Routledge
Taylor & Francis Group

The Washington Quarterly

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rwaq20

Democratic Deterrence: How to Dissuade Hybrid Interference

Mikael Wigell

To cite this article: Mikael Wigell (2021) Democratic Deterrence: How to Dissuade Hybrid Interference, The Washington Quarterly, 44:1, 49-67, DOI: 10.1080/0163660X.2021.1893027

To link to this article: https://doi.org/10.1080/0163660X.2021.1893027

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 23 Mar 2021.

Submit your article to this journal

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=rwaq20

Mikael Wigell

Democratic Deterrence: How to Dissuade Hybrid Interference

Western democracy is being attacked like never before, but not through overhyped "hybrid warfare." It is in reality threatened more acutely by hybrid *interference*, attacks that are often subtle, manipulating for cover the very same liberal democratic values that the attack is designed to subvert. The cornerstones of Western democracy—state restraint, pluralism, free media, and economic openness—provide openings for authoritarian actors to interfere in democratic society through a host of covert, non-military means calibrated to undermine their internal cohesion and accelerate political polarization.

For instance, disinformation campaigns have become increasingly evident since the 2016 US elections and have stepped up in the midst of the COVID-19 crisis. Russia, and increasingly China, are deploying disinformation to aggravate the public health crisis in Western countries. Exaggerated and fabricated stories of how Western governments have been mismanaging the spread of the coronavirus have been used to play on the anxieties of Western populations.[1] While not all such disinformation efforts succeed in persuading the public, the

Mikael Wigell is Program Director of Global Security Research at the Finnish Institute of International Affairs and Non-Resident Associate at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). He has been Visiting Scholar at the Changing Character of War Centre, Oxford University, and his latest book is the edited volume *Geo-Economics and Power Politics in the 21st Century: The Revival of Economic Statecraft* (Routledge, 2018). He can be reached at mikael.wigell@fiia.fi.

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.
The Washington Quarterly • 44:1 pp. 49–67
https://doi.org/10.1080/0163660X.2021.1893027

cumulative impact can be very effective in sowing distrust, rendering democratic states less capable of countering either the epidemic or the aggression itself.

Financial support is also being channeled to radical political parties and movements to accelerate centrifugal forces within and among Western democracies.[2] Part of this toolbox involves exploiting the economic openness of Western democracies to capture strategic sectors of the economy—such as critical infrastructure, finance, and media—by which these authoritarian actors can attempt to destabilize Western democracies and purposefully corrupt them.[3]

Democracies urgently need to find means to defend against such hybrid interference without jeopardizing the values that they are meant to defend. Extending state control over civil society is not a viable liberal democratic strategy. Neither should Western democracies mirror the use of weaponized corruption, disinformation, election meddling, and other means of hybrid interference, as this would only further erode liberal democratic values around the globe.

Open societies are agile in responding to strategic challenges

For all their amassed military might, a particular advantage of Western democracies lies in their soft power and inclusive politics. Western democracy still commands widespread attraction and political legitimacy, and open societies are agile in responding to strategic challenges. Rather than the rigidness of state-based solutions, Western democracy harnesses market- and society-based approaches to dealing with risks and threats. These can readily be used to strengthen deterrence against hybrid interference. It is crucial to recognize the deterrent value of democracy itself, namely how it can provide means for deterrence by both denial and punishment. Wielded with confidence, democracy itself is a potent strategic weapon.

This article outlines the strategic logic of hybrid interference and how it puts Western democratic governability in jeopardy. It argues that deterrence policies need to be revamped in the face of this new challenge and suggests a new strategic concept—democratic deterrence—as a framework for dissuading hybrid interference. It asks what deterrent value democracy itself has and envisages a host of non-military means to adapt deterrence to the current non-military challenges. By evolving the concept of deterrence in this way, democratic deterrence shows how liberal democratic values need not be security vulnerabilities, but can be turned into strengths and tools to credibly deter hybrid aggressors, while making our Western democracies more robust and resilient.

The Strategic Practice of Hybrid Interference

Much of the debate on new "hybrid" threats has revolved around "little green men" and other grey zone military tactics, or hybrid warfare, essentially a military approach to conducting "indirect war" under special circumstances.[4] The more pressing challenges from a Western perspective are the more subtle, non-military activities deployed by authoritarian regimes to penetrate democratic society. "Hybrid interference" is a concept developed to capture non-military practices for the mostly covert manipulation of other states' strategic interests.[5] As such, it bears resemblance to what was referred to as "active measures" during the Cold War and, more recently, in Russian strategic debate as *gibridnaya voyna*.

The idea of *gibridnaya voyna* is to avoid the traditional battlefield with the aim of destroying "the political cohesion of an adversary from the inside by employing a carefully crafted hybrid of non-military means and methods that amplify political, ideological, economic and other social polarisations within an adversary's society, thus leading to its internal collapse."[6] While keeping diplomatic relations intact, and thus not breaking any official threshold of war, the aggressor mobilizes oppositionists and radicals within the target state through a host of means ranging from disinformation campaigns to corrupting political actors and financing subversive movements, carefully synchronized to compound the effect.

Hybrid interference avoids the use of overt kinetic means in order to maintain plausible deniability. Yet, it may include the use of targeted violence, through proxies, to inject fear and exploit emotional pressure points in the target society. In 2014, for example, pro-democracy protesters in Taiwan were attacked by some with links to the Chinese Communist Party to incite political tensions and undermine democratic governability.[7] In Montenegro, Moscow instigated a coup attempt before the 2016 elections. The attempt involved harnessing its close relations to the Orthodox Church and the Serb minority population to foment distrust in the democratic process and, in the final phase, using Russian intelligence operatives disguising as police officers to create disruption by shooting protesters and blaming the Montenegrin government for killing innocents.[8]

Central to hybrid interference is *subversion*. Subversion refers to an aggressor state's purposeful attempt to destabilize and undermine the authority of a target state by using local proxy actors.[9] It specifically involves the use of disinformation and economic inducements to recruit and assist these actors inside the target country, detach their loyalties from the target government, and use them as interlocutors to transform the established social order and its structures of authority and norms. The aim is to weaken democratic governance and norms as a means of enhancing their own authoritarian standing. Not only are weakened democracies less able to directly confront these authoritarian aggressors, but they will also look less appealing as models of success and partners for others.

By portraying Western democracies as corrupt and ungovernable, authoritarian regimes such as China, Iran, Russia, and Turkey are less at risk of being overthrown by their own populations.

As such, hybrid interference is designed as a flexible approach in which the tools and tactics can vary but will always be tailored to manipulate existing cleavages and sow internal dissension in target countries and alliances. Hybrid interference does not adopt a one-size-fits-all approach but exploits specific vulnerabilities depending on the context in the target country. The hybrid aggressor interferes in domestic politics by seeking to amplify divisions and hatred, undermining the "civic culture" that has been found to be so important for democratic governability by tempering the intensity of political conflicts and cleavages.[10]

The migrant crisis in Europe offered an excellent opportunity for authoritarian aggressors. By exposing rifts between "liberals" and "anti-liberals," it allowed Russia and Turkey to leverage refugees as a disruptive force, fanning the already simmering political tensions in Europe. Following the outbreak of the Syrian civil war, Russia and Turkey began actively pushing migrants over the borders to Europe, while simultaneously engaging in disinformation campaigns by playing up rumored (or actual) misdeeds by immigrants and portraying European governments as unwilling or unable to manage the influx of people.[11] To compound the polarizing effect, Russia also began channeling money to anti-immigrant and anti-EU political parties and movements such as France's National Front.[12] In this way, particularly Russia has contributed to Europe's surge in anti-immigrant sentiments and populist support, as well as rising democratic dissatisfaction.[13]

Democratic Deterrence as a Novel Strategy

Western democracies urgently need to find counter measures against hybrid interference, recognizing that traditional military deterrence only works against predominantly military threats. By reducing clarity about who is doing what, or even whether somebody is actually doing anything, hybrid interference complicates traditional deterrence.[14] Yet, the attribution problem is not insurmountable. The responsibility for interfering in US elections, for example, was traced and attributed to Russia, though only after a painstaking process involving much controversy and resources.[15] But the question, then, even after the attribution problem is solved, becomes what to do about it? Any prudent deterrence posture needs to avoid unnecessary escalation, and a military response to political interference does not seem proportional.

The strategic concept of democratic deterrence suggests a novel way of thinking about deterrence to dissuade these hybrid interference activities by

Table I: Contrasting Traditional Deterrence with Democratic Deterrence

	Traditional Deterrence	Democratic Deterrence
Agency	State-based	Whole-of-society
Power Base	Hard	Soft
Means	Military	Non-military
Response	Symmetrical	Asymmetrical
Security Aim	Absolute	Limited

authoritarian states. Table 1 summarizes the differences between traditional military deterrence and democratic deterrence.

First, in contrast to traditional deterrence that is state-based, democratic deterrence rests on a whole-of-society approach, albeit one in which the state retains a coordinating role. It harnesses market- and society-based actors in an effort to pull together resources and take full advantage of democracy's societal strengths and cultural capital. This difference is important because in this new era of subversive politics, where the classical Westphalian dichotomy between internal and external state affairs has been blurred, deterrence is harder to achieve by state action alone. Deterring hybrid interference requires a whole-of-society response whereby various societal actors build resilience capacities, support the state in maintaining preparedness, and ensure the continuity of vital societal functions and supply lines. For instance, private actors often own full or partial stakes in critical infrastructure such as energy pipelines, undersea cables, railways, banking and finance, health services, and food supply. Ensuring that they live up to their responsibilities with regard to safety measures must form an essential part of any modern defense. The whole-of-society approach is thus an inclusive model of cooperation and joint preparedness that aims to bring all relevant actors together into a comprehensive system of deterrence. It involves an effort to diversify and devolve responsibilities for security production to market- and societal-based actors, while maintaining a strong coordinating role for the state.

Second, while traditional deterrence relies on hard power, democratic deterrence uses the soft power base of Western democratic societies.[16] Soft power rests on the ability to attract, and liberal democratic values and norms continue to exercise a strong international pull, not least among autocratic subjects.[17] Democratic norms and values are thus strategic assets that can be used to deter authoritarian regimes. Western democracy promotion efforts have helped catalyze regime change in many parts of the world. During the Cold War, Radio Free Europe, a radio broadcasting company set up by the United States, contributed to the demise of communist regimes in Eastern Europe.[18] By signaling strong and concerted preparedness to vigorously engage in democracy promotion, Western democracies can again help deter authoritarian leaders. Crucially, in

an information age, when power is less hierarchical and social networks have become more important, projecting soft power is not only a matter for states. Nonstate actors such as NGOs, research institutes, and corporations are also important for generating soft power. The flexibility of non-governmental actors, such as the National Endowment for Democracy, in building relationships and networks across borders can provide a crucial gateway to strengthen normative legitimacy and mobilize the cause of advancing democracy.

Third, and related to the above, democratic deterrence crucially relies on non-military, democratic means. Democratic values and instruments such as transparency, the rule of law, and citizen activism provide tools for non-kinetic deterrence. Functioning under the threshold of war, they are well calibrated to avoid escalation, while helping deter grey zone activities such as hybrid interference. Hybrid agents thrive on being covert, so transparency is a key means of deterring hybrid interference. Similarly, a strong rule of law is essential to deny efforts to destabilize and accelerate polarization in democratic societies by means such as weaponized corruption. Citizen activism provides a force multiplier in efforts to both deny as well as punish hybrid interference by harnessing civil society's capabilities and agility.

Fourth, while traditional deterrence often relies on "in kind" measures, namely a symmetrical response, democratic deterrence takes the response outside the domain in which the action occurs. In fact, asymmetry is a necessary feature of democratic deterrence. Responding in kind to hybrid interference—and thus mirroring the use of election meddling, corruption operations, disinformation campaigning, and other means of sharp power—will only contribute to the further erosion of liberal democratic values and undermine the normative legitimacy of Western democracy.[19] Moreover, because outright attribution is a troublesome process with regard to hybrid interference, with the hybrid agent using proxies and artificial intelligence (AI) for obfuscation purposes, symmetry can seldom be the optimal response. Instead, by relying on a "democratic playbook" of response options that draw on Western democracy's soft power base, outlined below, hybrid interference can be deterred without compromising normative legitimacy.

Democratic deterrence takes the response outside the domain in which the action occurs

Lastly, whereas traditional deterrence aims at wholly deterring any aggression, democratic deterrence accepts that some actions cannot be deterred. Indeed, absolute deterrence may even induce hostile actors to seek alternative and more dangerous ways to attack Western democracy. Unlike nuclear deterrence, deterrence against hybrid interference is more like crime prevention—not all crimes can be deterred and not all represent significant threats to national security. Conscious

about the need to tolerate a certain set of hostile activities, democratic deterrence settles for a more restrictive aim whereby external interference is not wholly deterred, but modified to render it less effective and frequent.

Advocating for democratic deterrence does not mean that traditional deterrence has become obsolete. Military deterrence remains vital for dissuading armed aggression and various forms of sabotage. It may also contribute to deterring hybrid interference by instilling doubt about the level of response. Traditional military deterrence policies therefore need to be maintained and perhaps even strengthened. Yet, the argument here is that traditional deterrence measures fall short of effectively dealing with the challenge of hybrid interference and therefore need to be complemented by new measures, namely those proposed here.

A Two-Pronged Democratic Deterrence Strategy

Hybrid interference calls for new tools of non-military deterrence. Importantly, any new deterrence posture needs to maintain the openness of democracy and avoid sacrificing any of the Western democratic cornerstones in the name of security. Deterrence is based on increasing the perceived costs of hostile actions to the point of outweighing their potential benefits. In deterrence theory, measures to dissuade hostilities are often divided into two broad categories: denial and punishment.[20] Both categories are also applicable to democratic deterrence. Indeed, much like traditional military deterrence, democratic deterrence can also be designed as a two-pronged strategy of deterrence by denial (i.e., resilience) and by punishment (i.e., compellence). Both are necessary to stop hybrid interference attempts.

Strengthening resilience is a necessary building block of any democratic deterrence posture, but it is insufficient as it is unlikely to deter hybrid interference. Russia's meddling in Western democratic elections, for instance, has continued, despite being publicly exposed and despite measures to strengthen resilience against such external interference. Without any credible deterrence by punishment, these attacks are a relatively low-cost endeavor and can thus be expected to continue. Thus, democratic deterrence must consist of both measures to enhance denial through resilience and punishment, which has not been sought to date.

Strengthening resilience is a necessary building block of any democratic deterrence posture

Deterrence by Denial: Improving Democratic Resilience

Resilience refers to the ability to absorb, adapt, and recover from disruption and duress. High resilience will make it difficult for an aggressor to achieve its strategic

aims, thereby making an attack not worth the costs and effort.[21] Improving resilience helps modernize total defense doctrine by addressing vulnerabilities across state and society. The emphasis needs to be on continuity management of vital societal functions, supply lines, and critical infrastructure, including democratic infrastructure such as elections. As many critical functions are operated partly or even wholly by private sector actors, public-private cooperation is paramount for improving democratic resilience. Small Northern European countries accustomed to the idea of state-society collaboration and pooling resources to balance Russia may serve as an example: Finland's comprehensive security model builds on enhancing preparedness through sustained cooperation between authorities, business operators, and civil society organizations in order to secure the vital functions of state and society.[22] Similarly, democratic deterrence involves preventing or making hybrid interference difficult by harnessing and doubling down on liberal democracy's strengths: activating autonomous civil society, increasing transparency of money flows, and broadening inclusive politics.

Activate civil society

While the open environment of Western democracy presents loopholes for covert interference, it simultaneously provides an enabling environment for citizen activism and market-based innovation. Citizen activism can play a major role in identifying interference and building institutional and societal resilience against it.[23] The essential watchdog functions of the open media environment serve to enable citizen activism by shedding light on hybrid interference. Investigative journalism is a pertinent example, as evidenced by novel online sources like Bellingcat, whose investigations helped solve the Salisbury poisoning case, in which Sergei Skripal—a former Russian military officer and double agent for the British intelligence services—was poisoned together with his daughter by assassins connected to the Russian GRU military spy agency.[24] Similarly, the Organized Crime and Corruption Reporting Project, a network of investigative reporters, helped uncover a Russian money laundering scheme through which funds were channeled to groups lobbying for closer relations between EU countries and Russia.[25]

Citizen activism can play a major role in identifying interference and building resilience against it

Western democracies should encourage investigative civil society groups and media to monitor and detect hybrid interference. Specific measures should include developing rapid alert systems and media literacy programs as well as training media professionals themselves in recognizing fake news. Finland's

Mediapooli, a joint organization set up by the country's media companies, helps train journalists through capacity-building programs, anti-fake news education, and freely distributed guides on how to better protect sources and counter disinformation.[26] In the United States, the Countering Foreign Influence Task Force of the Department of Homeland Security, in coordination with the FBI, began operations for countering disinformation before the 2018 US midterm elections. Its focus has been on raising public awareness about the dangers with foreign disinformation campaigns and working with social media companies and academia to better recognize, understand, and build resilience against foreign disinformation.

The exponential growth of open data is also changing the nature of intelligence from an almost exclusively governmental realm to one with private firms and civil society organizations central in monitoring and exposing hybrid interference. Especially in the digital realm, the private sector is often a step ahead of government in developing new analytic technologies. Facial recognition software, now deployed by most intelligence services whether private or governmental, was developed by Israeli companies. Britain and the United States are increasingly emulating Israel, where government intelligence agencies are embracing the commercialization of espionage instead of battling it.[27] By supporting societal and market-based mechanisms in this way, resilience can be strengthened within the confines of democratic rule of law.

Increase transparency

Second, increased transparency with regard to foreign influence activities will help disrupt and deter alliances between hybrid aggressors and domestic groups, making it more difficult to advance covert agendas. Exercising rights of religious freedom and freedom of speech, Swedish Salafi networks, preaching radical jihadi narratives and seeking out Muslims to decouple them from democratic processes, have expanded rapidly. As it stands, such activities are fully legal and protected by the Swedish constitution and are therefore difficult for the national authorities to scrutinize and restrict. These networks have clear international links and enjoy the support of foreign states such as Saudi Arabia.[28]

To straddle the gap between such illegitimate clandestine interference and legitimate public diplomacy, Western democracies ought to create foreign influence transparency registers. This would require individuals and entities undertaking activities on behalf of foreign principals to register themselves, while criminalizing foreign interference activities. Recent legislation in Australia—namely the Foreign Influence Transparency Scheme Bill and the Espionage and Foreign Interference Bill—provide an example in this regard.[29] The aim of the legislation is to facilitate transparency regarding foreign influence on political processes. It does not prohibit foreign actors from being involved in the country's

political processes, but it creates obligations to disclose information, permitting influence on domestic interests to be assessed. As such, it informs the public about influence activities that might otherwise remain hidden, while also expanding the investigative options with regard to those actors that fail to register.

Economically, transparency of money flows is particularly important. This transparency requires updating regulations regarding ownership disclosure, mechanisms for screening foreign investment, and legislation invoking national security considerations toward foreign investment permit procedures, particularly with regard to strategic resources and critical infrastructure. The European Union's new foreign investment screening mechanism is a step in the right direction, but it will remain toothless without additional regulation at the member state level.[30] In the wake of Chinese acquisitions of sensitive technology companies, Germany introduced new regulations in 2017 and again in 2018, reducing the threshold for screening and blocking foreign purchases.[31] According to German security officials, losing a key technology to Chinese takeover risks making Germany not only more dependent on China but also vulnerable to politicization and espionage—Chinese firms are required by law to share data with the Chinese government and set up Communist party committees, giving the Chinese government control of company decisions.[32]

Most EU member states need new regulation in order to block similar acquisitions on national security grounds, and financial regulators need to be given stronger mandates to investigate financial networks to prevent economic interference. Financial intelligence units and cooperation as well as integrity-building and anticorruption mechanisms are important tools to build institutional resilience and prevent hostile actors from exporting corruption. Two major reports by CSIS show how large economic players in the European Union such as financial and corporate service providers have been entangled in Russian illicit finance schemes, functioning as "enablers" of Russian hybrid interference with direct consequences for democratic processes.[33] In effect, by the purposeful use of corruption and cronyism, Russia has been able to capture influential European political and business elites and, through them, gain influence over decision-making processes while simultaneously weakening and discrediting democratic structures in Europe.

Furthermore, NGOs, political parties, media, research institutes, and think tanks should be required to publicly report their sources of funding. The regulation of digital platforms, such as Facebook and Twitter, is also important in this regard. At present, malicious actors make use of the underregulated environment of digital platforms to collect data and manipulate algorithms to accelerate political polarization.[34] Russia's army of internet trolls (online profiles operated by humans) and bots (operated by automated processes) is well known. It has

been set up to flood social media and web pages with polarizing content, including conspiracy theories, fabrications, and falsehoods, all carefully targeted to compound the effect.[35] Increasing transparency on social media platforms, including political ads, can help reveal the identity of troll accounts and thus help counter disinformation by bringing it into the open.

Broaden inclusion

Third, Western democracies should take advantage of their inherent structures of inclusive politics to improve resilience. Quite simply, the population needs to be made aware of hybrid threats and involved in resilience-building as a precondition for societal security. Societal security seeks to broaden political participation (expand inclusive politics) and improve social welfare as remedies for social cleavages to promote social stability. Enhancing social cohesion, for example, can prevent a hybrid aggressor from using extant social cleavages and political pressure points, such as the Black Lives Matter protests, to fan political polarization. Any hybrid deterrence effort should therefore include policies that enhance education, social cohesion, and welfare.

In particular, such policies need to be directed toward integrating diasporas and minorities, who otherwise risk being used as proxies for hybrid interference efforts. For years, the Kremlin has been mounting a massive disinformation campaign about Finnish authorities practicing terror against Russian families living in the country. The aim seems to be to drive a wedge between the Russian-speaking community living in Finland and the Finnish government and erode Russians' positive image of Finnish democracy.[36] However, the campaign shows few results so far. The Russian-speaking community has been well-integrated, enjoying full citizenship rights and services. The Finnish public broadcaster YLE has expanded its Russian language services and has become an important source of information for the Russian-speaking community. In contrast, the Finnish branch of *Sputnik*, the state-funded Russian media outlet, had to close in March 2016 after failing to attract enough readers.[37]

Obviously, elections remain the cornerstone of democratic inclusiveness. Many Western governments need to amend existing electoral laws to account for meddling tactics; legislation should cover issues like foreign funding of domestic political parties and associations, as well as increased transparency of political advertisements. In the United States, the campaign finance system particularly needs reforming to prevent foreign interference in elections. Current legislation allows foreign companies to spend money on US campaigns through subsidiaries. Even foreign governments can fund campaigns through "dark money" groups that are not required by federal law to disclose their donors. Online political ads are also currently omitted from the laws that prohibit foreign nationals giving money to campaigns.[38] Both the Honest Ads Act and the

DISCLOSE Act, designed to close some of these loopholes in the US campaign finance system, have failed to make it through the US Congress. Online advertisements have been found to be central to Russian election meddling tactics designed to increase tensions over wedge issues.[39]

Deterrence by Punishment: Discovering Democratic Compellence

To be effective, democratic deterrence also needs to incorporate a focus on reciprocity and punishment.[40] At present, hybrid interference largely goes unpunished—and as long as this is the case, interference remains a highly tempting and potentially effective strategy. Compellence refers to a strategy designed to change a target's strategic calculus by way of making a coercive threat.[41] Usually compellence is thought of in terms of military posturing or coercive diplomacy such as economic sanctions, but in addition to sanctions, democracy itself can be a means of compellence. Since antiquity, many authoritarian powers have been terrified by democracy and the threat it poses to authoritarian control. (The Spartans, for example, were famously terrified by the culture of democracy that helped sustain the Athenian empire.)[42] Threatening to double down on democracy promotion in cusp states and regions, which lie uneasily on the political and normative edge of an authoritarian regime's sphere of influence, can present autocrats with a compellent threat.

Democratic deterrence also needs to incorporate a focus on reciprocity and punishment

Communicate response thresholds

First, a strategy of democratic compellence should communicate thresholds of response, or what are deemed unacceptable behaviors that will have consequences. Autocratic adversaries will need to be persuaded of Western democracies' capacity to identify hybrid interference and to respond by imposing costs for such aggression. The response will not be symmetrical, as hybrid interference clashes with liberal principles such as non-interference, but it should be made clear that specific punishment measures and sanctions will be applied in response to specific actions. Calling out hybrid interference is also key for discrediting existing proxies and deterring other potential ones.

Hybrid aggressors should be reminded of the blowback effect inherent in Western democracy, in which an independent media and autonomous civil society perform watchdog and advocacy functions beyond state control. In Western democracies, naming and shaming is often automatic, adding pressure on democratic governments to take counter measures. Russia's interference in

the 2016 US elections was eventually detected and called out, resulting in new sanctions even as President Trump at first seemed reluctant to take any measures. Herein, the signaling effect is important, making potential interferers and their enablers think twice before taking action.

Expand sanctions

Second, Western democracies' autocratic adversaries should be made aware of their own asymmetrical vulnerabilities. The world today is more interdependent and interconnected than at any time in history. All states, including authoritarian ones, depend on being able to connect to the flows of goods, resources, data, and capital that are crisscrossing the globe for their security and wealth. Importantly, these global flows are still mostly controlled by Western democracies, although China has rapidly been extending its "flow power" as well.[43] By banding together, Western democracies can therefore inflict considerable pain on their autocratic adversaries through well-calibrated sanctions and other policies of containment and engagement, including in cyberspace.

For instance, the sanctions against Russia have led to considerable costs for the Russian economy. By depriving Russian state-controlled banks and companies of an important source of long-term financing, credit costs have gone up and investment contracted. According to the International Monetary Fund (IMF), sanctions have reduced Russia's growth rate every year in 2014–18 by 0.2 percent.[44] They have also deprived Russia of important technology needed to uphold Russia's energy and military power.[45] Importantly, Western democracies have come nowhere close to exhausting the sanctions toolbox. The centrality of Western currencies to global capital markets provide the United States and its European allies with extraordinary capabilities to ramp up financial sanctions; by controlling central nodes in the international economy, such as the SWIFT financial messaging network, these sanctions can be reinforced with major costs for target states.[46]

Western democracies have come nowhere close to exhausting the sanctions toolbox

By signaling preparedness to harden sanctions in a coordinated manner, Western democracies can strengthen deterrence. The goal of such compellence is not necessarily to have to carry out the threat in the end, but for compellence to be effective, retaliatory measures need to be in place and able to be actively used when the threshold for a response is crossed. For instance, blocking Internet access to the Internet Research Agency (IRA) in Russia served as a useful reminder of US cyber capacities. This infamous Russian troll factory reportedly sought to repeat its disinformation campaign from the 2016 US elections by trying to sow discord among American during the 2018 midterms. The US operation

prevented the IRA from mounting large-scale cyber-incursions on the eve of the elections by taking it offline and involving direct messaging by way of targeting hackers working for the Russian military intelligence agency—the GRU—letting them know that their real identities were known, causing consternation among them.[47] Similar measures would be useful against Chinese state-supported hackers.

Promote democracy

Third, democratic compellence involves harnessing democracy's soft power to threaten retaliation for hybrid interference. Democracy is a strong value that exercises considerable international pull; therefore, Western democracies have a soft power advantage that can be used to challenge hybrid aggressors on their own turf.[48] Pushing the truth against internal propaganda and cover-ups in authoritarian regimes will serve to challenge them. Threatening to release data about the corrupt practices of authoritarian regimes can be used as a means of compellence.[49] For instance, the Russian leadership has significant assets harbored in the West, which it prefers not to come under public scrutiny in Russia, that can be used as leverage when communicating with Moscow.

Visibly strengthening programs of democracy and human rights promotion will also communicate resolve and threaten to shift the battleground to the authoritarian states' neighborhood and home turf. In this vein, cultivating Western democracies' own influence of networks and proxies—using civil society as an interlocutor and other means of soft power such as cultural institutions and citizen diplomacy—provide the means for democratic compellence. Civic associations in authoritarian states often view their counterparts in the West as kindred spirits and uphold relations with them. These relations can be targeted for support, forcing the authoritarian regime to choose between either allowing them and risking more citizen activism or going harder on civil society, with the risk of further eroding its own legitimacy. Supporting political dissent not only can target autocracies, but can also be an effective way to break through authoritarian controls among their diasporas residing in Western democracies. During the Arab Spring, diaspora activists working in partnership with dissidents in the home country were instrumental in publicizing information that the regimes sought to repress.[50]

What authoritarian regimes fear most is bottom-up democratizing developments

What authoritarian regimes fear most is bottom-up democratizing developments, such as the color revolutions and the Arab Spring. Planning for a vigorous and concerted democracy and human rights promotion effort in the Chinese and

Russian neighborhood would help create a situation in which hybrid aggressors would need to weigh benefits of continuing its campaigns against potential risks more carefully. For instance, signaling preparedness to support democracy and human rights in an escalatory manner in places like Belarus and Hong Kong may be used as compellence vis-à-vis Russia and China.

Western democracies' adversaries will no doubt denounce even this soft retaliation as merely another form of hybrid interference. In reality, there are differences in terms of normative legitimacy. Whereas hybrid interference is covert, and therefore illegitimate, democracy and human rights promotion is overt and transparent, and therefore a form of legitimate public diplomacy, albeit with a sharp edge designed for compellence purposes. In contrast with hybrid interference, democratic compellence is in line with international law.

Western democracies should not be naïve about the effects of such democracy and human rights promotion. Authoritarian regimes are likely to respond to it by cracking down on any dissent. However, by publicly exposing their authoritarianism in this way, the struggle for normative legitimacy will tip even more in favor of Western democracies, boosting their soft power. In other words, overturning any authoritarian government is not always the goal, but raising the threat of civil strife in those countries serves the purpose of democratic compellence to help deter hybrid interference.

Conclusion

In essence, hybrid interference entails a coordinated attack on democracy, using the very democratic infrastructure to accelerate polarization and weaken democratic governance. If successful, it risks deconsolidating Western democracy. Western democracies must therefore take urgent measures to minimize their vulnerabilities to hybrid interference. This involves rediscovering and revamping deterrence policies free from the analogy to Cold War-era nuclear deterrence, the aim of which was total prevention through the threat of massive retaliation. In the hybrid era, deterrence should focus on consistency and making attacks less effective, while recognizing that some elements of interference will be hard to deter entirely.[51]

At the same time, hybrid interference also paradoxically presents opportunities. By exposing our vulnerabilities, it provides a "stress test" of democracies. Crafting effective policy responses involves deepening democratic infrastructure and values so as to make them more robust against illiberalism and institutional decay. Authoritarian regimes such as China, Iran, Russia, and Turkey did not create the initial conditions of the current polarizing tendencies that make Western democracy vulnerable—they are merely seizing the moment to

opportunistically foment these tendencies. It is therefore up to the Western democracies themselves to address these underlying problems of social distrust, polarization, and weak institutions. If seen as an opportunity, it may catalyze democratic development.

The concept of democratic deterrence shows how democratic values are not only vulnerabilities, but that they can be turned into strengths and tools for a credible deterrence response to hybrid interference. Democratic deterrence focuses on strengthening our liberal democratic values and infrastructure: transparency, accountability, inclusiveness, and civil society. To this end, deliberately focusing on *democratic* deterrence will simultaneously improve democratic governance, making Western democracies more robust and resilient. Adversaries would like democracies to react to their hybrid interference by closing off their open platforms, in line with their narrative about a supposed trade-off between democracy and security. The concept of democratic deterrence shows how there need not be any such trade-off and that deepening democracy may go hand-in-hand with strengthening security. Security can be provided—even strengthened—all while maintaining the openness inherent to Western democracy.

Democratic deterrence is designed to render hybrid interference less efficient and less attractive as a strategy. While any hybrid defense will also need to rely on armed forces, putting the focus on democratic deterrence has the advantage of avoiding outright military escalation. But make no mistake, democracy is also a strategic weapon, much feared by the Spartans of both yesterday and today. As such, it will be particularly effective when all of its elements are wielded collectively by Western democracies.

Notes

1. EUvsDisinfo, *COVID-19 Disinformation* (Brussels: EEAS, May 2020), https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid19-pandemic-updated-23-april-18-may/.
2. Alina Polyakova, Marlene Laruelle, Stefan Meister, and Neil Barnett, *The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom* (Washington, DC: Atlantic Council, 2016), https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/.
3. Heather A. Conley, James Mina, Ruslan Stefanov and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Lanham: Rowman and Littlefield, 2016)
4. Ofer Fridman, *Russian 'Hybrid Warfare': Resurgence and Politicisation* (London: Hurst & Company, 2018).
5. Mikael Wigell, "Hybrid Interference as a Wedge Strategy," *International Affairs* 95, no. 2 (2019): 255–75, https://doi.org/10.1093/ia/iiz018.
6. Fridman, *Russian 'Hybrid Warfare'*, 96.

7. James Jiann Hua To, *Qiaowu: Extra-territorial Policies for the Overseas* (Leiden: Koninklijke Brill, 2014).
8. Heather A. Conley, *Russian Malign Influence in Montenegro: The Weaponization and Exploitation of History, Religion, and Economics* (Washington, DC: CSIS, May 14, 2019), https://www.csis.org/analysis/russian-malign-influence-montenegro.
9. Henrik Breitenbauch and Niels Byrjalsen, "Subversion, Statecraft and Liberal Democracy," *Survival* 61, no. 4 (2019): 31–41, https://doi.org/10.1080/00396338.2019.1637118.
10. Larry Diamond, *Developing Democracy: Toward Consolidation* (Baltimore, MD: Johns Hopkins University, 1999).
11. See, for example, Stefan Meister, "The 'Lisa Case': Germany as a Target of Russian Disinformation," *NATO Review*, July 25, 2016, https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html; Katri Pynnöniemi and Sinikukka Saari, "Hybrid Influencing – Lessons from Finland," *NATO Review*, June 28, 2017, https://www.nato.int/docu/review/articles/2017/06/28/hybrid-influence-lessons-from-finland/index.html.
12. Paul Sonne, "A Russian Bank Gave Marine Le Pen's Party a Loan. Then Weird Things Began Happening," *Washington Post*, December 27, 2018, https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html.
13. For a recent analysis, see Hanspieter Kriesi, "Is There a Crisis of Democracy in Europe," *Politische Vierteljschrift* 61 (2020): 237–60, https://link.springer.com/article/10.1007/s11615-020-00231-9.
14. Multinational Capability Development Campaign, *Can Hybrid Attacks Be Deterred? And If So, How Do We Do It?* (Vienna: MCDC, March 2018), http://mepoforum.sk/wp-content/uploads/2019/03/CHW-Information-Note-Can-Hybrid-Attacks-be-Deterred.pdf.
15. See Robert S. Mueller, *Report on the Investigation into Russian Interference in the 2016 Election* (Washington, DC: US Department of Justice, March 2019), https://www.justice.gov/storage/report.pdf.
16. On soft power, see Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs, 2011).
17. Richard Wike, Katie Simmons, Bruce Stokes, and Janell Fetterolf, "Globally, Broad Support for Representative and Direct Democracy," *Pew Research Center*, October 16, 2017, https://www.pewresearch.org/global/2017/10/16/globally-broad-support-for-representative-and-direct-democracy/.
18. A. Ross Johnson, *Radio Free Europe and Radio Liberty: The CIA Years and Beyond* (Stanford: Stanford University Press, 2010).
19. On sharp power, see Christopher Walker, "What is Sharp Power?," *Journal of Democracy* 29, no. 3 (2018): 9–23, https://www.journalofdemocracy.org/articles/what-is-sharp-power/.
20. For the original categorization, see Glenn H. Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 1961).
21. MCDC, *Can Hybrid Attacks Be Deterred?*
22. The Security Committee, *The Security Strategy for Society* (Helsinki: Finland Government, November 2, 2017), https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.
23. Mathieu Boulègue, Orysia Lutsevych, and Anaïs Marin, "Civil Society under Russia's Threat: Building Resilience in Ukraine, Belarus and Moldova," *Chatham House*,

November 8, 2018, https://www.chathamhouse.org/publication/civil-society-under-russias-threat-building-resilience-ukraine-belarus-and-moldova.
24. Luke Harding, "A Chain of Stupidity: The Skripal Case and the Decline of Russia's Spy Agencies," *The Guardian*, June 23, 2020, https://www.theguardian.com/world/2020/jun/23/skripal-salisbury-poisoning-decline-of-russia-spy-agencies-gru.
25. Organized Crime and Corruption Reporting Project, "The Russian Laundromat Exposed," March 20, 2017, https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/.
26. Elisabeth Braw, "Loose Lips Sink Democracies?," *Foreign Policy*, November 19, 2019, https://foreignpolicy.com/2019/11/19/russia-using-west-reporting-against-here-how-to-respond/.
27. Edward Lucas, "The Spycraft Revolution: Changes in Technology, Politics, and Business Are All Transforming Espionage. Intelligence Agencies Must Adapt – Or Risk Irrelevance," *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/.
28. Magnus Ranstorp et al., *Between Salafism and Salafi-Jihadism: Influences and Challenges for Swedish Society* (Stockholm: Swedish Defence University, 2018).
29. Gareth Hutchens, "Sweeping Foreign Interference and Spying Laws Pass Senate," *The Guardian*, June 28, 2018, https://www.theguardian.com/australia-news/2018/jun/29/sweeping-foreign-interference-and-spying-laws-pass-senate.
30. European Commission, "EU Foreign Investment Screening Regulation Enters into Force," press release, April 10, 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=2008.
31. Holger Hansen and Michael Nienaber, "With an Eye on China, Germany Tightens Foreign Investment Rules," *Reuters*, December 19, 2018, https://www.reuters.com/article/us-germany-security-m-a/with-eye-on-china-germany-tightens-foreign-investment-rules-idUSKBN1OI0UP.
32. Andrea Shalal, "Germany Risks Losing Key Technology in Chinese Takeovers: Spy Chief," *Reuters*, April 11, 2018, https://www.reuters.com/article/us-germany-security-china/germany-risks-losing-key-technology-in-chinese-takeovers-spy-chief-idUSKBN1HI2IS.
33. Conley et al., *The Kremlin Playbook*; Heather A. Conley, Donatienne Ruy, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook 2: The Enablers* (Lanham, MD: Rowman and Littlefield, 2019).
34. For a recent account, see Nicole Perlroth, "A Conspiracy Made in America May Have Been Spread by Russia," *New York Times*, June 15, 2020, https://www.nytimes.com/2020/06/15/technology/coronavirus-disinformation-russia-iowa-caucus.html.
35. To understand Russian use of disinformation, see Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016).
36. EUvsDisinfo, "'Finland Puts Russian Kids in Prison' – Disinformation that Shaped the Minds of Millions," August 6, 2018, https://euvsdisinfo.eu/finland-puts-russian-kids-in-prison-disinformation-that-shaped-the-minds-of-millions/.
37. Reid Standish, "Why Is Finland Able to Fend Off Putin's Information War?," *Foreign Policy*, March 1, 2017, https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.
38. For an analysis, see Brennan Center for Justice, "Limiting Foreign Meddling in U.S. Campaigns," August 14, 2019, https://www.brennancenter.org/our-work/analysis-opinion/limiting-foreign-meddling-us-campaigns.

39. See, for example, Young Mie Kim, "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen," *Brennan Center for Justice*, March 2020, https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more.
40. Heine Sørensen and Dorthe Bach Nyemann, *Going Beyond Resilience: A Revitalized Approach to Countering Hybrid Threats* (Helsinki: Hybrid CoE, November 2018), https://www.hybridcoe.fi/wp-content/uploads/2019/01/Strategic-analysis-Sorensen-Nyeman-11-2018.pdf.
41. See Maria Sperandei, "Bridging Deterrence and Compellence: An Alternative Approach to the Study of Coercive Diplomacy," *International Studies Review* 8, no. 2 (2006): 253–80, https://www.jstor.org/stable/3880225.
42. See Andrew Lambert, *Seapower States: Maritime Culture, Continental Empires and the Conflict that Made the Modern World* (New Haven: Yale University Press, 2018).
43. Jonathan Woetzel et. al., "China and the World: Inside the Dynamics of a Changing Relationship," McKinsey Global Institute, July 2019, https://www.mckinsey.com/featured-insights/china/china-and-the-world-inside-the-dynamics-of-a-changing-relationship#.
44. International Monetary Fund, "Russian Federation," *IMF Country Report*, no. 19/260 (August 2019), https://www.imf.org/en/Publications/CR/Issues/2019/08/01/Russian-Federation-2019-Article-IV-Consultation-Press-Release-Staff-Report-48549.
45. Antto Vihma and Mikael Wigell, "Unclear and Present Danger: Russia's Geoeconomics and the Nord Stream II Pipeline," *Global Affairs* 2, no. 4 (2016): 377–88, https://doi.org/10.1080/23340460.2016.1251073.
46. For a recent discussion, see Thomas Oatley, "Weaponizing International Financial Interdependence," in *The Uses and Abuses of Weaponized Interdependence*, ed. Daniel W. Drezner, Henry Farrell, and Abraham L. Newman (Washington DC: Brookings Institution Press, 2021).
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. J.P. Singh and Stuart MacDonald, *Soft Power Today: Measuring the Influences and Effects* (Edinburgh: University of Edinburgh, 2017), https://www.britishcouncil.org/sites/default/files/3418_bc_edinburgh_university_soft_power_report_03b.pdf.
49. Thomas Wright, "Democrats Must Act Now to Deter Foreign Interference in the 2020 Election," *Brookings*, October 4, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/10/04/democrats-must-act-now-to-deter-foreign-interference-in-the-2020-election/.
50. Dana M. Moss, "The Importance of Defending Diaspora Activism for Democracy and Human Rights," Freedom House, 2020, https://freedomhouse.org/report/special-report/2020/importance-defending-diaspora-activism-democracy-and-human-rights.
51. Multinational Capability Development Campaign, *Hybrid Warfare: Understanding Deterrence* (Vienna: MCDC, March 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795220/20190304-MCDC_CHW_Info_note_6.pdf.