Hostile State Disinformation in the Internet Age

Richard A. Clarke

Foreign actors, particularly Russia and China, are using disinformation as a tool to sow doubts and counterfactuals within the U.S. population. This tactic is not new. From Nazi influence campaigns in the United States to the Soviets spreading lies about the origins of HIV, disinformation has been a powerful tool throughout history. The modern "information age" and the reach of the internet has only exacerbated the impact of these sophisticated campaigns. What then can be done to limit the future effectiveness of the dissemination of foreign states' disinformation? Who has the responsibility and where does the First Amendment draw the boundaries of jurisdiction?

State-sponsored disinformation (SSD) aimed at other nations' populations is a tactic that has been used for millennia. But SSD powered by internet social media is a far more powerful tool than the U.S. government had, until recently, assumed. Such disinformation can erode trust in government, set societal groups – sometimes violently – against each other, prevent national unity, amplify deep political and social divisions, and lead people to take disruptive action in the real world.

In part because of a realization of the power of SSD, legislators, government officials, corporate officials, media figures, and academics have begun debating what measures might be appropriate to reduce the destructive effects of internet disinformation. Most of the proposed solutions have technical or practical difficulties, but more important, they may erode the First Amendment's guarantee of free speech and expression. Foreign powers, however, do not have First Amendment rights. Therefore, in keeping with the Constitution, the U.S. government can act to counter SSD if it can establish clearly that the information is being disseminated by a state actor. If the government can act constitutionally against SSD, can it do so effectively? Or are new legal authorities required?

The federal government already has numerous legal tools to restrict activity in the United States by hostile nations. Some of those tools have recently been used to address hostile powers' malign "influence operations," including internet-powered disinformation. Nonetheless, SSD from several nations continues. Rus-

https://doi.org/10.1162/daed_a_02088

sia in particular runs a sophisticated campaign aimed at America's fissures that has the potential to greatly amplify divisions in this country, negatively affect public policy, and perhaps stimulate violence.[1]

Russia has created or amplified disinformation targeting U.S. audiences on such issues as the character of U.S. presidential candidates, the efficacy of vaccines, Martin Luther King Jr., the legitimacy of international peace accords, and many other topics that vary from believable to the outlandish.[2] While the topics and the social media messages may seem absurd to many Americans, they do gain traction with some – perhaps enough to make a difference. There is every reason to believe that Russian SSD had a significant influence on, for example, the United Kingdom's referendum on Brexit and the 2016 U.S. presidential election. But acting to block such SSD does risk spilling over into actions limiting citizens' constitutional rights.

The effectiveness of internet-powered, hostile foreign government disinformation, used as part of "influence operations" or "hybrid war," stems in part from the facts that the foreign role is usually well hidden, the damage done by foreign operations may be slow and subtle, and the visible actors are usually Americans who believe they are fully self-motivated. Historically, allegations of "foreign ties" have been used to justify suppression of Americans dissenting from wars and other government international activities. Thus, government sanctions against SSD, such as regulation of the content of social media, should be carefully monitored for abuse and should be directed at the state sponsor, not the witting or unwitting citizen.

Government regulation of social media is problematic due to the difficulty of establishing the criteria for banning expression and because interpretation is inevitably required during implementation. The government could use its resources to publicly identify the foreign origins and actors behind malicious SSD. It could share that data with social media organizations and request they block or label it. A voluntary organization sponsored by social media platforms could speedily review such government requests and make recommendations. Giving the government the regulatory capability to block social media postings – other than those clearly promoting criminal activity such as child pornography, illegal drug trafficking, or human smuggling – could lead to future abuses by politically motivated regulators.

Over time, we have moved from the Cold War to the hybrid war. Russia and China are today engaged in a hybrid war with the United States. Aspects of this kind of competition include hacking into computer networks, publicly revealing (and sometimes altering) the data they hack, running active espionage programs, creating and disseminating disinformation, inventing American identities online, and stoking internal dissent on emotionally contentious issues.[3]

Both Russia and China have similar goals: to turn America's attention inward to limit its foreign presence and involvement, to weaken U.S. national unity, to sow dissension, and to undermine worldwide confidence in the U.S. government

and its system of democracy and liberties. Both openly state their goal is to subvert what they see as a hyperpower's global hegemony.[4] Unstated is the goal of reducing interest within their own countries in American-style democracy and human rights guarantees ("See what calamity and dysfunction it brings in America").

Russia (then the Soviet Union) and China had similar goals during the Cold War (1945–1989), but that competition did not morph into a conventional or nuclear war (although there were many proxy wars and Chinese forces did directly combat U.S. forces in the Korean War). Nor did the tools of hybrid war succeed then in causing significant domestic security problems for the United States.

There are, however, reasons to think that hybrid war may be more damaging and more successful now than in its earlier incarnations. About the same time that the Cold War ended, the Information Age began. With the global rise of the internet came the morphing of news media, the creation and rapid mass adoption of social media, and now the introduction of generative artificial intelligence (GenAI), complete with fake news and synthetic personas.

Many believe it is necessary to restrict First Amendment protections for those who disseminate "fake news," for those among them who are foreign actors, or at the very least for synthetic personas. Advocates of further limitations point to the first known successful attempt by a hostile foreign power to affect the outcome of a U.S. presidential election (2016) as the prime example of the harm that unrestricted, foreign-generated or -amplified expression can cause.[5] They see a hidden, or sometimes not-too-covert, Russian hand in the gun control debate, anti-vaccination lobbying, and both sides of the Black Lives Matter movement, and they wonder what role Moscow might have played (if any) in the January 6th sedition. Convincing fake videos, such as one of former president Barack Obama seeming to say things that he never uttered, give rise to concerns about what damage unrestricted GenAI could soon bring.[6]

These concerns can (and should) cause us to review what restrictions we have and what further restrictions we might need on the First Amendment's protections for hostile foreign powers and their agents, witting and unwitting. But let us first turn to some important definitions.

Big lie: A term first used by the Nazis, meant to suggest that something that should be on its face preposterous might be believed if properly asserted by credible sources. It is first attributed to Adolph Hitler and his contention that "in the big lie there is always a certain force of credibility; because the broad masses of a nation are always more easily corrupted in the deeper strata of their emotional nature than consciously or voluntarily; and thus [are more likely to] fall victims to the big lie than the small lie."[7]

Cyber war: Computer operations designed to create damage, disruption, or destruction of computer networks and/or devices controlled by software.

Deepfakes: Images and videos made with the use of GenAI that appear to show people doing and/or saying things that they never did or said. The software realistically mimics voices and styles of speaking, as well as moves the lips in the image in synchronization with the audio track.

Disinformation: A term first used by the Soviet Union to characterize state-sponsored strategic deception spread through a variety of means, both at home and abroad. It became a central activity of Soviet intelligence as early as the 1920s and continued as a major program component through the Cold War. Russian intelligence in the twenty-first century has resumed the use of disinformation as a significant tool.[8]

Fake news: Information in traditional or newer media, including social media, which is (or is claimed to be) intentionally erroneous; also, a characterization of news sources that regularly carry intentionally erroneous material.

Fake personas: Actors on social media platforms and elsewhere whose identity is intentionally inaccurate, assumed, or fabricated. Russian and Chinese agents have created thousands of social media accounts with American names and hometowns to convince American readers that the views that are being espoused are those of their neighbors or people like them.[9]

Hybrid war: The use of a panoply of techniques employed in the absence of, before, or during a conventional military conflict, such as unauthorized entry into computer networks, public dissemination of the hacked material in its original or altered state, cyber warfare, the spread of disinformation, activities designed to create dissent and disruption in the enemy state, sabotage, espionage, covert action, subversion and, in some uses, special forces operations behind enemy lines.

Information warfare: State use of true and/or false accounts and themes to persuade an enemy or potential enemy audience to act in a way that is beneficial to that state actor; the role of the state actor as the originator of the information may or may not be overt.

Influence operations: A campaign by a state actor to cause a foreign audience to support the policies of the state actor or to oppose the policies of an opposing state; the campaign may include bribery of foreign officials or media personnel, the spread of disinformation, propagation of truthful stories that support the image of the state actor or damage the image of another nation, foreign development assistance, disaster relief aid, direct foreign investment, military and security assistance, training, scholarships, and cultural exchanges.

Psychological operations: A term used by the U.S. military until the 1990s to describe its activities that are now known as information warfare and/or influence operations.

Sleepers: Foreign intelligence personnel who create or use a false identity of a citizen of a target country and then live in that country, usually for an extended period, usually with jobs and families to add to the credibility of their cover story;

a Soviet and now Russian intelligence technique that entered American public consciousness with the exposure of a network of such intelligence personnel in the United States in 2010, later popularized in the television series *The Americans*.

Synthetic personas: Similar to fake personas, but also employing facial and other images, still or video, created by GenAI programs. Additionally, video images of real people altered by GenAI programs to portray them doing or saying things that they did not do or say.

Let us turn now to a brief history of foreign interference in the United States. Disinformation operations have been recorded since before the Greek's wartime gift of a horse statue to the city-state of Troy. American history is also replete with hostile foreign attempts, real and imagined, to influence domestic events, usually during wars. Often these concerns lead to federal government overreaction. The canonical decision of *ex partite Mulligan* stems from President Lincoln's use of Article 1, Section 9 of the Constitution to arrest and deny *habeas corpus* rights to those engaged in antiwar subversion in support of the rebellious states.[10] In World War I, agitation, strikes, and bombings in support of anarchism and Communism led to widespread law-enforcement suppression activities. This included the infamous Palmer Raids, designed in part to identify, arrest, and deport alleged foreign agents. The Espionage Act of 1917 and the Sedition Act of 1918 (repealed in 1921) were written, passed, and enforced to deal with foreign and domestic antiwar and antidraft activities.[11]

The Espionage Act and the Sedition Act, which expanded the government's authority to limit criticism of the war, were challenged many times for their constitutionality. But *Schenck v. United States* (1919) solidified the Espionage Act's legality. The unanimous decision of the Supreme Court held that the First Amendment's Free Speech Clause did not protect activities that were deemed unlawful under the Act's restrictions, which were further justified under Congress's wartime authority.[12] Prior to its repeal in 1921, the Sedition Act was similarly upheld by the Supreme Court in *Debs v. United States* (1919), *Frohwerk v. United States* (1919), and *Abrams v. United States* (1919).[13]

In World War II, unfounded fear of foreign interference led to the unconstitutional internment of over one hundred thousand American citizens of Japanese ethnicity.[14] While those Japanese Americans posed little or no risk, there was an overt attempt by the German Nazi government to sponsor a Nazi party and movement in the United States beginning in 1933 with the Friends of New Germany organization. Some members of the successor organization, the German American Bund, were prosecuted under the Espionage Act. Others were prosecuted under the Selective Service Act of 1940, which authorized military conscription (some had their convictions overturned in 1945). One Bund leader, a German immigrant, had his U.S. citizenship rescinded.[15]

During the Vietnam War, fears of alleged foreign involvement in the antiwar movement led to unconstitutional surveillance of Americans – as an active teenage participant in the anti–Vietnam War movement, I can assure readers that its vehemence and popularity owed nothing to any foreign hand. In the 1970s and 1980s, there were allegations of a foreign hand in the "Ban the Bomb" and then the "Nuclear Freeze" campaigns led by Americans supportive of international arms control.[16]

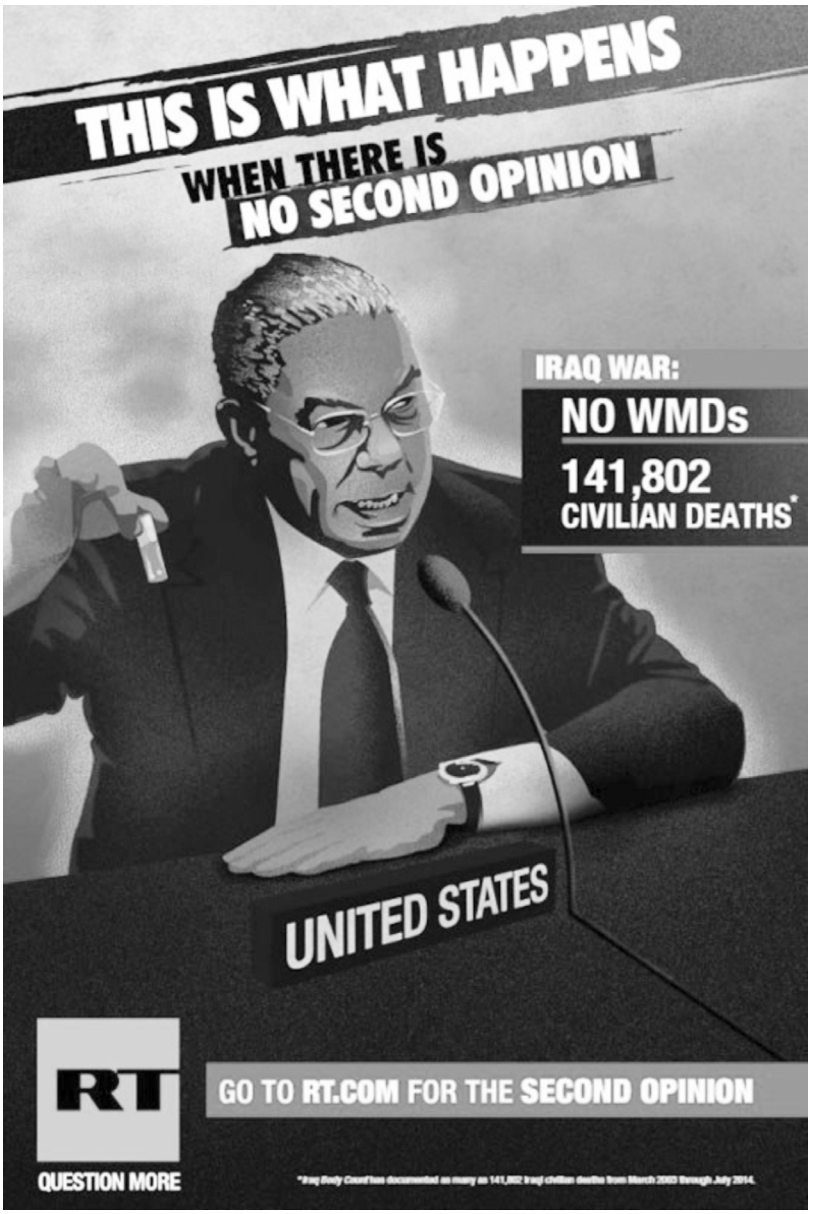
My first encounter with foreign propaganda was as a teenager using a shortwave radio in the 1960s. Listening to Radio Moscow through the atmospheric electronic static left me with the distinct impression that America had nothing to fear from that source of Communist propaganda. The U.S. government implicitly agreed with that conclusion and did nothing to jam the signal. But twenty years later, as deputy secretary of state for intelligence, I was surprised to learn how effective Soviet propaganda had been in Africa. My colleague in the Intelligence Bureau, Kathleen Bailey, was among those who revealed that the Soviets had, among many other disinformation efforts worldwide, convinced much of Africa that the United States had invented HIV/AIDS, at Fort Dietrich in Maryland and at the Wistar Institute on the University of Pennsylvania campus, as a biological weapon to kill Black people.

The 1980s HIV disinformation campaign, apparently known in the KGB as Operation Denver, involved bribing newspaper editors to run erroneous stories, sponsoring conferences, and distributing articles from "scientific journals." One allegation in the campaign was that the United States was distributing condoms in Africa that were laced with HIV. While it all seemed ridiculous to most U.S. government officials, it is an example of a successful use of the big lie technique.[17]

By 2010, the Russian government broadcasted a polished English cable television news channel, Russia Today (later rebranded as simply RT), in the United States and Europe. In 2014, I was startled to see Russian government–funded advertisements emblazoned on the sides of Metro buses in Washington, D.C., complete with an artist's rendering of former Secretary of State Colin Powell holding a vial and discussing alleged Iraqi biological weapons at the UN Security Council. The ad (Figure 1) read, "This is what happens when there is no second opinion. Iraq War: No WMDs, 141,802 civilian deaths. Go to RT.com for the Second Opinion."[18] That propaganda operation was a long way from the scratchy broadcasts from Moscow I had listened to as a kid. It was convincing.

In 2015, Adrian Chen wrote a prescient article for *The New York Times Magazine* in which he exposed an organization in St. Petersburg, Russia, known as the Internet Research Agency, as a propaganda and influence operation. The supposedly private organization had created a number of convincing posts online pretending to be U.S. television news reports, social media responses from average Americans, and local government announcements, all concerning a large explosion at a

Figure 1
Poster from 2014 RT (Russia Today) Ad Campaign on Plurality in Media



Source: John O'Sullivan, "Russia Today Is Putin's Weapon of Mass Deception. Will It Work in Britain?" *Spectator Australia*, December 6, 2014.

chemical plant in Louisiana. There had, however, been no such explosion. It was an experiment in advanced disinformation using sophisticated deception on the internet.[19] Despite Chen's warning, when Russia engaged in a massive disinformation operation a year later, U.S. intelligence and law enforcement did not detect it in real time. Nor did its target, the presidential campaign of Hillary Clinton.

As documented by congressional and Justice Department investigations, Russian intelligence services interfered in the 2016 U.S. presidential election by, among other things, creating thousands of fake accounts on numerous social media apps, pretending to be U.S. citizens, and then spreading both a partisan message and what was indisputably disinformation. But the Russian internet activity went beyond simple messaging. Russian intelligence had a role in the hacking and public release of files from the Democratic National Committee, timed to sow discord at the Democratic Party's convention. Russian intelligence agents on the ground in the United States interviewed Americans to help hone their message.[20]

Russian disinformation focused on swing states and on particular voting groups and neighborhoods within those states. One goal was to suppress Black Americans' votes, which Russia assumed would be overwhelmingly for the Democratic candidate. Fake personas on social media spread lies about the Democratic candidate and urged Black voters to boycott the election. In those targeted locales, ballots from Black Americans declined.[21] Similarly, synthetic internet personalities targeted voters who prioritized climate concerns, urging votes for the Green Party candidate, Jill Stein. Stein was feted in Moscow, sitting at President Putin's table. In several swing states, Hillary Clinton lost by fewer votes than Stein received.[22]

Such is the power of social media that the synthetic Russian personas were able not just to influence the thinking of some American voters, but to cause them to act in real life. One trick messaging effort successfully encouraged partisans to dress up as a Hillary Clinton lookalike in orange prison garb, locked up in a pretend cage that was then put on display at political rallies. On other occasions, the St. Petersburg "Americans" created political counter-demonstrations and rallies in the United States at specific times and places.[23] Russian disinformation, hacking, and fraudulent internet activity were sufficient to make the difference in the outcome of the 2016 U.S. presidential election.

What was the most dangerous path of Russian disinformation? Following the 2016 election, the fake personas continued to spread disinformation in the United States, focusing on the COVID-19 pandemic, circulating "antivax" themes. Russian personas have also supported gun rights, been on both sides of the Black Lives Matter movement, and called for the secession of various states from the Union (a Russian disinformation campaign had similarly supported Brexit covertly prior to the UK referendum).[24]

Following the Russian invasion of Ukraine in 2022, Moscow's disinformation campaign targeted nations in the Global South to support the "special military activity." Among the disinformation they spread were accounts of a joint U.S.-Ukrainian program to develop biological weapons in Kyiv, a big lie that would have little traction in America. More recently, campaigns like Doppelganger are creating deepfake videos and fake media sites to spoof legitimate news and undermine Western support of Ukraine. Although slow to gain traction in the United States, these instances are part of a highly successful influence operation that has led to scores of nations abstaining or voting with Russia on UN resolutions condemning the Russian war.

The objectives of China's influence operations are traditionally defensive, but have recently shifted toward an offensive approach. One of their defensive themes, recalling the 1980s Soviet effort on AIDS, is that the United States invented COVID-19, which their army brought to Wuhan during the World Military Games athletic competition that took place there in 2020.[25] In addition, Chinese disinformation claimed the United States lied about the conditions of the Uighur ethnic group in Xinjiang.[26] China's messaging also uses U.S. activity to justify Beijing's creation of new islands with military bases on them in the South China Sea.

On offense, China mimics Russian efforts, amplifying existing division to encourage mistrust of the U.S. government, and has become more aggressive in attempts to undermine credibility of the United States through disinformation. One long-running disinformation campaign, dubbed Spamouflage or Dragonbridge, has shifted from defensive, pro-CCP (Chinese Communist Party) content to direct disinformation against the United States.[27] This network was first identified in 2019, but the American-oriented accounts were identified in 2022. As part of the campaign, accounts claimed that the Chinese-sponsored hacking group APT41 is backed by the U.S. government. APT41 is known for intellectual property theft, espionage and intelligence-collection operations, and supply-chain compromises.[28] They also claim that the United States bombed the Nord Stream pipelines as part of their goal to replace Russia as Europe's dominant energy supplier.[29]

China's influence operations have evolved from the bots, trolls, and click farms of 2019. Accounts connected to Chinese influence operations use a complex strategy of GenAI, impersonation, profile-hijacking, and coordinated posting. They impersonate real cybersecurity and media accounts to support their narratives using the same name and profile picture and similar usernames as the authentic accounts. These accounts use tactics such as plagiarism, alteration, and mischaracterized news reports, including content that is AI-generated or AI-enhanced.

The strategies are becoming increasingly sophisticated in their narrative production and ability to avoid detection, but there is little evidence of success in attracting the attention of the American public or swaying public opinion.[30] Although those Chinese themes' credibility may be lacking in the United States and in some

other target countries, videos of supposed television news broadcasts being distributed as part of Chinese disinformation are quite convincing. Some of the videos appear to show American reporters and news anchors, but they are deepfakes and synthetic personas produced by AI programs. Microsoft reported an uptick in the use of GenAI to produce audio, video, and other visual content by Dragonbridge. Two instances relate to conspiracies that the U.S. government was behind the wildfires in Maui in August 2023 and the Kentucky train derailments in November 2023.[31]

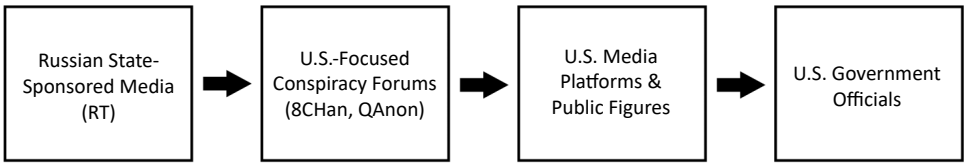
Assuming that the U.S. government was sufficiently concerned by the potential of Russian or Chinese disinformation campaigns in the United States to influence elections or provoke violence, what can it legally do today? What tools does the U.S. government now have to counter SSD?

The State Department's Global Engagement Center, supported by separate programs in the CIA and Department of Defense's (DoD) Special Operations Command, address the problems of Russian and Chinese disinformation abroad. The three agencies uncover the disinformation, attempt to label it in some way as fake news, and engage in counter-messaging to reveal the U.S. version of the truth to the same audience. The State Department also works to generate similar and supportive actions by friendly governments. In the United States, however, it is a different cast of departments and agencies that can use a myriad of existing legal authorities to deal with aspects of foreign disinformation and malign influence operations.

One tool the U.S. government can and should use to counter disinformation is "naming and shaming." As shown in Figure 2, the progress of disinformation, from its introduction through Russian state-sponsored media to wider reach via U.S. government officials, is completely revealable. Members of the U.S. government should regularly call out colleagues who spread Russian or Chinese disinformation, knowingly or unknowingly. The White House should hold weekly briefings from the podium to label Chinese and Russian disinformation in the news and identify which U.S. officials, especially in Congress, are parroting this information. The United States has employed this technique before. In 2017, as the extent of Russian malign activity in the 2016 election became more apparent, the United States moved against RT television, which is funded by the Russian government. Using the Foreign Agent Registration Act (FARA) of 1938, the Justice Department required RT to file as a Russian government entity.[32] Many cable outlets dropped the service and, following the Russian invasion of Ukraine in 2022, the satellite operator DirectTV did as well. RT then shut down its U.S.-based operation and programming.[33] FARA is not a ban; it simply requires the entity in question to admit its foreign sponsorship and file with the Justice Department.

If a non-U.S. citizen was found to be promoting disinformation or malign influence operations while they were present in the country, the Department of

Figure 2
The Life Cycle of Russian Disinformation



Source : Author's illustration.

Homeland Security could deport them on the grounds that their activity violated the terms of their entry visa, which could be revoked under the Immigration and Nationality Act of 1965.[34] If financial activity of any kind takes place in support of a foreign malign influence operation, the use of the sanctions authority is an available tool. By declaring a threat to U.S. national security, the U.S. economy, or U.S. foreign policy, the Treasury Department can ban financial transactions with specific sanctioned entities or individuals the Secretary of the Treasury designates under the International Emergency Powers Act (IEPPA) of 1977.[35] Hundreds of Russian organizations and individuals have been so sanctioned following the invasion of Ukraine. Were any American individual or organization to knowingly receive financial support from a sanctioned entity, they could be charged with a felony, the transaction blocked, and assets seized.

If certain other statutes are violated as part of the foreign malign influence operation, the Justice Department can charge criminal violations. If a computer network was hacked as part of a hybrid war campaign, as was done to the Democratic National Committee's system in 2016, the hacker could be charged under the Computer Fraud and Abuse Act of 1986.[36] Indeed, five named Russians have been so charged. Charges can be brought against an actor who was outside of the United States, provided that the targeted computer was in the United States. Other Russians who engaged in the 2016 campaign to influence the U.S. election have also been criminally charged with attempting to defraud the U.S. government, engaging in wire fraud, bank fraud, and aggravated identity theft.[37]

Certain actions in support of a foreign malign influence operation may violate the Espionage Act of 1917. In 2019, journalist and Wikileaks founder Julian Assange was indicted under that law for receiving and publishing classified information that had been hacked from a U.S. government network.[38] If a malign influence operation is planning, has engaged in, or is conspiring to encourage vio-

lence directed at the government, sedition may also be charged. Although some sedition laws have been repealed and others have been found unconstitutional, there remains the seditious conspiracy violation, which criminalizes behavior involving conspiracy "to overthrow, put down, or to destroy by force the Government of the United States, or to levy war against them, or to oppose by force the authority thereof, or by force to prevent, hinder, or delay the execution of any law of the United States, or by force to seize, take, or possess any property of the United States contrary to the authority thereof."[39]

Although seditious conspiracy was seldom charged in the last fifty years (prior to the January 6 insurrection), it was used in 1993 against an Egyptian, Abdul Rahman, residing in New York City for his involvement in planned terrorist attacks. Following the 1993 arrest of Rahman, Congress passed the Antiterrorism and Effective Death Penalty Act of 1996, which makes it a felony to "provide material support" to organizations and individuals designated by the secretary of state as terrorists.[40] Some U.S. citizens who participated in the January 6 insurrection have been charged with seditious conspiracy and some have been convicted. As of June 12, 2023, the Department of Justice charged sixty individuals with conspiracy to obstruct the certification of the election. Within these charges, eighteen individuals have been charged with seditious conspiracy.[41] And as of this writing, appeals, as well as more prosecutions, are underway.[42]

One expansion of U.S. government authority to deal with SSD could be to criminalize knowingly providing material support (by U.S. citizens or foreign nationals) to operations by foreign hostile powers engaging in disinformation and malign influence operations that caused or threatened to cause (drawing on the example of the International Emergency Economic Powers Act) significant harm to the national security, foreign policy, or economy of the United States. If that were to be considered, however, great care would be needed to prevent abuse or infringement upon First Amendment guarantees. Any such new law should be very specific about what activities would be considered material support to a hostile foreign power and what standards should be used.

How should the United States respond to these challenges? The president already has executive authorities to counter hostile foreign powers engaging in hybrid war activities against the United States. If the president finds that a covert "action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States," and so notifies the designated members of Congress, the president may direct intelligence agencies to carry out appropriate activities without public acknowledgment.[43]

Under such a "finding," intelligence agencies could hack back against a nation involved in hostile operations against the United States, disrupting computer-

related operations, revealing foreign government secrets, or any number of other activities, including lethal action. Thus, the U.S. government could attack those involved in directing hostile operations against it or could launch its own disclosure and influence campaigns (disinformation operations conducted abroad by the U.S. government raise sensitive issues concerning "blowback," the possibility that U.S. citizens or U.S. media operations would see, believe, and disseminate the disinformation in the United States).

The president may also order the Department of Defense to conduct cyber operations to counter hostile foreign influence operations, or other hybrid war activities, under the DoD and White House interpretation of existing legal authorities. As the DoD's General Counsel explained,

> National Security Presidential Memorandum-13 [NSPM-13] of 2018, United States Cyber Operations Policy . . . allows . . . the Secretary of Defense to conduct time-sensitive military operations in cyberspace. Congress also has clarified that the President has authority to direct military operations in cyberspace to counter adversary cyber operations against our national interests . . . whether they amount to the conduct of hostilities or not, and . . . are to be considered traditional military activities.[44]

Using that interpretation, the secretary of defense ordered U.S. Cyber Command to carry out certain activities to protect U.S. elections, including actions directed against the St. Petersburg–based Internet Research Agency.[45] The NSPM and DoD directives and policy reportedly establish First Amendment–related tests and are apparently limited to countering U.S. election-related hostile actions.

But this federal authority in cyberspace need not stop at countering U.S. election-related hostile actions. Led by the White House, the federal government should make a concerted effort to interpret and establish the existing authority it has through the previously mentioned laws and policies. Through cyberspace and social media platforms, hostile foreign actors are no longer limited by location or numbers. The U.S. federal government should coordinate and calibrate its available resources and legal authority to limit these hostilities.

None of the existing legal or direct response authorities, however, prevent social media platforms from being used to spread disinformation that could provoke damaging activity in the United States. To do that, new legislative and regulatory authorities would be required.

How, then, can or should we regulate social media? Social media's impact on modern culture and sentiment is indisputable. This goes hand-in-hand with foreign and/or nefarious actors' attempts to establish influence across these platforms. The current public policy debate revolves around regulating the content on social media platforms (X, Facebook, and YouTube) and regulating the existence of the platforms themselves (TikTok).

TikTok is a wholly owned subsidiary of ByteDance Ltd., a Chinese company registered in the Cayman Islands but headquartered in Beijing. Herein lies the problem. Chinese companies, under new data access laws, can be required to release their data to the Chinese government upon request. With more than one hundred seventy million U.S. TikTok users, the U.S. government has become increasingly concerned with China's possible access to Americans' data.[46]

TikTok U.S., which has a headquarters in Culver City, California, had previously been banned from government devices in multiple states, and ByteDance Ltd. received orders to relinquish its ownership of the company under authority of the Committee on Foreign Investment in the United States.[47] This committee, chaired by the Treasury Department, can mandate a foreign divestment in a U.S. business or block a transaction from occurring, if the result is determined to be a national security risk.[48] This process, which requires a thorough review, could be expanded to further limit foreign influence on social media companies with U.S. users.

Following the Office of the Director of National Intelligence's direct reference to TikTok as a possible threat to national security, Congress passed a measure to outlaw the platform in the United States. The measure passed on April 24, 2024, and gave Byte Dance nine months to sell or initiate a sale of the company, and six months to divest from its U.S. subsidiary. If it fails to comply, the app will no longer be available for U.S. users to download or update. The ban has faced significant backlash from many of its American users and content-creators. Many argue that access to information does not equate evidence of harm, and therefore the ban is not proven to be necessary to protect U.S. citizens. In this case, a ban on the platform will restrict First Amendment rights and internet freedom. Others argue that the threat to national security is substantial enough, and that the ban is necessary to prevent the Chinese government from weaponizing information collected from ByteDance and directing personalized influence operations at Americans.[49]

Social media platforms vary widely in what they will permit to be posted by their users, but what goes up and what is banned is almost entirely up to the companies that own and operate the services. The few legal exceptions to what can be written or said on social media involve child pornography (the posting of which is already a federal crime) or, conceivably, incitement to violence or seditious conspiracy.

Some social media companies employ thousands of staff and spend millions of dollars attempting to identify accounts created by fake personas and posts involved in disinformation campaigns. Other social media companies are less attentive to those considerations, perhaps because controversial content drives usage, and that, in turn, affects advertising rates and income. Or perhaps they do not self-regulate or moderate content out of a deep abiding commitment to the values of free expression. While various research agencies often publish reports that identify influence efforts and fake accounts, they do not have the authority to regulate content or suspend accounts.

Some social media platform executives, notably Meta/Facebook CEO Mark Zuckerberg, have called for regulation, but they have not offered any detailed proposals. Perhaps this is because it is difficult to specify the types of content that should be banned or, alternatively, labeled as disinformation. While Russian disinformation efforts have raised concerns about vaccinations and have opposed gun control legislation, so have American citizens without prompting from Moscow.

In addition to the reaction to a possible TikTok ban, the Utah Social Media Regulation Act and the public's reaction to its passing exemplifies how difficult and controversial it is to regulate social media platforms. This law mandates that social media companies provide parents and guardians of minors and Utah's government with unilateral control over minors' accounts and prevents social media companies from collecting any data or content connected to minors' accounts.[50] This legislation has generated strong criticism from free speech groups on the ground that this erodes civil liberties and safety online.[51] Judicial review seems certain, but even if this was held to be constitutional, it is likely to be easily circumvented by minors.

Identity-management systems and programs to control malign foreign entity creation of fake personas are probably technically feasible. There have been proposals that using such systems means that all social media users be verified as real people, not fake personas. Requiring that by law, however, raises constitutional questions. Moreover, there are numerous situations in which someone might for good reasons want to post information anonymously to avoid reprisals.

The federal government (and some of the larger IT companies) could, however, identify fake personas in use or those attempting to be created. By monitoring known hostile foreign powers' internet activity outside of the United States, the government could look for indications that someone was not who they claimed to be. It could notify social media companies about such possible fake personas. The companies could then temporarily block such accounts from appearing in the United States until their owners proved to the company (not to the government) that they were legitimate users, according to some specified standards or criteria. Some such cooperation is likely ongoing today, but not systematically. A more formal system might not prevent all foreign fake personas, but it might significantly reduce their number.

A law could, conceivably, require internet providers and/or social media companies to abide by a doctrine of "due care" to identify fake personas, to label obvious disinformation, and to give special treatment to postings that would be likely to inflame civil unrest or promote possible violence against protected populations. Flagrant disregard for due care could be prosecuted and fines imposed. The constitutionality of such a law under the First Amendment could be hotly contested, however. Recent attempts by state governments to regulate content-moderation practices in Florida and Texas were deemed unconstitutional in a unanimous decision by the Supreme Court. This decision upheld the First Amend-

ment right of social media companies to remove or publish content at their discretion, without government directive.[52]

In support of such a law, or possibly instead of it, voluntary standards of conduct could be created by a council of social media companies and/or major advertisers, in collaboration with civil society and nongovernmental groups concerned with preventing incitement to violence or hatred against people based upon protected classes like their race, ethnicity, religion, and gender preference. This council could be modeled after the existing Global Internet Forum to Counter Terrorism (GIFCT), which brings together representatives and information from technology experts, government, civil society, and academia to counter terrorist and violent extremist activity online.[53]

If a council modeled after the GIFCT – which was originally founded by Facebook, Microsoft, Twitter, and YouTube in 2017 – created standards of due care, and if some platforms consistently and flagrantly violated those standards, the council could call upon advertisers to place them on a do-not-support list. These standards of due care, with guidance from the previously mentioned council, could be further expanded to encourage social media companies to actively combat disinformation through a system of labeling, rating, and exposure. This practice would encourage a more responsible social media environment, as companies would be encouraged to label content, rate the validity of content, and expose users and sites in which disinformation is regularly posted or referenced while providing references to fact-checked sources.

Establishing a system of collective responsibility through adherence to established standards, whether legal requirements or industry standards, is one potential way to combat disinformation and foreign influence online. Responsible social media sites could effectively (possibly through incorporation of AI) label these accounts and posts as inaccurate, rather than deleting them.

Consideration might also be given to having internet service providers (ISPs, such as Verizon and Comcast) granted safe harbor to block servers, social media, or other websites that are found by such a council to be propagating disinformation that could lead to violence or that foster hate groups. Under the FCC's existing stance on net neutrality, ISPs may already have such authority. Many ISPs block particularly offensive pornography websites. ISPs that fail to block such disinformation could come under pressure from civil society groups and leading advertisers.

So what is to be done? The problem of state-sponsored disinformation is real, significant, and likely to become more damaging with the wider use of AI. The U.S. government has a legitimate interest in minimizing the effectiveness of foreign nations' attempts to amplify our internal divisions and their campaigns to spawn violence.

The government has a panoply of existing legal authorities to counter SSD, from criminal prosecutions of foreign agents at home to covert action and cyber operations abroad. Although the Justice Department must retain the sole authority to determine when and whom to prosecute, a White House coordinator should actively orchestrate the multitude of U.S. government entities that can track, expose, prosecute, and otherwise counter state-sponsored disinformation.

Such a White House coordinator should also work with private sector social media companies, internet service providers, and advertisers to establish voluntary standards for acting against state-sponsored disinformation. Such actions could include naming and shaming U.S. officials who spread disinformation, and labeling, systematically exposing, or possibly blocking malign activity originating with hostile intelligence services and propaganda agencies. All of that should be tried in earnest before any thought is given to further regulating free expression by real people.

ABOUT THE AUTHOR

Richard A. Clarke is the CEO of Good Harbor Security Risk Management, a cybersecurity consultancy, and former Chairman of the Board of Governors of the Middle East Institute. He worked for the State Department during the presidency of Ronald Reagan. In 1992, President George H. W. Bush appointed him to chair the Counterterrorism Security Group and to a seat on the United States National Security Council. In 1998, President Bill Clinton appointed him the National Coordinator for Security, Infrastructure Protection, and Counterterrorism, and the chief counterterrorism adviser on the National Security Council. Under President George W. Bush, Clarke served as Special Advisor to the President on cybersecurity. In 2013, Clarke served on an advisory group for the Obama administration as it sought to reform NSA spying programs following the revelations of documents released by Edward Snowden. Clarke is the author of ten books, including *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (with Robert K. Knake, 2020), *Warnings: Finding Cassandras to Stop Catastrophes* (with R. P. Eddy, 2017), and *Cyber War: The Next Threat to National Security and What to Do About It* (with Robert K. Knake, 2010).

ENDNOTES

[1] Senate Intelligence Select Committee, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Senate Report No. 116-290, Volume 1 (Washington, D.C.: United States Congress, 2020), 5–7.

[2] Ibid., Volume 2, 12–13.

[3] Christopher S. Chivvis, "Understanding Russian 'Hybrid Warfare' and What Can Be Done about It," testimony presented before the House Armed Services Committee on March 22, 2017, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

[4] Xi Jinping, "Forging Ahead to Open a New Chapter of China-Russia Friendship, Cooperation and Common Development," Ministry of Foreign Affairs: People's Republic of China (March 20, 2023), https://www.mfa.gov.cn/eng/zxxx_662805/202303/t20230320_11044359.html.

[5] Darrell M. West, "How to Combat Fake News and Disinformation," Brookings Institution, December 18, 2017, https://www.brookings.edu/articles/how-to-combat-fake-news-and-disinformation.

[6] Jordan Peele, "Obama Deep Fake," Ars Electronica Center, https://ars.electronica.art/center/en/obama-deep-fake (accessed June 7, 2023).

[7] Adolf Hitler, *Mein Kampf, Volume I*, trans. James Vincent Murphy (London: Hurst and Blackett, 1939), https://web.archive.org/web/20080724025441/http://gutenberg.net.au/ebooks02/0200601.txt.

[8] Senate Intelligence Select Committee, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Volume 2, 11–20.

[9] Ibid.

[10] General Order No. 141 (September 25, 1862), https://www.gilderlehrman.org/sites/default/files/content-images/06099p1_0.jpg.

[11] Espionage Act of 1917, Pub. L. 65-24 (1917); and Sedition Act of 1918, Pub. L. 65-150 (1918).

[12] *Schenck v. United States*, 249 U.S. 47 (1919).

[13] *Debs v. United States*, 249 U.S. 211 (1919); *Frohwerk v. United States*, 249 U.S. 204 (1919); and *Abrams v. United States*, 250 U.S. 616 (1919).

[14] "Japanese-American Incarceration During World War II," National Archives, https://www.archives.gov/education/lessons/japanese-relocation (last updated March 22, 2024).

[15] *United States v. Kuhn*, 49 F. Supp. 407 (S.D.N.Y. 1943).

[16] Leslie Maitland, "Sources Are Cited for Charge of Soviet Tie to Arms Freeze," *The New York Times*, November 13, 1982, https://www.nytimes.com/1982/11/13/us/sources-are-cited-for-charge-of-soviet-tie-to-arms-freeze.html.

[17] Christopher M. Andrew and Vasilij N. Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive & the Secret History of The KGB* (New York: Basic Books, 1985), 624–625.

[18] RT News, "RT London Ad Campaign Rejected and Redacted as 'Politically Motivated' (UNCENSORED)," October 9, 2014, https://www.rt.com/uk/194520-rt-ads-redacted-london.

[19] Adrian Chen, "The Agency," *The New York Times Magazine*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[20] Senate Intelligence Select Committee, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Volume 5, v, xii–xiv, 170–259.

[21] Ibid., Volume 2, 6–7.

[22] Ibid., 33–34.

[23] Ibid., 37.

[24] Ibid., 45.

[25] Steven Lee Myers, "China Spins Tale That the U.S. Army Started the Coronavirus Epidemic," *The New York Times*, March 13, 2020, updated July 7, 2021, https://www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html.

[26] Ministry of Foreign Affairs, People's Republic of China, "Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on March 2, 2022," March 2, 2022, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/202203/t20220302_10647299.html.

[27] Donie O'Sullivan, Curt Devine, and Allison Gordon, "China Is Using the World's Largest Known Online Disinformation Operation to Harass Americans, a CNN Review Finds," November 13, 2023, https://www.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html.

[28] Nalani Fraser, Fred Plan, Jacqueline O'Leary, et al., "APT41, A Dual Espionage and Cyber-Crime Operation," Mandiant, August 7, 2019, https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation.

[29] Mandiant Intelligence, "Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections," Mandiant, October 26, 2022, https://cloud.google.com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections.

[30] Fraser, Plan, O'Leary, et al., "APT41, A Dual Espionage and CyberCrime Operation"; and Mandiant Intelligence, "Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections."

[31] Microsoft Threat Intelligence, "Same Targets, New Playbooks: East Asia Threat Actors Employ Unique Methods," Microsoft, April 4, 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/east-asia-threat-actors-employ-unique-methods.

[32] Letter from Heather Hunt, Chief, FARA Registration Unit, to RTTV America, Inc. c/o Brian E. Dickerson, Esq., August 17, 2017, https://www.politico.com/f/?id=00000160-79a9-d762-a374-7dfbebe30001.

[33] Gerry Smith, "RT America Shuts Down After DirecTV, Roku Drop Channel," Bloomberg, March 3, 2022, https://www.bloomberg.com/news/articles/2022-03-03/rt-america-shuts-down-after-directv-roku-drop-channel.

[34] Immigration and Nationality Act of 1965, Pub. L. No. 89-236, 79 Stat. 911, enacted June 30, 1968.

[35] International Emergency Powers Act (IEPPA) of 1977, Pub. L. No. 95-223 (1977).

[36] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474 (1986).

[37] *Indictment in United States v. Ionov, et al.*, Case No. 8:22-cr-259-WFJ-AEP (2023).

[38] *Indictment in United States v. Assange*, Criminal No. 1:18-cr-111 (2020).

[39] 18 U.S.C. § 2384, Seditious Conspiracy (1909).

[40] Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. 104-132 (1996); and "Destruction of, or Interference with, Vessels or Maritime Facilities; Bar to Prosecution," 18 U.S.C. § 2933b.

[41] Mark Denbeaux and Donna Crawley, "The January 6 Insurrectionists: Who They Are and What They Did," Seaton Hall University School of Law, August 7, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4512381.

[42] For example, see *United States v. Rhodes, et al.*, No. 22-cr-15 (2022).

[43] 50 U.S.C. § 3093, Presidential Approval and Reporting of Covert Actions (1947).

[44] Paul C. Ney, Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," U.S. Department of Defense, March 2, 2020, https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference.

[45] W. J. Hennigan, "How the Pentagon Is Working to Protect U.S. Elections from Hacking and Disinformation," *Time* magazine, September 11, 2020, https://time.com/5887998/pentagon-protecting-us-elections.

[46] U.S. Department of Commerce, "Rescission of Identification of Prohibited Transactions with Respect to TikTok and WeChat," 86 FR 32757, June 16, 2021, https://www.federalregister.gov/documents/2021/06/23/2021-13156/rescission-of-identification-of-prohibited-transactions-with-respect-to-tiktok-and-wechat.

[47] "Ban TikTok in Montana," MT S.B. 419 (2023), https://leg.mt.gov/bills/2023/billpdf/SB0419.pdf.

[48] The Defense Production Act of 1950, 50 U.S.C. § 4501 et seq. (1950).

[49] Bobby Allen, "Legal Experts Say a TikTok Ban without Specific Evidence Violates the First Amendment," NPR, May 14, 2024, https://www.npr.org/2024/05/14/1251086753/tiktok-ban-first-amendment-lawsuit-free-speech-project-texas#:~:text=NPR%20reached%20out%20to%20a,on%20TikTokkers%20First%20Amendment%20rights.

[50] Social Media Regulation Amendments, UT S.B. 152 (2023), https://le.utah.gov/~2023/bills/static/SB0152.html.

[51] Jess Weatherbed, "Utah Governor Signs New Law Requiring Parental Consent for Under-18s to Use Social Media," The Verge, March 24, 2023, https://www.theverge.com/2023/3/24/23654719/utah-social-media-bill-law-minors-age-verification-tiktok-instagram.

[52] John Kruzel, "U.S. Supreme Court Sidesteps Dispute on State Laws Regulating Social Media," Reuters, July 1, 2024, https://www.reuters.com/legal/us-supreme-court-set-decide-fate-texas-florida-social-media-laws-2024-07-01.

[53] Global Internet Forum to Counter Terrorism, https://gifct.org (accessed May 31, 2023).