.S. citizens and the Nation’s adversaries, it cannot be fully successful.41

One of the most effective things that the U.S. Government could do to counter disinformation is practice consistent messaging and, in the case of disinformation and public health, deliver a consistent, science-based message. During the aftermath of the attempted assassination of Sergei Skripal in the United Kingdom using Novichok, Russia put out hundreds of conflicting narratives to confuse, deflect, and deny its involvement.42 The United Kingdom, rather than play whack-a-mole by attempting to disprove each falsehood, put out a consistent, science-based message that helped reveal the lies and inconsistencies within the Russian messaging.43

Furthermore, the United States must call out Russia for its cross-domain misdeeds, including in the area of information operations. The United States
must respond directly to these threats through targeted sanctions, international condemnation in multilateral forums, and other asymmetric responses. Despite Russia’s attempts at deniability of its role in these campaigns, the United States and its allies should present evidence in a forum such as the United Nations Security Council to show the links between these bad actors and the Russian government. Because of Russia’s veto on the Security Council, no resolutions would be passed, but this high-visibility action would highlight to the world Russia’s malign activities and perhaps rally support of other nations around stopping this bad actor. The United States needs to assess Russia’s actions not only by its methods but also by its effects. If Russia’s social media meddling results in a physically weakened society, even inadvertently, the United States must consider treating these actions as more akin to a bioattack than to a cyber attack.

Industry partners would play an important role in the solution. Silicon Valley, the home of the platforms on which this misinformation and disinformation spreads, struggles with balancing the hazards of fake news with freedom of speech and shareholder pressure and therefore has not done nearly enough to combat the information warfare waged on social media sites. As a democratic society, we will not be able to shut down this threat but rather must accept that false content exists and focus on empowering companies and users to identify and expose this content. In the midst of COVID-19, Twitter implemented a new system to identify and draw attention to articles and posts that may be considered dangerous or spreading disinformation. In June 2020, Twitter slapped a fact-check on Chinese Ministry of Foreign Affairs official Lijian Zhou’s tweet advertising a bioweapon conspiracy theory. While this social media policing is fraught with censorship and free speech concerns and a “whack-a-troll” approach is inefficient, it is a good first step to draw users’ attention to the reality that all tweets, even from verified accounts, must be read with a healthy dose of skepticism.43

As social media continues to evolve into more visual platforms including TikTok, it will be important to flag manipulated media such as artificial intelligence–enabled deepfakes. Though it presents a great challenge, as the technology to create believable deepfakes improves, so does the technology to counter it. Tech companies are investing in methods that reveal clues for when an image has been altered, such as water droplets on an image, a tell-tale sign of media manipulation.44 There are also algorithms to assess when the title of an article does not match the content, which could then alert users and discourage them from sharing misleading information based on the title alone.45 Incorporating these technologies into social media platforms to flag manipulated media before it is shared further would both slow the spread of false information and help create a society with a healthy level of skepticism and improved media literacy. To maintain freedom to access all information, we must ensure users have the tools they need to help recognize and counter disinformation.

The most important change that must happen to effectively counter Russian disinformation is an educated and empowered U.S. population capable of identifying and discrediting Russian disinformation. Deterrence will not work to stop or slow Russia’s disinformation efforts; the United States should therefore focus on inoculating the population against Russia’s attempts to influence the information domain. A challenge of countering disinformation during a public health crisis is balancing the need for a media-literate society that is highly attuned to detect false information, while inherently trusting institutions in equal measure. The United States must invest in media literacy and instill an awareness of the methods and goals of these targeted campaigns. In addition to making the public aware of Russia’s role in these targeted information attacks, Americans must assess other fissures in U.S. society that might be targeted in this manner in the future.

Russia’s theory of the United States is that its diversity is its weakness. To counter this narrative, the United States must show strength in its pluralism and work as a country to heal the divisions that make it the ideal target for this methodology. Russia is drilling deeper into the preexisting fault lines of American society—distracting, dividing, and weakening. Particularly in the face of the Presidential election and a modern pandemic, all Americans must be vigilant in questioning where information originates and hyperaware of the seams and fissures in American society that are primed for this type of attack. Healing the wounds and divisions of an increasingly polarized nation will go a long way toward protecting the United States from Russia’s social media weaponization.

Gerard Toal, Near Abroad: Putin, the West, and the Contest Over Ukraine and the Caucasus (New York: Oxford University Press, 2017).


Elizabeth Townsend, Understanding


Gamberini and Moodie, “The Virus of Disinformation.”


40 Amy Klobuchar et al., “Letter to Secretary Esper, Director Ratcliffe, Director Wray, General Nakasone, and Acting Secretary Wolf,” U.S. Senate, 2020, available at <www.klobuchar.senate.gov/public/_cache/files/1/d199087c-0a26-4242-a0cf-a5867d208a18/D1FD0C7DAF35260CBB3D51CBADB52062d0sinformationletter.pdf>.


45 Ibid.