Laura Rosenberger and Lindsay Gorman

How Democracies Can Win the Information Contest

A central distinction between authoritarian and democratic systems is their view of information. Democracies believe in—and depend on—the open and free exchange of information that empowers citizens to make informed decisions to select their representatives and engage in political debate.[1] They champion freedom of expression, association, and press as universal rights. The International Covenant on Civil and Political Rights captures this vision: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his [*sic*] choice."[2]

Authoritarian regimes, by contrast, view information as a threat to state authority if allowed to flow freely and as an instrument of social control if managed and employed deftly.[3] These regimes engage in censorship, surveillance, and propaganda, using the media and other tools to control and manipulate information on behalf of the state.[4] Put simply, in democratic philosophy, information rests with citizens; in the autocratic vision, it rests with those in power.

These opposing visions of public discourse inform different approaches to an emerging twenty-first century struggle between authoritarianism and democracy that is increasingly playing out in the information arena.

Authoritarian regimes like Russia and China see information and cyber warfare as integrated domains of asymmetric conflict distinct from kinetic operations.[5] They weaponize information to fight back against democracies' promotion of

Laura Rosenberger is the director of the Alliance for Securing Democracy and a senior fellow at the German Marshall Fund of the United States, and she previously served in a variety of positions for the State Department and the National Security Council. Laura can be followed on Twitter @rosenbergerlm. Lindsay Gorman is the fellow for emerging technologies at the Alliance for Securing Democracy and can be followed on Twitter @LindsayPGorman.

The Washington Quarterly • 43:2 pp. 75–96
https://doi.org/10.1080/0163660X.2020.1771045

free information as a universal right, which these authoritarian states see as a deliberate threat to regime survival. As Harvard university researchers Eric Rosenbach and Katherine Mansted have observed, authoritarian states offensively deploy information operations externally as tools of foreign policy, while defensively using propaganda and censorship as means of domestic control.[6] In this autocratic approach, social media and online information platforms are weapons to be mastered to weaken democratic systems, alliances, and credibility.[7] These regimes advocate internationally for a "sovereign" information space "where there are no universal norms, just zones of influence."[8]

To the extent that the United States and its democratic peers have recognized the contest unfolding within and over the information environment, they have largely approached it in one of three ways: first, as a traditional question of public diplomacy and strategic communication, where the focus is on narrative content and the objective is to tell their story louder and better, hoping the truth will prevail; second, as an ancillary to kinetic warfare or other military operations, particularly the way technology and information abundance are changing the nature of kinetic warfare (even US thinking on cyberwarfare has traditionally focused on the use of cyberattacks to damage network infrastructure—not on the theft or manipulation of data itself for use as an information weapon); or third, as an economic or security challenge arising from technological competition, without considering implications for the broader information environment. While these three approaches are necessary, each one focuses on a different aspect of the challenge in isolation—public diplomacy, the nexus to kinetic warfare, or technological competition—and none is sufficient.

Instead, an effective strategy recognizes that the information arena has emerged as a domain of sustained and permanent competition that touches on all traditional aspects of national power. In other words, information is both a domain of operations in itself and an arena that affects all other traditional domains of nation-state competition.

The very conception of the information space as a domain of war is problematic for democracies.

Democracies' and autocracies' divergent views on information create asymmetries in the information domain—the very conception of the information space as a domain of war is problematic for democracies. Controlling and manipulating information is inherently more comfortable for and advantageous to authoritarian regimes, while it is inconsistent with democratic values and the function of democratic society. And construing information as a weapon or engaging in information warfare involving non-military targets risks undermining the very space democracies seek to protect. As journalist

and media scholar Peter Pomerantsev puts it, the authoritarian notion of "information warfare" is part of a world view and interpretation of history "where all values, ideals, ideas are mere fronts to subvert the other side, where there is no qualitative difference between independent journalism and a covert social media psy op."[9]

The very notion of engaging in "information warfare" risks playing on a battlefield defined by democracies' authoritarian competitors and acceding to the closed, controlled, and manipulated view of information that authoritarians champion. But while democracies should not define this contest as "warfare," they need to recognize that their authoritarian adversaries do—and that such regimes believe democracies to be information aggressors, wielding information to undermine authoritarians' power and closed systems.[10]

Instead, democracies should understand the challenge as a global information contest that encompasses the use or manipulation of information (data and content) itself; the architecture, or the systems, platforms, or companies that transmit it; and the governance frameworks, including the laws, standards, and norms for content, data, and technology. This contest is a key avenue for advancing one system of values over another, and it both reflects and affects the broader geopolitical competition between authoritarians and democracies. Therefore, democracies must engage in a manner that affirms, rather than degrades, the information arena. The focus of this paper is on the first dimension of this contest—the manipulation of information itself, primarily via digital means—but we place this analysis in the broader strategic context of the information contest. At present, democracies are not meaningfully preparing for this struggle.

This paper addresses how democracies can compete in this larger strategic contest without engaging in activities that advance the information model of state censorship and weaponization that authoritarian regimes want. It outlines the reasons why democracies need to engage in the information contest, the values and principles that should guide a democratic approach, the steps they should take to compete, and the ways in which democracies should structure themselves to effectively engage in this contest.

Why Democracies Need to Engage in the Information Contest

While the information space as a contested domain poses challenges for democracies, they have little choice but to engage. Democracies cannot afford to sit out the information contest for two chief reasons.

First, authoritarians are already contesting this domain and exploiting democracies' inaction. Whether or not democracies care for information warfare, information warfare is being waged against democracies. Democratic societies, where

information flows openly, are particularly vulnerable to information manipulation, and authoritarian actors exploit this openness to weaken them. These regimes are filling the information space in areas of the globe where democracies' voices are absent. Contesting this space in a way that puts democratic values and principles about information at the center is essential to preserving the democratic institutions that protect those values.

Second, the use and manipulation of information to achieve national objectives is an increasing locus of great power competition. Although additional actors will adopt information manipulation tactics in this asymmetric and low-cost battlespace, the primary information challenges to liberal democracies will continue to come from Russia and China due to their scope and sophistication. Operations short of armed conflict—many of which find fertile ground in the information domain—are becoming a mainstay of twenty-first century geopolitical competition.[11] A national security paradigm that ignores information as a contested domain risks forfeiting some of the largest conflicts of the twenty-first century.

The use and manipulation of information is an increasing locus of great power competition.

While democracies need to contest the information space because of external threats from authoritarian competitors, they also need to combat the degradation of their own information environments from within. Here, democracies face significant internal challenges. The emergence of what scholar Shoshana Zuboff calls "surveillance capitalism" as a business model incentivizes the surveillance of citizen data for profit and erodes privacy.[12] The rise of information platforms with hidden inner workings for how content is prioritized and shown to users, like YouTube and Facebook's NewsFeed, provides a ripe target for algorithmic manipulation to advance divisive narratives and conceal external manipulation. And as some platforms have grown increasingly large, they have written the rules that govern wide swaths of the information space while remaining accountable only to their shareholders. The failure of legal and regulatory regimes to keep pace with technology and ensure protections for a free and open information arena has perversely created room for authoritarian information models to expand and decreased the global attractiveness of open systems.

Beyond the digital realm, the traditional media sector in many countries across the freedom and democracy spectrum has increasingly fractured, and the collapse of local and independent print media has created vacuums of quality information and undermined democratic accountability.[13] Meanwhile, even private companies and media outlets in democracies are vulnerable to coercion by the Chinese Communist Party, which uses access to the valuable Chinese consumer market to

compel favorable coverage and to suppress employee speech or corporate information on websites or products that counter the regime's strict censorship rules.[14] Successfully competing in the information domain will require democracies to get their own houses in order.

Democratic Principles for Engaging in the Information Arena

How democracies approach this contest is therefore central to their success. Contesting the information arena should not mean jumping onto a playing field defined by democracies' adversaries. Rather, liberal democratic states must define their own terms of engagement that are consistent with the values they seek to protect. They must move from a reactive, tactical approach toward a proactive, sustainable, and strategic one. And they must recognize that their own shortcomings in protecting a healthy, open information environment have created space for competing authoritarian models. Ultimately, democracies' goal should be to promote a healthy, open, and transparent information arena as an element of the global commons. Such a conception stands in contrast to the authoritarian norm of cyber sovereignty, in which individual states set, control, and restrict their own information environments. The following principles should guide this democratic approach.

Affirming the value of information

Recognize that while information can be and is being weaponized, information in and of itself is not a weapon. States that believe in universal values of human rights, freedom of information, and independent facts should avoid this reductive capitulation. Instead, democracies need to pursue strategies that affirm, rather than degrade, the value of information and its centrality to deliberative democracy. Quality of information is more valuable than quantity. Wikipedia is a prime example of a forum that—while not perfect—affirms the value of information and prioritizes quality through a fair and open consensus-seeking process with trusted contributors and transparent mechanisms for adjudicating conflicts.[15]

Openness

Retain the open information systems that set democracies apart. That means setting an example by resisting the temptation to censor content. It also means fighting for universal—not sovereign—internet governance models and protecting open innovation and competition. Democracies will face hard choices in addressing threats from external actors, some of which may require imposing higher standards on the companies that participate in critical information

sectors around infrastructure and personal data. But their bias should be toward remaining as open as possible.

Transparency

Establish transparency and accountability from both governments and technology. This principle applies to the handling of content such as political ads and the removal of illegal content by online information platforms. But it also applies to the structures that underpin and organize information, including the algorithms that select and deliver news, videos, and search queries. Transparency is an area where many democracies have fallen short and where redoubling focus will be essential to strengthening their hand.

Empowering information consumers

Put users in control of their data and of how information is shown to them, allowing them to understand where their data is going and how it is shaping the content they are shown. Increasingly, algorithms invisibly shape our realities and guide our decisions. In the laissez-faire model, these algorithms are profit-driven. In the authoritarian model, they are control-driven. Neither is good for democracy. In Peter Pomerantsev's vision, users should be "empowered to have a stake in the decision-making process through which the information all around us becomes shaped, with public input into the Internet companies who currently lord over how we perceive the world in darkness."[16]

Truthfulness

Employ factually verifiable information in democratic actors' *own* messaging, rather than simply blocking content from others. Importantly, while this normative principle should guide democratic actors' use of information, requirements of truth should not be legislated, imposed by democratic governments, or used as criteria for private actors moderating online content. For truthful ideas to succeed in an information-saturated world, they should look qualitatively different from falsehoods—by including trails for independent verification, even in today's information morass. A corporate statement or State department communique, for example, that included sourcing when making claims would build trust and credibility. The further politicians and public figures in democracies stretch the bounds of truthfulness, the more democratic societies lose the ability to distinguish fact from fiction. A world in which there is no objective truth is one in which democracies cannot succeed.

Civil liberties

Protect and respect civil liberties—core pillars of democratic societies—in the information commons. This principle includes protecting privacy from both

state and corporate actors; preserving space for activist communities; safeguarding free expression and the freedoms of belief, religion, and association that are increasingly under authoritarian attack; and upholding due process in an era of surveillance—both online and off.

Multilateralism

Stand together. The information contest is best understood as a competition between systems and values, not just of nations. Authoritarian information and influence efforts seize on divisions within and between democracies, while also targeting countries that feel unaligned. Eroding the international consensus around universal values is the autocratic mission. A multilateral approach with all of the aforementioned principles at its center is the best defense against the authoritarian strategy of divide-and-conquer.

> The information contest is a competition between systems and values, not just nations.

What Democracies Should Do to Engage in the Information Contest

In the face of information manipulation from authoritarian actors, democracies should focus on two lines of effort for their engagement in the information arena: (1) building information resilience in society and (2) seizing the information initiative in accordance with the principles outlined above.

Building Information Resilience: Fortifying the Democratic Model

Authoritarian efforts to manipulate the information environment inside democracies leverage inherent asymmetries. But responding requires democracies to build resilience in their own information model while ensuring they do not create the hardened and closed information space authoritarian regimes promote. To do so, democracies must do the following:

> Responding requires democracies to build resilience in their own information model.

Focus on behavior, not content, to protect the democratic information commons

A reactive tendency to police content risks solidifying authoritarian norms of information control. For example, under the banner of countering "fake news," nations from Bangladesh to Brazil to Cambodia to France have put forth laws

empowering governments to control information and in some cases punish the authors of what the government considers "fake news."

Instead, to strengthen and affirm the value of information, the focus of defensive efforts needs to be on perpetrators and their modes as well as means of manipulation—not on suppressing content, which is itself a tactic of manipulation.[17] Authoritarian information manipulation tactics include building online information platforms to censor speech, as with indigenous Chinese platforms TikTok and WeChat; pressuring private sector actors such as the NBA to present information according to specific narratives; or coordinating activity of inauthentic social media accounts to amplify information, as in the Russian magnification of divisive narratives during, before, and after the 2016 US presidential election.

Focusing on countering the underlying behavior of actors engaged in malicious activity takes a more systemic approach to countering information manipulation than focusing on content, while upholding democracies' commitments to openness and freedom of expression.[18] Whereas an authoritarian approach would censor speech by subject matter and, in some cases, imprison those responsible, democratic actors should look to expose and remove coordinated deception on the part of state and non-state actors.[19]

Require transparency from online information platforms

Engagement-driven metrics guiding the algorithms that organize, prioritize, and display information—and the opacity surrounding them—allow malign actors to degrade the information space by manipulating search results and promoting divisive content.[20] Popular social media platforms that adhere to authoritarian censorship rules by removing or demoting certain content can also subtly shape public perception, even in democracies. Reports of video-sharing app TikTok censoring content related to Hong Kong pro-democracy protests is a case in point.[21] Without transparency requirements for the way information is displayed on information platforms, this manipulation is difficult to detect and assess.

To build resilience against information manipulation, democracies should construct algorithmic transparency regimes to shine light on how information is prioritized online. While specific algorithms and computer code itself is proprietary information, companies could provide information on *how* algorithms operate without disclosing trade secrets or opening up their code entirely. One idea is to implement algorithmic audits, borrowing an analogy from the financial services industry. These audits might include tests on algorithms to assess the characteristics they prioritize and their freedom from censorship. Increased transparency would empower users to make informed choices about the platforms on which they conduct social, professional, and increasingly political communications. They would also give regulators and researchers a window into how the democratic

information space is degrading and who is responsible. To protect open discourse, democracies need to ask more of all information intermediaries.

Require data protection and privacy from the private sector and empower users around their data

In the information arena, authoritarian governments have seized on the collection of personal information on citizens as a means for manipulation and control.[22] But democracies have struggled to protect citizen data from both authoritarian governments and corporations. Information manipulators collect personal data for a suite of uses: to more precisely target manipulation, to provide *kompromat*, to identify intelligence and counterintelligence targets, and to train artificial intelligence surveillance systems.[23] Tech companies amass personal information and sometimes leave it unsecured, gift wrapping that data for malign actors. Here, a failure to empower users through robust and multilateral data protections renders democracies vulnerable to information manipulation and the dissolution of privacy as a universal right.

But democracies face tensions between the desire to protect citizen data from authoritarian governments and a commitment to a universal open information environment. China's strict data localization laws, for example, require all personal data collected in China to stay in China. These laws may enable regimes to hoard data within borders but also advance a sovereign internet at odds with universal rights and open access. Democracies need to balance the protection of citizen data from authoritarian capture with an open internet. One approach to this challenge may be to designate classes of sensitive personal data, such as biometric or health information, for which tighter controls are appropriate.

Some jurisdictions, including the European Union, Australia, and Brazil, have passed comprehensive data protection legislation that returns agency to users by allowing them to opt-out of online tracking and reclaim their personal data from companies that hold it. Many also require companies to rapidly disclose data breaches of their systems to a regulator in order to aid response. At present, these laws face steep implementation challenges in setting up and empowering regulators.[24] In the United States, a lack of political will at the federal level is paving the way for a convoluted patchwork of privacy legislation at the state level.[25] A consumer- and competition-focused approach can empower users to take control of their data, and a vantage point that seeks to protect national security should also address how authoritarian regimes exploit it by requiring actors that handle sensitive personal information, such as DNA, to be explicit about with whom that data could be shared.

Build "information intelligence" across the public and private sectors

Resilience against authoritarian information manipulation can only be as good as knowledge of it. But capabilities and prioritization here lag, and in a largely

civilian domain on a private battlefield, there are inherent challenges for tracking these efforts in a manner consistent with democratic values.

Specifically, democracies must balance an interest in monitoring for signs of information manipulation with the inherent collateral collection of information on their own citizens—even if that information is publicly available. A system that read, collated, and processed content from every Facebook account, for example, might be effective at detecting information manipulation on the platform, but in the hands of a government would pose serious problems for the privacy and civil liberties of its citizens.

Online, this response should include careful information sharing among companies and government actors on inauthentic behavior patterns and coordinated takedowns of this activity. Coordination across platforms has improved in recent years—such as when Twitter and Facebook together took down Chinese-linked disinformation about pro-democracy protests in Hong Kong[26] and disinformation from an Iranian network about the coronavirus in April 2020.[27] But this balance should become muscle memory through a formalized approach. A principled response should also prioritize and support civil society and independent research efforts to study the information environment, particularly in the domestic sphere where democratic governments should not be conducting surveillance.

"Information intelligence" requires coordination among the public sector, the private sector, and civil society.

In practice, building "information intelligence" requires coordination among the public sector, which can assess motives and nation-state strategy; the private sector, which houses information playing fields; and civil society, with independent research capacity. As the information contest crosses borders, multilateral coordination on threat intelligence will be needed.

But constructing this picture is not solely about social media monitoring. Democracies need to understand how their adversaries shape the broader information environment, beyond platforms. This holistic view stretches across society and includes the full complement of authoritarian information efforts: targeted media and diplomatic narratives, coercion of public and private sector actors, the manipulation of personal data for influence or control, the deployment of surveillance technologies, and international engagement to advance sovereign internet norms.

Intelligence agencies will need to reprioritize open source information—where appropriate and consistent with their authorities limiting domestic collection—to recognize these broader tactics and integrate them into their understanding of adversary objectives. They will also need to inform broader

segments of governments and societies on their findings. Six months in advance of Canada's fall 2019 elections, for example, its intelligence community's Communications Security Establishment released a public report on cyber threats to the nation's democratic processes, including the manipulation of information to influence voter opinions in the context of global trends. The report found that political parties, candidates, and staff; Canada's elections infrastructure; and Canadian voters themselves were all targets of malicious cyber activity and that the Canadian public was likely to see voter influence attempts through the manipulation of information online in the lead-up to the election.[28] For a whole-of-society picture, governments, too, need to be transparent about the threats they face.

Seizing the Information Initiative: Advancing the Democratic Space

Democracies should embrace an external focus that communicates the attractive power of the democratic information model to democracies, autocratic populations, and in-between states while recognizing the internal work necessary to build a model that can compete with what authoritarians are selling. Ultimately, democracies should harness open and truthful information to proactively contest the information space and promote and defend a global information commons.

Democracies should harness open and truthful information to promote a global information commons.

To guide their efforts, democracies should apply the framework of persistent engagement, which US Cyber Command has adopted to describe its continuous and proactive engagement to maintain initiative in cyberspace, to the information arena—not as a military doctrine, but as a civilian-led interagency effort.[29] This framework would recognize that the information contest is ongoing, falls outside of traditional boundaries of conflict, and must contend with adversaries' actions that are unlikely to be deterred. It also recognizes that in the information arena, democratic engagement must be ongoing due to a distinct first-mover advantage: setting the narrative is far easier than changing it, and information vacuums are readily filled.[30] In the technical digital realm, unique, new, or uncommon search terms associated with breaking news or obscure queries create "data voids" where little authoritative content exists and manipulators can flood the zone with their content.[31]

In the geopolitical realm, unfolding events absent quality information and analysis create space for authoritarians to shape the narrative. To seize the information initiative and advance and harness the affirmative value of information, democracies should take the following actions:

Align policy with credible and truthful messaging

Since the end of the Cold War, democracies have neglected the importance of the information component of their actions, relying instead on the openness of the media to tell their stories. In the information age, effective policy needs an effective message. Too often, an absence of coordinated messaging alongside policy creates a vacuum that democracies' competitors fill. In 2014, Russia paired its invasion of Crimea with a significant information campaign advancing the narrative that Crimea was actually part of Russia, not Ukraine.[32] Democracies failed, in this case, to provide an equally rapid and sophisticated response in the information domain.

In the United States, most Deputies Committee meetings traditionally have "public diplomacy" or "strategic communications" as the last item on the agenda, usually resulting in a tasking for the State Department to circulate talking points, which a desk officer dutifully drafts and virtually no one uses. But an integrated information component of policy is not just pro forma talking points developed after policy decisions that no one uses. Rather, it involves advancing transparent and truthful information to prevent others from filling information vacuums and ensuring that the information dimension of every government action is prioritized, not viewed as an afterthought. An integrated information component in policymaking includes analyzing the information effect of policy options as part of decisions, prioritizing an information strategy in policy implementation, identifying the best channels for disseminating and propagating information, and understanding likely adversary counter-messaging. In short, integration of an affirmative information component into all government actions will be critical for contesting the information space and for ensuring the success of policies across all domains. This holistic integration also includes understanding that government is not necessarily always the right messenger and that marshalling trusted outside voices is often the best approach.

New York Governor Cuomo's communication strategy during the COVID-19 pandemic is a model of integrating an information component as a vital element of the policy response. In daily briefings, he has provided open, transparent, and truthful updates on the unfolding crisis and has built a cross-platform public service campaign: "Stay at Home, Save Lives."[33] PSAs featuring the hashtag #NewYorkStateStrongerTogether enlisted celebrities from Danny Devito and Robert de Niro to Ben Stiller and Alec Baldwin for the policy message. Cuomo himself participated in the #IStayHomeFor campaign, featuring Jennifer Lopez, Alex Rodriguez, Kevin Bacon, and Nick Carter.[34] Because the success of the policy intervention requires public buy-in, an effective policy strategy is impossible without this information component.

US allies have also provided helpful models for integrating information strategy into policy action. In response to the March 2018 poisoning of Sergei and Yuliya

Skripal by Russian intelligence officers, for example, the UK both expelled Russian diplomats and, in September of that year (after a period of being caught off-guard), swiftly countered the massive Russian disinformation campaign that emerged. Partnering with other countries that had experienced Russian subterfuge, namely the Netherlands and the United States, the UK government released a detailed list of crimes committed by Russian agents. In the weeks that followed, just one of the top 25 most viral subjects on the story was from a pro-Russian outlet.[35] This counterattack was also greatly aided by the UK's earlier decision to release details about the attackers. The action enabled non-governmental organizations including Bellingcat and *The Insider* to successfully use open source research to identify the assailants' true identities as agents of Russian military intelligence hiding behind assumed identities.[36]

In addition to governments, private sector actors also need to develop strategies around information. As the NBA and other companies operating in China have learned, the Chinese party-state does not hesitate to coerce private companies—even those based in democracies—when it disapproves of the messages they or their employees deploy. In October 2019, the NBA faced a strong backlash by the Chinese party-state after Houston Rockets' General Manager Daryl Morey tweeted his support for Hong Kong pro-democracy demonstrators, including Chinese basketball associations suspending broadcasting and merchandizing deals with the Houston Rockets.[37] Too often, companies have responded defensively or with an instinct to stifle speech. This approach will lead to scenarios in which China dictates companies' messaging. Private sector entities need to develop affirmative approaches to messaging that ensure they—and not authoritarian regimes—set the terms, maintain the initiative, and protect the free flow of information.

Harness and assert the positive value of open information

Finally, democracies should harness open and truthful information to contest the information space proactively. In practice, this harnessing involves joining with likeminded nations to point out failures of authoritarian regimes, spotlight censorship, and condemn repressive acts in the information environment loudly, clearly, truthfully, and multilaterally instead of tacitly accepting them. After the Chinese media backlash to Daryl Morey's tweet, for example, Morey issued a partial apology, and the NBA initially issued a statement calling his comments regrettable.[38] In 2018, the Chinese government similarly coerced Marriott Hotels into denouncing an employee who liked a Facebook post supporting Tibetan independence. This kowtowing behavior on the part of private corporate actors is at odds with the preservation of free expression in a global information commons.[39]

Harnessing and asserting the positive value of open information also means upholding freedom of information worldwide. Here, democracies can look to their militaries for inspiration: the US Navy conducts "freedom of navigation

operations," patrolling open waters to protect open passage through internationally recognized waterways and challenge excessive maritime territorial claims. In the information domain, analogous "freedom of information operations" could protect an open information commons.

Analogous "freedom of information operations" could protect an open information commons worldwide.

On third-country playing fields, these operations could be deploying truthful messaging to spaces that authoritarians are attempting to fill and using information to pierce the narrative they seek to construct about themselves, such as in the case of the CCP's "discourse power" strategy that seeks to elevate CCP narratives and neutralize criticism abroad through engagement, agenda-setting, and propaganda.[40] Funding independent journalism and publishing these outlets' standards of independence to showcase the distinction from authoritarian-funded and controlled media such as China's *Global Times* or Russia's *RT* could also be part of this picture.

In autocracies, "freedom of information operations" could be technological efforts to mute the effectiveness of authoritarian information control mechanisms like China's Great Firewall that blocks access to foreign websites deemed problematic or Russia's System of Operational-Investigatory Measures (SORM) that mandates a government eavesdropping capability. These include providing virtual private networks (VPNs) for activists such as in China or Iran. To be sure, these efforts will threaten authoritarian regimes and feed their view of democracies as information aggressors; however, they hold and propagate this view regardless of democracies' actions.

In choosing when and where to apply this policy, democracies should not ignore the potential for authoritarian backlash—including with narratives that paint democracies as aggressors that weaponize information to advance their interests and engage in the same behavior authoritarians do. Ultimately, when calculating foreign policy actions and interests, democracies will need to weigh the downsides of this backlash with the potential gains from stemming the flow of information control technology and tactics. And to blunt the effectiveness of this authoritarian messaging, these "freedom of information operations" need to be truthful and transparent, refrain from manipulation, be conducted by democratic governments or civil society organizations, and include their own coordinated messaging component when appropriate. In short, they should serve as a clear contrast to the ways authoritarian regimes engage in information manipulation. While engaging in the same types of operations as authoritarian states is a losing proposition for democracies, a blanket unwillingness to challenge authoritarian information control implicitly condones it and allows for its spread.

Design and promote information architecture and governance consistent with democratic values

Finally, democracies should recognize that competing on message alone is not sufficient. The arenas in which the modern information contest plays out increasingly involve the architecture of the information space itself and the norms governing it. In addition to the online information platforms addressed here, these architecture and governance dimensions include the physical network infrastructure that carries information, the international technical standards organizations that make decisions on global information technology requirements, the public and private surveillance systems that connect homes and cities, and the multilateral bodies and frameworks that govern the rules of these devices and the broader internet. In recent years, democracies have been largely absent from normative input into all of them. By contrast, China in particular has recognized the importance of this architecture layer in the broader information contest and is harnessing its state-driven private sector to set global technology standards.

Democracies need to provide an attractive counteroffer to the authoritarian model, both for themselves and for less-consolidated democracies. This counteroffer could be provided through methods such as arguing for robust lawful access and data protection provisions in information systems, enacting strong data privacy legislation, competing in standards-setting organizations to build out the internet architecture of the future, and developing and championing ethical frameworks on AI bias, transparency, and accountability. Building positive, multilateral frameworks for the ethical application of information-driven technologies would put needed rhetorical distance between how democracies and authoritarian regimes use them while steering their use in a direction that protects democratic values, affirms the positive role of information in society, and rejects authoritarian misuse.

Who Should Lead Democracies' Efforts to Contest the Information Space?

Once democracies have determined how to approach the information contest, they need to determine who is leading the fight. The information contest spans governments' domestic and foreign policy institutions. Most democratic governments have no single actor with responsibility for either analyzing the information space holistically or coordinating democracies' defense or engagement in it. As Stanford researcher Herb Lin has detailed, fourteen US government agencies touch some aspect of the information contest.[41] Yet democracies are not well resourced or structured to confront the challenge.

Democracies are not currently well resourced or structured to confront the challenge.

To successfully contest the information space, someone needs to be in charge. But this is not an area where government is the primary actor, since much of the contest takes place on private playing fields. And authoritarian regimes can leverage their private sectors in ways democracies cannot and should not. Contesting the information domain will require innovation and nimbleness in approach, analysis of which roles are appropriate for government, and leadership from and coordination with the private sector and civil society. Democracies need new structures, modes of operation, and means of collaboration. Several characteristics should guide how democracies organize themselves to engage in this contest.

First, a democratic approach to the information contest must be civilian-led. Information warfare activities from Russia, China, Iran, and other authoritarian states often include significant military and intelligence components, and there is temptation to mirror this approach in response. But the targets of information manipulation are largely civilian, and the battle surface non-military. If protecting and advancing an information environment defined by democratic values is the goal, a military-led approach that weaponizes information undermines this objective. Democratic governments, therefore, should identify a civilian entity responsible for coordinating their engagement in the information space, in line with the principles articulated above. Crucially, this entity should not be authorized to remove content and must recognize the limitations of governments as direct messengers while empowering outside voices that promote quality information.

Two examples from Europe present building blocks for democracies in forming and directing such an approach. The French government responded to a 2017 disinformation attack by creating a taskforce representing Foreign and Defense Ministries as well as academic and civil society groups. It shared lessons learned publicly, including that reporting on hacks *before* the disclosure of stolen documents helped inoculate voters.[42] In Sweden, the government has distributed leaflets on disinformation and trained thousands of civil service employees, political parties, and journalists to identify foreign influence campaigns. It also constructed a dedicated line of communication with Facebook, Twitter, and Google to allow government officials to report fake pages and accounts.[43] While not exhaustive, these efforts notably recognize the societal element of the information contest and crucially its non-military dimensions.

Second, a civilian-led approach needs to put coordination with online information platforms at the center of its mission. This coordination will require government to be more transparent in sharing information with private companies and provide assessments of the strategic information environment and particular threat actors. The European Union's Code of Practice on Disinformation represents a first step in building a common public-private understanding on threats and remediation measures, even if its self-regulatory approach falls short.[44] In the United States, a provision to establish a social media data analysis

center that would facilitate such sharing was included in the 2020 National Defense Authorization Act, though it has yet to be implemented.[45] Ensuring appropriate protections for privacy and speech in this process will be critical to upholding civil liberties.

Third, a civilian-led approach needs to be supported by robust and holistic assessments of the information environment. This support will require coordination among the intelligence community, private sector, and civil society. For example, since 2016, the Estonian Foreign Intelligence Service has released an annual report to the public assessing the threat of Russian aggression and influence in Europe.[46] The reporting is part of an ongoing effort to enhance public communication and government accountability necessary to build resilience across society.

Fourth, the military does have a limited part to play. Militaries should build information environment awareness around traditional battlespaces and recognize that, in a permanent information contest, military operations themselves have a signaling effect that requires prioritizing the information component of an operation. For example, the lack of a coordinated information strategy around the US strike on IRGC Commander Qassem Solemani—including a delay in acknowledging the US role and mixed messages on the rationale—undercut any signaling effect to both adversaries and allies that the United States may have intended and created a vacuum for US adversaries to fill.

Militaries should also continue to engage in limited offensive cyber operations, including on the infrastructure supporting adversaries' information operations and the forward defense of democratic information networks from compromise. For example, in advance of the 2018 US midterm elections, US CYBERCOM reportedly pre-emptively and temporarily disrupted the internet access of Russia's Internet Research Agency out of concern for influence attempts.[47]

Fifth, legislatures need to be structured to take an integrated approach to the information contest. In most legislatures today, issues surrounding digital information platforms and information manipulation cross numerous committee jurisdictions, leaving no one with ownership of either the legislative development or oversight processes. In the United States, budgetary process failures compound jurisdictional issues. Because defense funding is often the sole authorizing bill passed, the military has become a de facto leader for all national security challenges.[48] This structure has to change to support a civilian-led approach. In December 2019, the Australian parliament broke down some of these silos when it established the Select Committee on Foreign Interference through Social Media. Since 1983, Australia has held a Joint Standing Committee on Electoral Matters, but the Select Committee is the first to focus exclusively on online foreign interference and misinformation and how Australia can counter it.[49]

Sixth, civil society should analyze and monitor the information domain, especially domestically, where democratic governments face limitations on

surveilling their own populations. Due to their independent credibility, civil society actors will often be the best sources for public-facing analysis of the information environment. The public and private sectors thus need robust means for cooperating with civil society while maintaining its independence. In the Baltic states, for example, groups of volunteer internet users known as "elves" work to debunk pro-Kremlin disinformation narratives by pushing out information from reliable sources.[50] A strong civil society is also important to holding governments and the private sector accountable to the principles outlined above.

The ability to bring to bear disparate, vibrant sectors of democratic society is vital to democracies' success in the information contest and to their global offering.

Reframing the Information Contest

Differing views between democracies and autocracies on the role of information in society create an asymmetric information domain. The current contest for this information space—often framed as "information warfare"—plays to authoritarians' strengths. The paradox for liberal democracies in this environment is that in quashing adversarial information efforts outright, they diminish the values of openness and inclusion for which they stand. And they risk creating the information environment that authoritarian regimes advance.

To succeed in the information arena, democracies need to reframe the contest to capitalize on their own advantages and exploit authoritarian weaknesses. This reframing requires aligning the goal of advancing the democratic worldview of information with the tactics of the information contest itself. It is this key element that is missing from democracies' current approach to the information environment that gives authoritarians the upper hand—right now, the authoritarian worldview and "information warfare" tactics are aligned.

Democracies need to compete on their own terms—not only to build a more resilient society against authoritarian information manipulation, but to seize the initiative in this contest: to openly, transparently, truthfully, and multilaterally empower information consumers and protect civil liberties to advance a global information commons that affirms and strengthens information's value in society. *How* this contest is fought is vital to who wins.

Notes

1. Michael Berkman, "Episodes," Democracy Works (podcast), McCourtney Institute for Democracy, accessed on January 29, 2020, https://www.democracyworkspodcast.com/episodes/.

2. International Covenant on Civil and Political Rights, General Assembly of the United Nations, December 19, 1966, https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf.
3. Eric Rosenbach and Katherine Mansted, "Can Democracy Survive in the Information Age?" Belfer Center for Science and International Affairs, October 2018, https://www.belfercenter.org/publication/can-democracy-survive-information-age.
4. Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models* (Washington, DC: Brookings, August 2019), https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.
5. David Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (New York: Penguin Random House, 2019).
6. Rosenbach and Mansted, "Can Democracy Survive in the Information Age?"
7. Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," *Asan Forum*, May 8, 2018, http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response/#1.
8. Peter Pomerantsev, "We Need to Stop Thinking of Conflict with Russia as an 'Information War'," *Time*, November 9, 2019, https://time.com/5722805/rethink-information-war-russia/.
9. Pomerantsev, "We Need to Stop Thinking."
10. Tom Uren, "Are We Preparing for the Right Kind of Conflict?" *Australian Strategic Policy Institute*, August 20, 2019, https://www.aspistrategist.org.au/are-we-preparing-for-the-right-kind-of-conflict/.
11. Kathleen H. Hicks and Melissa Dalton, *By Other Means Part II: Adapting to Compete in the Gray Zone* (Washington, DC: CSIS, August 2019), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_II_interior_v8_PAGES.pdf?R2GwIpHMlYuHkyBKPA63N40oZJhDS3w8.
12. Shoshanna Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).
13. Sarah Rapucci, *Freedom and the Media 2019: A Downward Spiral* (Washington, DC: Freedom House, June 2019), https://freedomhouse.org/report/freedom-media/freedom-media-2019; Penelope Muse Abernathy, "The Expanding News Desert," UNC Hussman School of Journalism and Media, accessed January 29, 2020, https://www.usnewsdeserts.com/.
14. Mike Spector and Wayne Ma, "If You Want to Do Business in China, Mind Your T's: Taiwan and Tibet," *Wall Street Journal*, June 3, 2018, https://www.wsj.com/articles/if-you-want-to-do-business-in-china-mind-your-ts-taiwan-and-tibet-1527937201; Ben Strauss, "ESPN's Politics Policy—and Its Journalism—Tested by NBA-China Controversy," *Washington Post*, October 15, 2019, https://www.washingtonpost.com/sports/2019/10/15/espns-politics-policy-its-journalism-tested-by-nba-china-controversy/.
15. Ethan Zuckerman, "Building a More Honest Internet," Columbia Journalism Review, Fall 2019, https://www.cjr.org/special_report/building-honest-internet-public-interest.php.
16. Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War against Reality* (New York: Public Affairs, 2019), 187.
17. Laura Rosenberger, "Foreign Influence Operations and Their Use of Social Media Platforms," statement before the United States Senate Committee on Intelligence, August 1,

2018, https://securingdemocracy.gmfus.org/foreign-influence-operations-and-their-use-of-social-media-platforms/.
18. Rosenberger, "Foreign Influence Operations."
19. Rosenberger, "Foreign Influence Operations."
20. Zeynep Tufekci, "YouTube, the Great Radicalizer," *New York Times*, March 10, 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.
21. Drew Harwell and Tony Romm, "TikTok's Beijing Roots Fuel Censorship Suspicion as It Builds a Huge U.S. Audience," *Washington Post*, September 15, 2019, https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/; Matt Schrader, "TikTok Risks Becoming New Front in China's Information War," *Nikkei Asian Review*, October 14, 2019, https://asia.nikkei.com/Opinion/TikTok-risks-becoming-new-front-in-China-s-information-war.
22. Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism* (Washington, DC: *Freedom House*, October 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.
23. Lindsay Gorman, "The Challenge in Securing Critical Information," *Fifth Domain*, July 24, 2019, https://www.fifthdomain.com/2019/07/24/the-challenge-in-securing-critical-information/.
24. Ben Allen et al., "Australian Government Passes Consumer Data Right Legislation on 1 August 2019," JD Supra, August 7, 2019, https://www.jdsupra.com/legalnews/australian-government-passes-consumer-57549/.
25. Michael Beckerman, "Americans Will Pay a Price for State Privacy Laws," *New York Times*, October 14, 2019, https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html.
26. Craig Timberg, Drew Harwell, and Tony Romm, "In Accusing China of Disinformation, Twitter and Facebook Take on a Role They've Long Rejected," *Washington Post*, August 20, 2019, https://www.washingtonpost.com/technology/2019/08/20/after-twitter-facebook-blame-china-hong-kong-disinformation-government-defends-its-right-online-speech/.
27. Thomas Brewster, "Iran-Linked Group Caught Spreading COVID-19 'Disinformation' on Facebook and Instagram," *Forbes*, April 15, 2020, https://www.forbes.com/sites/thomasbrewster/2020/04/15/iran-linked-group-caught-spreading-covid-19-disinformation-on-facebook-and-instagram/.
28. "2019 Update on Cyber Threats to Canada's Democratic Process," Canadian Centre for Cybersecurity, April 8, 2019, https://cyber.gc.ca/en/news/2019-update-cyber-threats-canadas-democratic-process.
29. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Washington, DC: United States Cyber Command, April 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010; Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," *Lawfare*, May 10, 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy; Bill Roche, "Summit Helps Chart Way Ahead for Maneuver in Information Environment," U.S. Army, August 7, 2019, https://www.army.mil/article/225430/summit_helps_chart_way_ahead_for_maneuver_in_information_environment.
30. Heidi Tworek, *Responsible Reporting in an Age of Irresponsible Information* (Washington, DC: Alliance for Securing Democracy, 2018), https://securingdemocracy.gmfus.org/responsible-reporting-in-an-age-of-irresponsible-information/#easy-footnote-15-1163.

31. Michael Golebiewski and Danah Boyd, *Data Voids: Where Missing Data Can Easily Be Exploited* (New York: Data & Society, 2019), https://datasociety.net/wp-content/uploads/2019/11/Data-Voids-2.0-Final.pdf.
32. Michael Kofman, et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Washington, DC: RAND Corporation, 2017), 12–16, https://www.rand.org/pubs/research_reports/RR1498.html.
33. "Amid Ongoing COVID-19 Pandemic, Governor Cuomo Launches Multi-Platform, Multi-Language Education and Awareness Campaign to Reach All New Yorkers across the State in All Zip Codes and Communities," Office of the Governor of New York, April 8, 2020, https://www.governor.ny.gov/news/amid-ongoing-covid-19-pandemic-governor-cuomo-launches-multi-platform-multi-language-education.
34. McKenna Aiello, "David Beckham and More Stars Pledging #IStayHomeFor during Coronavirus Outbreak," *E! News*, April 8, 2020, https://www.eonline.com/news/1132724/david-beckham-and-more-stars-pledging-istayhomefor-during-coronavirus-outbreak.
35. Tom McTague. "Britain's Secret War with Russia." *The Atlantic*, December 3, 2019, https://www.theatlantic.com/international/archive/2019/12/britain-russia-nato-disinformation/602836/.
36. "The GRU Globetrotters: Mission London," Bellingcat, June 28, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/.
37. Sopan Deb, "N.B.A. Commissioner: China Asked Us to Fire Daryl Morey," *New York Times*, October 17, 2019, https://www.nytimes.com/2019/10/17/sports/basketball/nba-china-adam-silver.html.
38. Josh Rogin, "The NBA Is Only the Latest Chinese Government Hostage," *Washington Post*, October 7, 2019, https://www.washingtonpost.com/opinions/2019/10/07/nba-is-only-latest-chinese-government-hostage/.
39. Josh Rogin, "How China Forces American Companies to Do Its Political Bidding," *Washington Post*, January 21, 2018, https://www.washingtonpost.com/opinions/global-opinions/how-china-forces-american-companies-to-do-its-political-bidding/2018/01/21/52a1d5a0-fd63-11e7-8f66-2df0b94bb98a_story.html.
40. Nadège Rolland, *China's Vision for a New World Order* (Seattle, WA: National Bureau of Asian Research, 2020), https://www.nbr.org/wp-content/uploads/pdfs/publications/sr83_chinasvision_jan2020.pdf.
41. Herbert Lin, "On the Organization of the U.S. Government for Responding to Adversarial Information Warfare and Influence Operations," *I/S: A Journal of Law and Policy for the Information Society* 15, no.1–2 (Spring 2019): 1–43, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/lin.pdf.
42. Jean-Baptiste Jeangène Vilmer et al., *Information Manipulation: A Challenge for our Democracies* (CAPS and IRSEM, August 2018), https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.
43. Chris Good, "Ahead of Election, Sweden Warns Its Voters Against Foreign Disinformation," *ABC News*, September 8, 2018, https://abcnews.go.com/International/ahead-election-sweden-warns-voters-foreign-disinformation/story?id=57694373.
44. "Code of Practice on Disinformation," *European Commission*, September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.
45. Dwight A. Weingarten, "Social Media Data Analysis Center Included in Senate's NDAA," Morning Consult, June 27, 2019, https://morningconsult.com/2019/06/27/social-media-data-analysis-center-included-in-senates-ndaa/; National Defense

Authorization Act for Fiscal Year 2020, H.R.2500, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/2500/text.

46. Estonian Foreign Intelligence Service, *International Security and Estonia 2019* (Tallinn, Estonia: EFIS, February 2019), 39–42, https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf; Sean Lyngaas, "Kremlin Interference in EU Vote Is Likely, Says Estonian Spy Agency," *Cyberscoop*, March 12, 2019, https://www.cyberscoop.com/russia-interference-eu-elections-estonia-intelligence/.
47. Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
48. Brett Rosenberg and Jake Sullivan, "The Case for a National Security Budget: Why a Better American Foreign Policy Requires a New Way of Paying for It," *Foreign Affairs*, November 19, 2019, https://www.foreignaffairs.com/articles/2019-11-19/case-national-security-budget.
49. Ben Packham, "Senate Committee to Probe Foreign Meddling via Fake News," *The Australian*, December 5, 2019, https://www.theaustralian.com.au/nation/politics/senate-committee-to-probe-foreign-interference-via-social-media/news-story/fb131a329f38ead74c9040f68721b2a1.
50. Benas Gerdziunas, "Baltics Battle Russia in Online Disinformation War," *Deutsche Welle*, October 8, 2017, https://www.dw.com/en/baltics-battle-russia-in-online-disinformation-war/a-40828834.