SOCIAL SCIENCES

The digital repression of social movements, protest, and activism: A synthetic review

Jennifer Earl[1]*, Thomas V. Maher[2], Jennifer Pan[3]

Repression research examines the causes and consequences of actions or policies that are meant to, or actually do, raise the costs of activism, protest, and/or social movement activity. The rise of digital and social media has brought substantial increases in attention to the repression of digital activists and movements and/or to the use of digital tools in repression, which is spread across many disciplines and areas of study. We organize and review this growing welter of research under the concept of digital repression by expanding a typology that distinguishes actions based on actor type, whether actions are overt or covert, and whether behaviors are shaped by coercion or channeling. This delineation between broadly different forms of digital repression allows researchers to develop expectations about digital repression, better understand what is "new" about digital repression in terms of explanatory factors, and better understand the consequences of digital repression.

Digital and social media offer important new tools for social movements, activists, and state critics (*1*) as well as substantial avenues for expanding state surveillance and suppression of those same actors (*2*, *3*). Here, we advance scholarship on these countervailing forces by organizing a growing welter of research under the concept of "digital repression." Repression is a broad concept that historically includes actions or policies that are meant to, or actually do, raise the costs of activism (*4*, *5*). A half-century-old literature on repression uses the label as a nonnormative term of art to describe actions taken against a wide variety of actors, including left- and right-wing groups, in more and less democratic countries. Repression is distinguishable from general governance in that it is designed to prevent, reduce, and/or control noninstitutional challenges (e.g., protest, social movements, and activism) and is distinct from broader carceral systems that govern many kinds of activity.

Digital repression is a newer term that is growing in use despite differing (*6*, *7*), and sometimes absent, definitions (*8*). It does not refer to basic Internet governance (*9*, *10*), unless that governance is designed to limit opportunities for contestation. In this review, we define digital repression as actions directed at a target to raise the target's costs for digital social movement activity and/or the use of digital or social media to raise the costs for social movement activity, wherever that contestation takes place. This conforms to key researchers' use of the term, including Feldstein (*11*), who focuses on the later aspect of our definition but also includes the former by including "the targeted persecution of online users" [(*11*), p. 35] in his conceptualization. He notes that "one of the favored techniques" of digital repression "particularly for governments that lacked more sophisticated capabilities—was to persecute individuals who advocated online for political change" [(*11*), p. 36]. Although many, but not all (*12*), scholars only include the use of digital tools for repression as digital repression (*13*), we argue below that this is incomplete and misses other aspects of what is "new" about some forms of digital repression.

Substantively, this means that digital repression is a capacious concept that includes (i) the use of traditional repressive techniques against digital protesters (e.g., the arrest of political bloggers or private harassment and/or violence against online activists); (ii) the use of digital tools in the performance of traditional repressive actions (e.g., state-of-the-art digital surveillance); and (iii) the development and deployment of information strategies designed to diminish protest (e.g., China's so-called 50-Cent Army). Through a typology that we introduce below, we argue that phenomena as distinct as online disinformation campaigns, digital social credit schemes, private online harassment campaigns by lone individuals, and regime violence against online political actors can all be conceptualized as digital repression.

These various forms of digital repression have been studied across many disciplines, which have approached them with dissimilar fundamental questions, diverse extant theoretical and methodological tool kits, and varying awareness of existing research on traditional forms of social movement repression (*14*). In addition to bringing work from social movement scholars (who primarily draw from sociology and political science), communication scholars, and interdisciplinary digital and social media scholars together in a common conversation, we update a well-used typology to organize and provide insights into this quickly developing research field.

FROM ANALOG TO DIGITAL REPRESSION

Governmental actors—including militaries and police, as well as private entities ranging from corporations, to hate organizations, to vigilantes—have long tried to prevent, limit, or otherwise control protest and social movements (*15*), most often by trying to control movement activists, movement organizations, and movement tactics. Referred to as the study of repression, this literature has sought to understand what explains repression (i.e., when it will be used, its form, its severity, etc.) and its impacts on activists and movements (i.e., deterrence, backlash, etc.). The lion's share of this work has focused on violence by local or national police and/or militaries (*5*). Smaller shares of research have focused on explaining the causes and consequences of arrests and other rights violations (*16*, *17*) as well as laws and/or corporate policies that affect the viability of protest (e.g., company towns that make any protest very difficult *18*), among other topics.

[1]School of Sociology, University of Arizona, Tucson, AZ, USA. [2]Department of Sociology, Anthropology, and Criminal Justice, Clemson University, Clemson, SC, USA. [3]Department of Communication, Stanford University, Stanford, CA, USA.
*Corresponding author. Email: jenniferearl@email.arizona.edu

A well-cited theoretical review by Earl (*19*) organized what decades ago was a jumble of research findings on repression to demonstrate the utility of a novel theoretical typology. Specifically, the typology focused on three critical distinctions: (i) whether repressors are state or private actors and, if state actors, whether those actors are directly controlled by national governments or are more decentralized (e.g., local police in the United States); (ii) whether repression is overt—where repressors recognize repression may be observed by others—or covert, as when repressors at least try to conceal their actions and/or motivations, even if they are not always successful; and (iii) whether attempts at control involve force and coercion (e.g., physical violence, arrests, or harassment-based strategies) or instead seek to incentivize preferred forms of expression and behavior, referred to in the literature as channeling (*20*), such as tax laws that reward nonprofits for education but discourage advocacy (*21*).

By crossing these three dimensions, Earl (*19*) identified 12 unique types of repression (e.g., overt coercion by national authorities and covert channeling by private authorities), reflected in the structure of Table 1. Subsequent research has shown the utility of this typology. It also revealed that some of its distinctions may be more complicated and/or empirically fuzzier than at first glance (*22*). For instance, boundaries between state actors and private actors may be fuzzy, with private actors sometimes acting on their own and sometimes acting in league with or on behalf of regimes. Subsequent research has also shown that media may play a larger role in conventional repression than the typology recognized (*23*). Of course, as is true of any typology, it conceals some variation within categories (e.g., some national authorities are easily controlled by political elites while others may be more independent). That said, the increasingly pervasive use of digital and social media and the massive growth in research on digital repression makes it clear that this typology could be usefully expanded, particularly if scholarship is to build on the strong foundation that already exists in the repression literature for analyzing the causes and consequences of repression.

We adapt and expand this typology in two ways to capture the dynamics of digital repression. Table 1, introduced in the next section, replicates Earl's typology but applies it to digital repression by focusing on forms whose impacts on activism are thought to operate through similar processes as predigital examples of the same type of repression. For instance, repressors still hope to use coercion to influence activism through deterrence or selective incapacitation, even if there are some differences in efficiency and collateral damage (*11*). We then extend Earl's typology in Table 2 in the Controlling and Channeling Information section to focus on forms of digital repression that differ in their operation in notable ways from traditional forms of repression. In making these distinctions, and using the term digital repression versus simply repression, we seek to recognize that there are both already well-known and new aspects to digital repression. To be sure, we do not believe that everything about digital repression is new; we argue that this burgeoning fields' potential is limited by the assumption that researchers can be experts on digital repression without also being experts on traditional social movement repression or authoritarianism. But it is also incorrect to assume that nothing is new. Other reviews of parts of this sprawling terrain exist, including reviews using a network layers approach (*24*) and a model focused on information control (*2*). However, our typology is more capacious and firmly connects the growing digital repression literature to the well-developed extant literature on repression.

Table 1. Digital repression drawing on traditional processes.

	Physical control			
	Physical coercion		**Channeling**	
	(e.g., violence, arrests, and surveillance)		**(i.e., carrots for preferred behavior or overbroad sticks)**	
	Overt	Covert	Overt	Covert
State agents tightly coupled with national political officials	Physical violence or legal action against digital activists by militaries or national police (e.g., arrest of bloggers)	Digital surveillance by national authorities (e.g., NSA surveillance in the United States)	State-sanctioned online grievance platforms (e.g., online petitions to the White House site)	National laws or policies that limit online speech and/or activity (e.g., online morality and defamation laws), including but not limited to dissent
	-1-	-2-	-3-	-4-
State agents loosely connected with national political officials	Physical violence or legal action against digital activists by local police (e.g., arrests of Twitter account holders)	Digital surveillance by local authorities (e.g., local U.S. police stingray use to monitor protesters' cellphones)	Local government online grievance platforms (e.g., local government complaint sites)	Regional or local social credit systems (e.g., local experimentation with social credit systems in Chinese cities)
	-5-	-6-	-7-	-8-
Private agents	Physical violence, harassment, or legal action by private actors (e.g., individuals and groups doxing and harassing protesters online; private lawsuits to harass online activists)	Private surveillance (e.g., security contractors tracking protesters through online media) and surveillance capitalism	Corporate online complaint forums and/or organizational social media policies (e.g., policies about candidate and/or employee social media usage)	Platform community standards and/or platform reward structures (e.g., Facebook and Twitter)
	-9-	-10-	-11-	-12-

Controlling people and movements: Physical coercion and channeling

Physical and legal coercion (or their threat) and channeling are being used to repress digital protesters and movements, just as they have been against (street) activists in the past. Table 1 reproduces the original categorizations from Earl (*19*) but illustrates those types of repression using examples from digital repression.

Overt coercion is typically the most obvious form of repression. Indeed, the performative nature of overt repression is often an important part of its deterrence-based motivation, as authorities seek to use observable punishment to deter specifically targeted activists (i.e., specific deterrence) and/or activism generally (i.e., generalized deterrence).Indeed, overt coercion—particularly by national militaries, nationalized police, and other national actors—has been the most prolific area of research on repression (*15*).

Often referenced in political science as the study of physical integrity violations [i.e., murders, disappearances, torture, and political imprisonment; see (*25*)], interest in overt coercion extends into scholarship on digital repression as researchers have worked to understand how often, under what circumstances, and to what effect national political actors use coercive tools against online activists and activists who use digital tools to mobilize others (see Table 1, cell 1). Many examples in nondemocratic contexts exist in the literature (*26*), including the imprisonment of Saudi bloggers (*27*), what Human Rights Watch calls the "vicious crackdown" on activists generally—including those that may use digital tools—by the Azerbaijani government (*28*), Kazakhstan arrests of bloggers and online activists (*29*), and other examples (*30*). Activists and movements often operate in both physical and digital spaces, and we do not seek to fixate on the distinction between repression and digital repression. We think it is important for digital repression research to attend to actors who are more threatening to a regime because of the size or scope of their online audience.

Targets for overt coercion may also be based on digital surveillance (*31*), discussed more under covert coercion below. Regimes have also learned how to use tools used against them—such as memes—to engage in more quotidian harassment of activists (*32*). Notably, Internet and social media proliferation has also globalized these methods of control into cases of "transnational repression" (*33*, *34*). For example, the Syrian government threatened diaspora activists' families to deter diasporic resistance, which often occurs online (*34*), and blacklisted dissidents from returning home (*35*).

There is also evidence that democracies use overt coercion against digital activists. For instance, the British police—coordinated by a national antiextremist unit—have monitored social media to make pre-emptive arrests before protests occur (*36*). In the United States, the Federal Bureau of Investigation has used Twitter posts to justify raids on activists' homes (*37*). More generally, one of the themes that we stress across the review is that repression has never been, and is still not, the proprietary domain of autocrats; researchers should not presume that digital repression is a question with which only students of autocratic regimes need be concerned.

The capacity and interest of authorities in democracies to use overt coercion are particularly clear when examining lower-level political actors (see Table 1, cell 5). Local British constabularies, for instance, have followed the national example of using social media to plan pre-emptive and event-specific policing tactics and have engaged in pre-emptive conversations with protest leaders and online influencers to warn that their actions are being monitored, in addition to digital surveillance discussed below (*36*). This reflects a trend in policing—whether in authoritarian or democratic regimes—to engage increasingly in so-called pre-emptive policing based on data analytics (*38*). In the United States, state police have arrested individuals who tweeted about police activity at protests (*37*), and state-level officials have threatened to prosecute people who used digital tools to challenge the Electoral College in innovative ways (*39*).

Private actors, whom traditional repression research has relatively ignored to its detriment (*40*) despite some recent rising interest in the topic (*22*), also have been overtly coercive online (Table 1, cell 9). Private efforts include individuals engaging in uncoordinated online harassment of social movement actors through social media, email, and other platforms. For instance, Sobieraj (*41*) discusses the intense harassment of women online, which she argues can include doxing, threats of violence, and other forms of harassment. Such harassment is often directed at women for their public and/or political statements but certainly occurs more broadly than that too (*42*). Repression by private actors also encompasses uncoordinated individual efforts coalescing into a more coherent attack, as it did against women broadly and feminists specifically, in #Gamergate. Benefiting from specific platform policies and algorithms, #Gamergate harassers used Reddit as a base for activism (*43*). Likewise, supporters of the Thai monarchy assembled a Google Map of more than 400 people they accused of speaking of the monarch (*44*); the map was presumptively public to facilitate private attacks.

Private overt coercion can also be coordinated from its inception, as when online collectives such as Anonymous engage in collective harassment of targets. Although Anonymous has targeted governments and major organizations (*45*), members have also doxed and harassed people involved in movements, including QAnon in the United States (*46*). Major organizations have also used these methods; for example, the Church of Scientology (which was itself a target of Anonymous) used the legal system to punish and push online critics toward bankruptcy (*47*).

Private actors, including private individuals, groups, and/or companies, can also collaborate with nation states. Countries such as Saudi Arabia have contracted with private actors to surveil and attack activists, dissidents, and journalists living outside its borders (*48*). For instance, regime supporters have attacked online critics as well as attacking other groups of people that the state may itself also seek to target such as sexual minorities (*49*). Relatedly, a Canadian oil company reimbursed Minnesota police for surveilling and arresting antipipeline activists (*50*). Sometimes these efforts may be seen as prosocial and/or as helping (or forcing the hand of otherwise reticent) authorities, as when antifascist and Black Lives Matter activists have used digital and social media to identify and "out" white supremacists (*51*).

Of course, coercion is not always meant to be observed: Covert repression seeks to achieve suppression through nonperformative means, such as using surveillance or agent provocateurs to dismantle the institutional capacity of social movements. In Table 1, we use the terminology of covert, although Earl (*19*) used "unobserved." In either phrasing, the meaning is common: actions that are more practical and/or thought more effective if unnoticed (Table 1, cells 2, 6, and 10) or done in ways that make the connection to protest harder to discern (as in channeling; Table 1, cells 4, 8, and 12).

Nation states' use of digital surveillance (Table 1, cell 2) is long-standing and well-documented (*2*, *3*, *52*). This surveillance can take many forms and allows governments to harvest intelligence

that can be used to target coercion (*13*, *30*, *53*–*56*). For instance, dual-use technologies, such as deep packet inspection, allow operators to monitor Internet traffic and content (e.g., email and content from apps and browsers) and funnel information into state-sanctioned torture programs (*31*). Likewise, social media can be monitored in similar ways (*57*). While traditional surveillance is often done on specific targets or smaller groups of targets, digital repression allows surveillance to happen "at scale" when done at the Internet backbone or Internet Service Provider (ISP) level, providing regimes unprecedented windows into public discontent (*58*), social movements (*59*), and even the performance of lower-level state functionaries whose incompetence or corruption may be inciting unrest (*57*). States such as India and China have had direct access to telecommunications networks and the phone calls, SMS messages, and email transferred across them (*60*, *61*). Syria and former Soviet states have used similar access to surveil the digital activities of opposition members (*62*, *63*). Although many are quick to focus on autocratic uses of surveillance, Western democracies—including the United States (*64*) and Britain (*36*)—have substantial surveillance capacities. They may use surveillance for similar purposes as autocrats, such as pre-emptive interventions to stop or limit protest. Given leaked information from Snowden, this includes covert access to telecommunications networks too (*65*, *66*).

Lower-level state actors often lack the same scale of access. They may, nonetheless, engage in social media monitoring and other forms of digital surveillance (Table 1, cell 6). In the United States, for instance, a range of local police departments and/or sheriff offices have directly monitored or contracted for the monitoring of the social media of movements and activists (*67*). This includes monitoring constitutionally protected speech and tracking movements without a clear legal basis (*68*). Other digital options are available to local and state police too, including the use of phone location records or technologies that intercept cellphone traffic such as StingRay (*69*). In democracies, local authorities' involvement in digital surveillance can be particularly problematic. Legal guardrails for protecting speech and assembly do not appear to be robustly in place across local law enforcement, risking the unlawful and/or unethical use of these technologies (*70*). Moreover, as the limited monitoring of the social media of pro-Trump insurgents before 6 January 2021 shows, law enforcement at all levels may be more likely to monitor for and believe sensational social media posts about groups they oppose and/or are socially distant from (e.g., Black Lives Matter) but fail to use surveillance capacities even in the face of clear threats from groups they support and/or are connected to (*71*).

Surveillance from national authorities or regional coordinating centers (e.g., so-called Fusion Centers in the United States) can also be funneled to local police for further investigation (*36*) or action. For instance, Xu (*58*) examines local government uptake of China's Golden Shield national digital surveillance program, resulting in increased arrests of political prisoners at the local level.

Covert surveillance can also be done by a range of private actors (Table 1, cell 10). First, individuals and groups may engage in online surveillance. Pearce (*72*) persuasively argues that covert Communist surveillance and harassment, referred to as kompromat, has been "democratized," allowing peers and youth organizations in Azerbaijan to use these tools. As she explains: "social media provide an excellent way for a kompromat distributor to spread compromising information and create political drama in fast, efficient, anonymous, and affordable ways that will be seen by a large audience" (*72*).

Second, corporations are also pivotal in this area on their own and through their partnerships with governments. Governments and corporations may contract directly with hacking groups or work with them indirectly through intermediaries such as private investigators (*73*, *74*). The rise of what has been called surveillance capitalism—the harvesting, joining, analysis, and sale of private data—has allowed simultaneously at-scale and microtargeted surveillance of users' actions and interests by corporations. While often deployed to make products, games, and platforms more enticing or addictive (*75*), these data can also be used to target mobilizing and demobilizing messages and to track activists and movements, among other uses, and are rife with the potential for misuse (*76*). Moreover, some of the same identifiers and policies that are profitable to social media companies, such as real-name policies and more rigorous registration policies, are a boon for governments intent on repressing activists (*60*, *77*). Private companies have profited by selling users' personal data to law enforcement (*78*, *79*); selling the technologies needed to conduct network-based surveillance to governments in Syria, Iran, and Libya (*31*); selling spyware that draws on zero-day exploits to turn mobile phones into mobile surveillance tools (*80*, *81*); and selling artificial intelligence tools that are used for broad surveillance and can be easily repurposed for repressive ends (*82*). For-profit firms such as the NSO Group, the Gamma Group, and the now-defunct Hacking Team also provide states access to exploitation, hacking, and surveillance services (*60*, *83*, *84*).

Digital repression can involve channeling, too. This occurs when incentives are delivered for voice and behavior preferred by the repressor and/or rules, policies, or, laws broadly limit voice and/or behavior but have notable protest-specific effects. The core idea is that whether by providing incentives or changing the constraints on various forms of action through broad laws or policies, repressors attempt to obtain preferred behaviors without direct pressure or force.

Overt channeling by national authorities is easily done by providing a forum for expression and/or complaints, which constrains the format of contestation while it appears to invite comment and display openness (Table 1, cell 3). In the United States, for instance, both the Obama and Trump White House websites offered petitioning platforms that allowed concerns to be cultivated like English gardens. Petitions on the Trump White House site revealed another use: as an apparently grassroots hub for promoting administrative action instead of challenging it. More generally, sites that allow citizens to complain to their governments are not unusual and also may benefit regimes in other ways too such as highlighting grassroots conflicts, which may demobilize citizens who otherwise may have been more active on an issue (*85*).

Lower-level government actors may also attempt to channel dissent by providing official complaint venues (Table 1, cell 7). For instance, there was widescale adoption of these platforms in China by 2006: 100% of provincial governments, 93% of city governments, and 69% of counties had official portals (*86*). Interestingly, at the local level, while this may channel dissent into approved forums, threats of broader protest and/or threats to reveal lower-level government failures to higher officials can lead to local responsiveness (*87*). That said, lower-level Chinese officials are often effective at limiting the flow of grassroots grievances to higher officials (*88*).

Private actors can also channel contention and in similar ways to states (Table 1, cell 11). For instance, social media teams are commonly used to respond to negative content online. Company-run

complaint forums can shield grievances more effectively from public view, but online complaint forums run by other companies likely surface more discontent than they channel (*89*, *90*). Companies also use internal discussion and complaint forums to control internal contestation through actual or apparent employee voice (*91*). Organizations may have broad social media policies for employees that discourage controversial speech on social media and/or vet job candidates using material harvested from candidates' social media posts, disadvantaging candidates with specific political beliefs (*92*). Interestingly, this is the least researched cell in Table 1 by repression researchers, but business scholarship readily advises companies on how to craft policies and practices that mitigate business risks through channeling (*89*–*92*).

Unlike overt channeling, which is usually clearly and directly connected to taming contentious voices, covert channeling involves overbroad incentives or controls that affect contention but go so far beyond that the effects on contention may be obscured for casual observers. For instance, at the nation-state level (Table 1, cell 4), Russia's RuNet was designed to protect cyber infrastructure and Russian values (*93*) and is surrounded by a legal framework that has developed over the last decade purportedly to protect children and the Russian way of life more broadly by promoting a "Clean Internet" (*94*). While touted as for the well-being of Russians, restrictions limit dissent alongside many other kinds of online information and activity. Turkey has adopted laws to reduce "immoral" online activity (*95*), but journalists and scholars argue that these laws also limit online dissent. China outlawed public disparagement of national heroes, which extends even to local government functionaries such as firemen (*96*). Indian officials have a track record of using anti-defamation, among other laws, to limit free speech online (*97*).

In each case, if the explicit and clear target of these laws was controlling dissent, then the laws would be properly classified as overt coercion. However, given that they regulate a large amount of speech and conduct online, only a subset of which is protest-related, these overbroad laws fall within covert channeling. Although some may see this as a distinction without a difference, it is important to note that dissent is not the sole or explicit target of these laws, although most of these governments have elsewhere specifically focused on repressing dissent. Instead, online dissent is a subcomponent of a larger class of antistate speech and action that the regime is interested in controlling. This both obscures specific attacks on dissent and evinces a much broader government interest in controlling online activity and speech.

Overt, carrot-based channeling also comes in the form of social credit systems. China, for instance, aspires to create a national-level social credit system to incentivize pro-government speech and action. This goes far beyond merely discouraging dissent, with some arguing that it is even more focused on regulating economic activity (*98*). Social credit systems in China also offer broad incentives for what the regime defines as prosocial and broad disincentives for what the regime labels antisocial.

Lower levels of government may also create social credit systems (Table 1, cell 8). Although China aspires to a nationwide system, there is currently only a patchwork of local, regional, and private social credit systems, which enjoy unexpected levels of public approval (*99*). While social credit systems are relatively new, lower state authorities have long been able to complete their administrative duties in ways that move potential dissidents, including those who use social media to promote their causes, toward other forms of expression or away from political expression together. For instance, Pan (*100*) shows how a social assistance program in China that is ostensibly designed as a social welfare program is administered by local officials to reduce contention through channeling.

Private actors can independently engage in channeling and support state-directed channeling. Platform community standards (e.g., Facebook and Twitter's community standards) shape online dissent, including dictating which tactics and causes are scrubbed from platforms (*101*). For instance, some movements distribute graphic videos of what they oppose (e.g., factory farming and regime violence), but platforms may remove this material as offensive (*102*). Moreover, while social media companies such as Facebook and Google have billed themselves in the United States as only selling ad space, research shows that they are much more active in shaping campaign communications than previously known (*103*). This opens up the possibility that these companies are offering more intensive services to other actors who may want to influence online discourse and/or political dissent as well.

Private social media platforms can also support state channeling efforts. For instance, private social credit systems such as Ant Financial's Sesame Credit reward consumers for economic and social relationships and behavior, and they legitimize social credit systems more generally (*104*). It is also often easier for a country to control domestic social media companies (e.g., to encourage content filtering and/or proregime platform policies), offering governments more leverage than they would enjoy with international firms (*105*).

CONTROLLING AND CHANNELING INFORMATION

Thus far, we have shown that a tremendous amount of digital repression can be understood through traditional repressive processes. There are elements of digital repression, though, that look like traditional forms of control, such as censorship and state-media systems, but influence action in ways that are substantively different from traditional repressive processes when scaled up using digital tools. Although not considered by Earl's typology (*19*), a large literature on authoritarian politics shows the centrality of information control and propaganda for authoritarian rule (*106*–*111*). Authoritarian, and sometimes democratic (*112*), governments have sought to control conventional media, including through censorship (*113*, *114*), state-based media systems (*115*, *116*), the synergy between censorship and state media (*117*, *118*), and cooperation with (or pressure on) private media producers (*119*, *120*). The traditional literature on social movement repression did not emphasize these efforts because of perceptions that such strategies were too diffuse and untargeted to be specific to protest (*15*) and only relevant to authoritarian governments.

With the pervasive use of digital and social media, the control of information is now an indispensable component of any modern typology of repression. In this section, we expand the typology shown in Table 1 by mapping strategies to control information (e.g., censorship) and channel information (e.g., disinformation campaigns) through the introduction of Table 2. While information control in the digital era builds on predigital trajectories, leading some scholars to see great continuity between predigital and digital censorship (*11*), we see evidence that digital technologies have changed the aims and scope of information control. Traditional censorship focused on suppressing knowledge (e.g., banning books and controlling media

Table 2. Digital repression expanding on traditional processes.

	Information control			
	Information coercion (i.e., controlling information by limiting access or content)		Information channeling (i.e., influencing production and consumption of information)	
	Overt	Covert	Overt	Covert
State agents tightly coupled with national political officials	Limited national Internet connectivity (e.g., North Korea), temporary Internet blackouts, and state-based content filtering	National content filtering where that filtering is not clear to users (e.g., returning 404 errors for filtered material)	Government accounts posting distracting information and/or flooding online spaces or hashtags with irrelevant material	Government disinformation and/or misrepresentations that influence contention
	-1-	-2-	-3-	-4-
State agents loosely connected with national political officials	Regional Internet blackouts and/or content filtering	Regional content filtering where that filtering is not clear to users	Local government or police information posting distracting information and/or flooding online spaces or hashtags with irrelevant material	Local government and/or police disinformation and/or misrepresentations that influence contention
	-5-	-6-	-7-	-8-
Private agents	Deplatforming activists or organizations and/or moderating activist or organizational content	Down-ranking, search filtering, shadow banning, throttling the spread of, or otherwise making protest-related material more obscure	Private actors posting distracting information and/or flooding online spaces or hashtags with irrelevant material	Private disinformation and/or misrepresentations that influence contention
	-9-	-10-	-11-	-12-

ownership), which influenced contention by preventing unfavorable information from circulating and allowing powerholders to construct "reality." Digital censorship certainly does all of this, but it also suppresses individual expression—the ability of individuals to speak to each other and to be seen by others—which has direct implications for coordination and mobilization. Because organizing often uses digital tools, online information control can now also directly disrupt movement coordination and mobilization efforts. Put differently, whereas traditional propaganda and state media systems had to rely exclusively on changing beliefs, information control and channeling strategies now also directly affect behavior as well as perceptions of the information environment.

Preventing access and controlling content

Some repressive actors have adopted strategies and tactics that attempt to control access to information. Restrictions on access to digital information are often clear and overt (Table 2, cell 1), as is the case with Internet shutdowns (*121*, *122*). In their 2011 article, Howard *et al.* (*123*) report 606 incidents in 99 countries since 1995 (39% of these occurred in democratic countries). Internet shutdowns have also occurred in Pakistan (*124*), during one-third of the elections in Sub-Saharan Africa (*125*), in Iran after the 2009 elections (*123*), and in Syria during its civil war (*62*). One of the most prominent examples of a state using Internet shutdowns to quash dissent was Hosni Mubarak cutting off Internet and cellphone access during the 2011 Egyptian uprising. However, these blackouts were slowly implemented and had the opposite effect on dissent (*126*). Similarly, the Syrian government organized the "Syrian Electronic Army" to attack the Web-based infrastructure of dissidents in the diaspora as a part of their transnational repression efforts (*35*). Other less severe forms of overt control may include banning tools like Tor and Psiphon that allow users to circumvent online surveillance through remote virtual private networks (VPNs) (*60*).

Substate actors are also able to use overt forms of information control to suppress dissent (Table 2, cell 5). India had 134 localized shutdowns in 2018, more than anywhere else in the world (*122*). In the United States, Bay Area Rapid Transit shut down cell service to disrupt protests that erupted in response to a police shooting (*127*).

Private corporations' role in overt information control is complex (Table 2, cell 9). Corporations may independently decide to remove posts and information and do so for a variety of reasons, including to generate profit, to buttress lobbying efforts, and/or to conform to their platforms' standards. For example, social media sites such as Facebook and Twitter have deplatformed activists (*101*) and stifled posting abilities for Palestinian activists (*101*), anarchist groups (*128*), and, perhaps less controversially, racist groups (*129*).

Corporate actions may also be compelled, whether through state ownership structures, domestic laws, or orders to private telecom companies, to restrict specific topics or cut access to citizens (*2*, *3*, *130*, *131*). For instance, the Chinese government issues censorship directives to Internet, print, television, and other media services such as gaming and instant messaging services (*61*, *132*–*138*), censoring approximately 13% of all social media posts on Chinese sites (*139*). This also occurs in Belarus, Uganda, and the Congo (*26*, *125*). Censorship in China is driven more by a post's capacity to stir collective action than otherwise offensive content (*132*). While these posts are deleted by private companies, what is removed is influenced by the government. Democratic governments have also pressured private digital media companies. For instance, U.S.-based

Craigslist (acquiescing to government pressure) placed a black bar reading "censored" over the adult services section of its website (*140*), and the United States pressured a variety of companies to cut services to WikiLeaks (*141*).

State control of information can also be covert, taking the form of less-detectable censorship, denial of service attacks, filtering, and slowing access to information from specific sources (Table 2, cell 2). Because these interventions are focused on infrastructure, users' online experiences feel unconstrained, leaving some unaware that specific content was restricted. For instance, Iran installed deep packet inspection systems that substantially slowed traffic after the 2009 elections sparked widespread protests (*123*) and developed a "national Internet" as a part of its efforts to minimize the potential influence of external threats from countries like the United States (*142*). Syria used spear-phishing attacks to gather data on dissidents abroad and potentially discredit them (*35*). Jordan hacked nongovernmental organization websites and shut down activist Facebook pages (*56*). In Kazakhstan, the government used selective filtering to limit access to political websites and posts while increasing the availability of nonpolitical media (*29*, *143*). China's "Great Firewall" is similar, blocking objectionable websites from IP addresses within the country while surveilling tracking requests (*61*, *133*, *144*).

Distributed denial-of-service (DDoS) attacks are an additional form of covert information control used by state actors. DDoS attacks are coordinated, distributed efforts intended to interrupt online communication (*144*, *145*). While the inability to access an entire website may be very noticeable, it is often difficult to determine why a site is inaccessible, let alone who is responsible, leading us to label DDoS attacks as covert. Earlier research found that DDoS attacks were more common when domestic education levels, nonviolent dissent, and rates of other forms of repression were higher (*145*). More recent work finds that nondemocratic countries target foreign states that host servers for domestic news websites with denial-of-service (DoS) attacks, especially around elections (*146*).

Although less commonly studied, local and regional governments also have the capacity to covertly control information (Table 2, cell 6). In Russia, local government officials insisted that the Russian social media site Vkontakte blocks events, groups, and pages related to an ongoing series of protests (*147*). These activists were also subject to a range of other digital interruptions and hacks. Regional variation is best documented in China where local authorities and organizations can control digital filtering decisions, resulting in a complex network of local and national institutions producing considerable heterogeneity in information filtering across China (*148*).

Private companies can also use covert methods of information control (Table 2, cell 10). In the United States, debates over net neutrality have focused on ISPs' ability to restrict access to specific webpages and the potential for a tiered Internet (*140*). Algorithms can be adjusted to slow the spread of protest-related information or filter it entirely. Platforms may also "shadow ban" users, which limits (or blocks) the visibility of some users' posts without their knowledge (*149*). Content management systems like Drupal even have packages to manage shadow banning (*150*). More often, private companies work in collaboration with the state to restrict access to websites and covertly collect information saved on private servers. For example, the Russian government requires telecommunications companies to share copies of electronic communication with local security officials [a process referred to as "SORM-compliance"; (*60*, *63*)]. Similarly, states may encourage search engine companies to down-rank (i.e., making a result appear later instead of on the first page of search results) or filter out results for politically sensitive searches (*151*, *152*). Recent reporting on China finds that Apple often precensors websites and information for Chinese users to pre-empt Chinese takedown requests (*153*).

Information channeling

Digital and social media have brought new opportunities for offensive influence-based forms of repression. This is a form of channeling, but as applied to information and attention. Here, repressors make paying attention to preferred information more accessible or attractive (*61*), analogous to the carrots that incentivize preferred behavior in traditional channeling. Repressors may also shape the overall information environment, analogous to the broader laws and practices that changed the context for protest-related decisions and behaviors in traditional channeling. For example, the information environment is altered by injecting a particular viewpoint, changing the topic, or making a particular viewpoint appear to have widespread support.

Unlike traditional propaganda, however, which seeks first and foremost to change attitudes, opinions, and beliefs, information channeling aims to influence behavior. Information channeling can prevent people from finding or even encountering information related to issues they would otherwise have supported and activities such as a protest that they otherwise would have joined. Beliefs and so-called second-order beliefs (i.e., beliefs about what others believe) may be influenced downstream, but indoctrination is not the primary objective of information channeling.

Information channeling operates differently from the defensive, access-based form of digital repression discussed in the prior section because it is not about limiting or removing access but, rather, redirecting or otherwise influencing attention. Long-time researchers of digital censorship label this "active engagement," positioning it as a preferred option for many in power because it is often easier to distract from content or overwhelm with other information than to ensure no one has technical access to information or posts (*2*, *60*).

In terms of specific forms, overt, informational channeling strategies by regimes (Table 2, cell 3) occur when state actors produce information to redirect public attention and/or obscure social movement information, as occurred during the 2014 anti-Maduro protests. At the height of these protests, the Venezuelan regime mobilized proregime National Assembly members to tweet to move online conversations away from the protest's narrative concerning failures of the government on economy and crime (*116*). Politicians were acting at the regime's behest rather than for the sake of advancing their power as politicians, making this an example of national-level channeling. In Kazakhstan, in addition to blocking some potentially political blogs and websites, state-owned service providers fill social networks with "lowbrow" nonpolitical sports personalities, celebrities, and pop stars whose accounts are managed by state-run media companies (*29*). In the Gulf countries and Saudi Arabia, governments mass-produce online content with automated "bot" accounts to drown out critics (*154*).

Information channeling strategies are also accessible to lower officials (Table 2, cell 7). In China, for instance, information channeling is primarily implemented by city- and county-level governments, such as when local government social media accounts flood online spaces with nonpolitical, highly positive content before periods where there is a heightened risk of collective action (*61*, *155*).

The leak of Democratic National Committee–hacked emails by WikiLeaks is an example of overt information channeling strategy performed by a private actor (Table 2, cell 11), although it occurred as part of the Russian state–organized campaign to influence the 2016 U.S. election. Mainstream media reported widely on the leak, which captured a great deal of attention on social media, showing how information channeling can, through the production of a specific type of information, reshape the broader information ecosystem. Whether acting of their own accord or contracted by state actors, private agents also engage in overt information channeling. They do so by flooding online spaces and activist hashtags with spam or other irrelevant content to derail social movement organizing and make such protest-related content more difficult to find (*156*).

Covert information channeling campaigns occur when disinformation is disseminated to influence conversations and/or when the real identity of a source is obfuscated or misrepresented, whether or not the information shared is accurate. These campaigns can redirect attention; change beliefs, expression, and/or behaviors; and influence what people believe about the opinions and actions of others (i.e., second-order beliefs). Importantly, whether an information channeling strategy is covert does not rest on the success of, but rather the attempt at, deception.

National-level, covert information channeling (Table 2, cell 4) is one of the few forms of repression where foreign state actors intervene to influence other countries' domestic politics (*157*). This, for instance, occurred when Russian state–sponsored influence campaigns used coordinated troll and bot accounts, disguised as American citizens and organizations, to post false information about social movements such as Black Lives Matter, in hopes of increasing polarization and sowing conflict (*158*–*162*). The Russian government is also suspected of carrying out covert information channeling campaigns domestically, hacking, and leaking information to discredit opposition figure Alexei Navalny (*163*). But democracies have also used this strategy against domestic threats. In 2012, agents of the South Korean National Intelligence Service posted hundreds of thousands of Twitter messages from hundreds of accounts made to look like those of ordinary citizens. These messages drew attention away from negative news, denigrated the opposition, and raised divisive issues (*164*). Also, among other examples (*156*), so-called "Peñabots" in Mexico promote trends and spread false information in hopes of distracting or diminishing interest in government criticism (*165*).

Another prominent example of covert information channeling that local governments carry out (Table 2, cell 8) is China's so-called 50-Cent Army. Thousands of county-level propaganda departments around China fabricate social media content as if it were the opinions of ordinary people to respond to and pre-empt social mobilization (*132*). These fabricated accounts generate cheerleading content entirely unrelated to the protests, and they are meant to redirect attention away from social mobilization.

As with overt information channeling, private agents are also integral to the covert information channeling ecosystem (Table 2, cell 12). Repressors benefit from a marketplace of bots, trolls, click farms, and digital influencers available to support online distraction and influence campaigns for profit (*166*). Countermovements may also attempt to diminish their opponents by using covert information channeling (*156*), as several right-wing and racist movements in the United States have done in spreading disinformation about their opponents (*167*–*169*).

EMERGENT QUESTIONS AND POTENTIAL RELATIONSHIPS

Beyond making it easier to understand and organize what is otherwise a welter of research on digital repression, Tables 1 and 2 together create a coherent typology that allows researchers to ask new questions. In this section, we suggest several questions and potential relationships that were not yet fully articulated in the literature but which become more obvious with this typology in play.

First, a casual review of the academic literature on digital repression offers a tour of autocracies, but our review questions this strong authoritarian gaze. Although autocrats certainly draw on many forms of digital repression, our review clearly shows that democracies engage in almost all forms of digital repression too. Moreover, the use of digital repression by autocracies does not suggest on its own that the availability of the Internet has changed the power asymmetries between a state and its citizens. While researchers may expect that state openness will continue to be relevant for explaining when states are willing to respond with coercion and surveillance to online speech and behavior (Table 1), and also how overtly information control is deployed and how regularly information channeling (Table 2) is deployed, this is not the full story or limited to autocracies. Likewise, some see democratic uses of digital repression as evidence that authoritarian practices are spreading to non-autocracies (*75*), but democracies and anocracies have long histories of repressive action (*170*, *171*). Indeed, in the next section, we suggest that digital repression researchers exploit variation between autocracies and across democracies, anocracies, and autocracies to understand the extent to which classic or new explanations of repression hold.

Second, bringing findings from the traditional study of repression into the study of digital repression enables examination of whether digital repression represents the continuation of existing dynamics or new dynamics ushered in by digital life. In other words, this typology facilitates more refined questions about what is new or unique about digital repression. For instance, although we suspect that deterrence, selective incapacitation, and other well-known repressive processes are behind the effects of forms of digital repression Table 1, the information channeling forms of repression that we introduced in Table 2 may be both uniquely digital (at least at scale) and also uniquely corrosive to democracies because they do not feel like repression to many who experience them; nonetheless, they constrain activists and social mobilization. Without a refined language like this typology with which to identify these nuances, their excavation may be needlessly delayed or forestalled.

Third, this typology and the distribution of research across its cells make plain that private repressors are critical actors. Put bluntly, repression researchers need to be paying far more attention to the role of private actors in repression and to the complex relationships that private repressors have with regimes. While this was needed before the rise of digital repression too (*40*), it is ever more important today. This is true partly because of the volume of contention that takes place on private platforms today, but also because there are so few major platforms (*101*), making their power consolidated and harder to route around. More research on private repression is also important because its determinants are so varied. We reviewed research documenting independent private repression, but we also reviewed research on the collaboration of private and public actors. While at times this involved regimes essentially forcing private actors to repress, it also involved willing collaboration in which private actors commodified repression by selling or managing repressive efforts for state actors (*31*), funneled repression into the

lobbying efforts (*101*), and/or built repression into their business models (*104*). Moreover, the form of this collaboration likely depends on regime and market characteristics (*105*), making it important to ask under what conditions different forms of public-private repressive partnerships will exist and/or thrive.

While many have studied the involvement of private actors, more explicit theorization about similarities and differences is needed. It may be that private repression shifts the terrain for repression in truly important ways. For example, in the United States, protesters enjoy legal protections for speech and assembly, but only in some types of public spaces and never on private property. Because the servers that major platforms and websites reside on are private property, protesters do not enjoy free speech and assembly rights while on them (*101*). This means that online there is no legally protected genuine public (as in government-owned) space for free speech and assembly. This looks more like an autocratic, than democratic, regime except that the control of public discussion is held by private companies, not governments.

We also argue that this typology helps to breathe specificity into a long-standing debate over whether digital tools are generally bad for social movements by introducing more nuanced and analyzable potential relationships, such as: What types of repression have digital and social media created? Do particular types of digital repression augment or replace traditional repressive capacities? Do digital tools afford states access to repressive capacities they were previously lacking because regimes lacked physical control over their territory but have more control over cyberspace? Moreover, different relationships likely exist for different types of digital repression and under different circumstances. For instance, it may be that digital and social media created capacity where repressive potential was previously weak. Alternatively, it may be that digital repression augmented already existing capacities. In either case, there is variation to be parsed.

There are also likely important relationships between different forms of digital repression. For instance, it is likely that some combinations of digital repression are complementary and generate greater impact when combined. While it has likely always been the case that regimes aspired to feed surveillance into overt coercive repression programs, research makes it clear that the scale and/or seamlessness of that coupling may have expanded as many states now funnel digital surveillance into the targeting of their overt coercion (*58*, *62*, *172*). The ability to pinpoint these combinations is important for both research and policy. Substitution effects may exist where forms of digital repression are used in lieu of traditional repression (*26*) or between different forms of digital repression, as when information channeling supplants information control strategies at the nation-state level (*2*, *60*). That all of these options are possible and have been observed suggests the urgent need to begin to ask more nuanced questions, such as under which conditions do different combinations or substitutions become more likely. It also lays bare the limits of generic claims about rising undifferentiated repressiveness popular in some quarters. Only by beginning to focus on more specific interrelationships between different forms of repression can scholars understand the conditions and consequences of these relationships and support successful prevention or amelioration strategies.

EXPLAINING DIGITAL REPRESSION

Our typology of digital repression not only enables researchers to recognize relationships between types of digital coercion and control as well as to ask different and more nuanced questions about digital repression but also to determine the political, economic, and social factors that influence when and where specific forms of digital repression will be adopted (e.g., factors that drive, for example, digitally enabled physical coercion may not matter for information channeling). While it is likely that there are important continuities between the factors that drive traditional and digital repression, we expect that new considerations—particularly technological capacity—will be important for understanding the dynamics of digital repression.

For instance, the proliferation of the Internet and digital infrastructure is likely important to explaining digital repression. It is difficult for countries to completely disconnect from the global Internet because it is vital for maintaining ties with the global economy (*173*) and it is hard to lock down because it is an important source of entertainment and information (*77*). This may discourage nations dependent on global trade from using some overt information control strategies like Internet shutdowns but encourage the use of overt coercion against digital activists (*11*).

States must also consider an array of technological concerns in selecting forms of repression. For example, Internet and broadband penetration makes information more available, the wider availability of smartphones makes communication and organization easier, and the proliferation of secure servers and VPNs makes opportunities to evade censorship and bypass barriers to information more accessible (*24*, *61*, *174*). As a result, the Internet, smartphones, and VPNs are likely to motivate different forms of digital repression. The speed and availability of the Internet may drive overt coercion and information coercion (*62*), while smartphone proliferation may lead to more digital surveillance and overt information coercion efforts to hinder connections. Roberts (*61*) argues that the availability of secure servers and VPNs will produce more overt and covert information channeling as governments and private agents try to "flood the zone" with information.

A regime's digital repressive infrastructure likely also matters immensely for where, how, and how much of different forms of digital repression are deployed. Governments have had decades to develop the coercive and surveillance infrastructure necessary for traditional repression. Developing similar digital tools takes time and expertise (*2*, *42*). While many regimes already have military and police available to carry out traditional repression and some forms of digital repression from Table 1, other forms of digital repression require digital infrastructure and thus the development of state infrastructure. As a result, some forms of digital repression (particularly forms of covert information coercion, see Table 2, cell 2) may be unavailable or operate at rudimentary levels until the regime's technological infrastructure reaches particular thresholds (*24*). More overt forms of information channeling (Table 2, cell 3) may also be less feasible, but these actions are also more readily outsourced to private firms.

Alternatively, the private sphere may allow some governments to leapfrog these infrastructural impediments by outsourcing the development of more refined tools for surveillance, control, and channeling. Indeed, the increased role of private actors may change states' capacity for digital repression (*105*). As a result, this may lead to more information coercion and channeling because of increased capacity and deniability. If states do not choose to collaborate with private sources, they may opt for the less infrastructurally intensive techniques of information channeling than infrastructural control.

Importantly, though, we do not believe that the explanation of digital repression is all new. Over 50 years of research on repression

shows that the major predictor of most forms of repression is the extent to which a movement or group is a threat (*5*, *19*, *175*). Governments often perceive protest and other civil conflicts as threats to order and stability and respond with repression. This phenomenon is referred to as "the law of coercive responsiveness" (*5*). Yet, this "law" also acknowledges that not all movements are seen as equally threatening. For instance, governments tend to repress larger movements more than smaller movements because they see them as a bigger threat. Governments also tend to see movements calling for radical systemic change as more threatening than movements with assimilationist goals.

Threat will likely continue to motivate digital repression. Moreover, existing research on threat as a predictor of traditional repression points out that it is not the objective level of threats like movement size, but the repressors' perception of threats, that leads to repression (*176*), particularly when movements have a source of power that regimes do not feel they control as solidly. We expect that what constitutes a threat may be shifting, and such shifts will affect the severity and/or forms of digital repression deployed. For example, Iran sees the Internet as a "digital battleground" and uses perceived external threats from democracy promotion, international cyberattacks, and state sanctions to justify the establishment of a national Internet that censors (i.e., Table 2, cell 2) international sources and information (*142*). The Chinese government and media companies are more likely to censor messaging that calls for collective action than actions that critique the state, presumably because they are more threatening (*132*). Regimes may also respond to calls for collective action that are in English or come from diaspora communities with information channeling while using either overt coercion or information coercion when similar calls are made in the country's dominant language and/or emerge domestically since these may be seen as more threatening.

Existing research on digital repression already shows the impact of threat perceptions on digital repression. Work on Syria and DDoS attacks find that states responded to protest with shutdowns, surveillance, and physical coercion (*121*, *145*). Other work finds that digital repression has allowed states to respond to (or even preempt) protests, identify key dissidents, and deter diffusion faster than ever before (*26*). But, as Gohdes (*62*) finds, states alternately opted for suppression, surveillance, or channeling depending on the inciting (i.e., threatening) action and the broader context. We should expect that threats will increase the likelihood of digital repression, but contextually dependent factors—such as the duration, severity, and groups responsible for the threats—will influence which forms the government adopts (and in what combinations). Long-standing conflicts will lead to the build-up of multiple forms of digital repression, whereas governments will respond to sudden large events with more overt physical coercion. Future research systematically tying variation in digital repression to threat levels is important to establish whether this "law of coercive response" continues to operate in digital spaces and if it is a general feature or limited to particularly digital forms.

Other factors known from decades of research on repression, such as the structure of political opportunities (*177*, *178*) and/or the weakness of challengers (*5*, *19*, *175*), may also affect digital repression. We should expect that autocratic regimes will be more willing to use all forms of digital repression than democracies, but, of the forms discussed here, democracies will be more likely to use tactics such as digital and information channeling (cells 3 and 4 in Tables 1 and 2). Democracies may gravitate toward traditional channeling (Table 1, cells 3 and 4) and information channeling (Table 2, cells 3 and 4) because they allow them to influence public opinion and protest without the appearance of directly intervening. But digital tools for repression may make it easier to target "weak challengers" for intimidation and surveillance. As a result, "old" explanations for repression may find new uses as the state's repressive tools grow, making it imperative that researchers who are studying digital repression integrate the useful guidance from existing research on traditional repression.

Likewise, social norms and demographics may shape how and how frequently states and private actors use digital repression. Prior research has found that the openness of legal institutions helps to predict traditional repression (*179*). While, as noted above, these may still matter, recent work suggests that broader measures of civil society—namely, freedom of association—may be more important for explaining digital repression (*26*). Indeed, states with more freedom of association and stronger civil society networks may be less likely to use digitally related physical coercion or overt information control (i.e., shutdowns) but more willing to use distraction and disinformation (i.e., Table 2, cells 3 and 4) to direct attention away from discussions and topics that may spur dissent.

While demographics have been considered relevant to dissent and repression for a long time, states and private actors may be more mindful of the demographics of their citizens and digital users. College-educated individuals have comparatively more technological skills and are more committed to seeking information outside of approved channels. Roberts (*61*) finds that 75% of Chinese citizens who evade the firewall are in college or have a college degree. Similarly, research on DDoS attacks finds that these were more prominent in states with higher proportions of college-educated individuals (*145*). But more comparative research is necessary to establish whether this relationship between higher proportions of college-educated individuals and information channeling (Table 2, cell 3) or covert forms of digital repression (Tables 1 and 2, cells 2 and 4) are robust. Relatedly, states with larger-than-average cohorts of young people (i.e., youth bulges) have been comparatively more repressive (*180*). These states may also use more online repression, particularly these same distraction and disinformation techniques to pre-empt the collective action potential of these potentially more digitally adept citizens.

CONSEQUENCES OF DIGITAL REPRESSION

The widespread use of digital repression by national political actors and agents under their direct control or supervision has led to substantial public concern based on a common, but incorrect, assumption that deterrence almost always follows from coercion (*181*). Indeed, decades of research show that although much is known about what explains repression, there is very little consensus about the consequences of repression (*15*). Virtually every conceivable relationship has been found—from deterrence, to backfire/backlash, to curvilinear relationships with deterrence or backfire, to time dependence, to effects on tactical choices but not mobilization levels.

If the traditional literature on repression is any guide, scholars can use this typology to theorize about how consequences may depend, in part, on the type of repression. For instance, some specific forms of repression may have different probabilities of deterrence versus backfire. Traditionally, overt coercion is more likely to backfire when used against nonviolent protesters (*182*), which may also

hold for digital activists. Timing can also influence when/whether backfire occurs: Weidmann and Rod (*26*) argue that Internet penetration and associated digital surveillance and repression have negative effects on protest emergence but can help sustain protests once they start. This mirrors findings on the consequences of traditional repression, which also suggest that effects vary depending on the timing of repression (*183*).

Likewise, some have argued that when information control strategies are used, this may draw other digitally active individuals and groups into protest (*141*, *184*), representing a backfire effect. This conforms with existing research, which has found that highly visible, sudden instances of information coercion often backfire (*185*). Hassanpour (*126*) suggests that Egypt's Internet shutdown during the Arab Spring resulted in backlash and pushed more people to take to the streets. Hobbs and Roberts show how China's highly visible ban of Instagram led users to install and use circumvention technologies (*186*). This not only enabled them to use Instagram but it also provided them with a gateway to access political information banned in China. The thinking is that because highly visible forms of information coercion can generate anger, backlash is often more likely than deterrence.

However, some research demonstrates that timing may complicate these effects. Rydzak (*122*) shows that maintaining Internet shutdowns beyond a week is associated with lower rates of protest as digital communication and means of coordination are disrupted. Over a much longer period, the deterrence effects may be even more pronounced. Chen and Yang show that Chinese college students, who have grown up with filtered Internet, have very little demand for access to uncensored Internet because of a lack of knowledge of the value of inaccessible information (*187*). They do not develop a demand for such information until they realize what they are missing, which only occurs if they are incentivized to consume censored information). Hyun and Kim (*188*) show that online political expression in China helps to build state legitimacy and nationalism.

In contrast, and without respect to timing, covert strategies as well as information channeling, which do not have a performative aspect, are often found to have a deterrence effect if their purposes are not revealed and they effectively redirect behavior attention (*61*). In other words, the strategies of digital repression delineated by the typology (as represented by the vertical columns of Tables 1 and 2) differ in their visibility and durability, which, in turn, may influence responses to repression. Hypotheses like these show that this typology can be used to tether digital repression to the broader, although sometimes conflicted, literature on consequences of traditional repression, and motivate nuanced questions about how different aspects of digital repression—what form is used (including who carries it out) and who is affected—may shape the probabilities of different consequences.

It is also essential to consider repression's effects not only on activists but also on the broader audience of bystanders, who may be sympathetic to a cause but who have not become part of one. Activism has moved to online spaces because of the ease of communication and coordination they afford, but activists have also come to these spaces because that is where audiences are reachable. Pan and Siegel show how arrests of prominent Saudi activists demobilize the activists themselves but do not deter their online supporters (*27*). Instead, online supporters sympathetic to the repressed activists become more critical of the Saudi regime. Backfire is also observed when people not targeted by repression believe government repression to be unjust and join a cause they otherwise would have been uninvolved in (*62*, *63*, *141*, *184*). In other words, even as repression may deter activists and core members of a cause, it may backfire by activating and mobilizing new supporters. Whether consequences consistently differ by group across the typology or differences are seen within the typology remains an open research question.

Another important implication from the typology is that the consequences of repression also vary depending on who is carrying it out (i.e., the rows in Tables 1 and 2). In particular, many experiencing repression do not conceive of the actions taken by private actors as repression, even when they have the same effects of deterrence as actions taken by the state actors. Traditionally, the state has been associated with repression because physical coercion was seen as integral to repression and the state monopolized coercive capabilities. As seen in the typology, the state does not in fact have a monopoly on strategies such as information coercion or information channeling. Private actors such as social media platforms play an increasingly large role in digital repression because they control the spaces and infrastructure on which digital activism is taking place. Adler (*140*) argues that private censorship harms marginalized groups and tends to have a more wide-reaching impact than government censorship alone.

The involvement of private actors in digital repression has far-reaching consequences for activism and social mobilization. It is one thing to recognize the consequences of private social media platforms deciding that certain groups cannot post certain types of content, but it is another thing altogether to recognize the consequence of the lack of legally protected spaces online (*101*). As activism moves online where all spaces are private spaces, democracies become much more similar to autocracies when it comes to freedom of expression and assembly because neither democracies nor autocracies protect freedom of expression and assembly in private online spaces where activists and protesters are mobilizing.

Last, the consequences of digital repression may be broad-ranging, including far more than just deterrence or backfire and those wider consequences may also differ across the typology. For instance, some forms of digital repression may diminish movement capacity. Social movement scholars have shown how government coercion that precedes a protest can undermine the institutional capacity of social movements in ways that are much more effective than crackdowns on protest, which often backfire (*183*). Agent provocateurs can reduce trust and harm movements (*189*). Information channeling strategies, especially covert strategies such as disinformation campaigns where repressors mimic activists, work similarly to damage trust among activists and undermine the institutional capacity of movement organizations to function effectively. Similarly, some forms of digital repression may also erode civil society. The literature on repression in autocracies shows the many ways in which repression hollows out civil society (*26*). Covert information channeling may be doing the same in democracies. By enflaming existing social tensions and introducing mistrust of democratic institutions, disinformation campaigns diminish the base of civil society from which movements can mobilize (*169*).

To summarize, we argue that the use of the typology we introduced would deepen research on the consequences of digital repression in at least five ways, by suggesting (i) different types of consequences for different types of repression, (ii) different consequences over time across different types of repression, (iii) different

actors affected by different types of repression, (iv) differences in impact based on who perpetrates repression (i.e., by row of the typology), and (v) differences in broader consequences of repression based on the type of repression.

CONCLUSION

The literature on digital repression, which extends a decades-old interest in how state and private actors try to control and constrain protest and social movements, is spread across so many disciplines and research traditions that it is increasingly entropic, making it a challenge to build on substantial existing research on repression dynamics. This limited connection to scholarship on repression that predates the Internet makes it difficult to discern areas of consensus, conflict, and underdevelopment, and to grasp fully how the forms, causes, and consequences of digital repression differ from that which predated the Internet. In addition to being bad for science, this has also been bad for policy as it has allowed overly simplistic assumptions about the effectiveness of repression to influence public and policy conversations (*181*).

In this review, we have taken an important step toward reversing these trends by adapting a well-known typology of repression for use in the digital age. Our typology uses a classic typology of repression to show that the 12 types of repression it identified (*19*) are still relevant. We used that typology to discuss types of digital repression that affect protest through well-known processes (see Table 1). We also discussed forms of digital repression that are unique to the digital age, at least in their scale and the processes through which they are expected to affect protest (see Table 2). We have organized a substantial volume of research, making it evident which forms of digital repression have been studied and what is known about each.

Further, we have shown that this typology helps to challenge potentially problematic latent expectations. For instance, some parts of the literature imply that digital repression is explained by autocracy; however, this view is inaccurate when the larger vista of research is visible and organized. Likewise, many digital pessimists argue that the Internet is a net loss for social movements because of repression, but this assumes a consensus in research on the impacts of repression that does not, and indeed has never, existed. Instead, there are far more complicated dynamics where states and private actors of all sorts engage in different forms of repression, likely differently explained by a mix of old and new predictors. Those actions sometimes deter, sometimes backfire, and sometimes have other effects.

The typology and the literature it organizes also make clear that there are pressing questions, including those regarding the role and impact of private actors in repression as well as relationships between different forms of repression. While private actors have long played a role in repression (*40*), their independent prominence in digital repression and their role in supplying the infrastructure for state repression both require deeper theorizing and research. Likewise, it is important that scholars begin to recognize synergistic, substitution, or time-ordered relationships between different types of digital repression. These may lead to advances in our collective ability to explain digital repression. For example, increased covert coercion by national authorities through surveillance may increase subsequent overt coercion by either local or national authorities who act based on that intelligence. This may also aid in our understanding of the consequences of repression (e.g., some forms of repression may be more associated with backfire than deterrence).

It is likely that, without some tether between extant scholarship on traditional repression and recent research on digital repression like this typology, important insights will be deferred and delayed. For instance, although not discussed in this review, scholars of digital media may struggle with the idea that both (ultra)liberal and (ultra)conservative activists and movements can be repressed. For many, repression is what happens to the groups you favor, whereas lawful governance is what affects groups you dislike. The repression literature shows, however, that repression happens to both, although not necessarily in equal measure, using the same forms, or to the same ends. For example, in the United States, white supremacists have been repressed but often only to discourage violence not to defeat their movement (*190*). In contrast, progressive groups have been repressed with the goal of ending or severely constraining the movements (*191*). Also, different tactics were used against each type of group (*192*). Early signs are that digital repression by both national and local governments are following these trends, but without a tie to this existing body of scholarship, it would be hard to see these connections or think through the difference between digital governance and digital repression.

REFERENCES AND NOTES

1. N. Caren, K. T. Andrews, T. Lu, Contemporary social movements in a hybrid media environment. *Annu. Rev. Sociol.* **46**, 443–465 (2020).
2. R. Deibert, J. Palfrey, R. Rohozinski, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press, 2010).
3. R. J. Deibert, J. Palfrey, R. Rohonzinski, J. L. Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT, 2008).
4. C. Tilly, *From Mobilization to Revolution* (Addison-Wesley Publishing Company, 1978).
5. C. Davenport, State repression and political order. *Annu. Rev. Polit. Sci.* **10**, 1–23 (2007).
6. S. Feldstein, Ed., *Issues on the Frontlines of Technology and Politics* (Carnegie Endowment for International Peace, 2021).
7. M. Josua, M. Edel, The Arab uprisings and the return of repression. *MediterraneanPolit.* **26**, 586–611 (2021).
8. A. Kendall-Taylor, E. Frantz, J. Wright, The digital dictators: How technology strengthens autocracy, in *Foreign Affairs* (2020), pp. 103.
9. R. Gorwa, What is platform governance? *Commun. Soc.* **22**, 854–871 (2019).
10. N. P. Suzor, *Lawless: The Secret Rules That Govern our Digital Lives* (Cambridge Univ. Press, 2019).
11. S. Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford Univ. Press, 2021).
12. C. Tenove, Networking justice: Digitally-enabled engagement in transitional justice by the Syrian diaspora. *Ethn. Racial Stud.* **42**, 1950–1969 (2019).
13. N. Al-Jizawi, S. Anstis, S. Barnett, S. Chan, A. Senft, R. Deibert, *Digital Transnational Repression* (2020 November 6); https://citizenlab.ca/2020/11/annotated-bibliography-transnational-digital-repression/.
14. J. Earl, Technology and social media, in *The Wiley Blackwell Companion to Social Movements*, D. A. Snow, S. A. Soule, H. Kriesi, H. J. McCammon, Eds. (Wiley Blackwell, ed. 2, 2018), pp. 289–305.
15. J. Earl, Political repression: Iron fists, velvet gloves, and diffuse control. *Annu. Rev. Sociol.* **37**, 261–284 (2011).
16. J. Earl, Protest arrests and future protest participation: The 2004 republican national convention arrestees and the effects of repression. *Studies Law Polit. Soc.* **45**, 141–173 (2011).
17. S. C. Poe, C. N. Tate, L. C. Keith, Repression of the human right to personal integrity revisited: A global cross-national study covering the years 1976-1993. *Int. Stud. Quart.* **43**, 291–313 (1999).
18. J. Gaventa, *Power and Powerlessness: Quiescence and Rebellion in an Appalachian Valley* (University of Illinois Press, 1980).
19. J. Earl, Tanks, tear gas and taxes: Toward a theory of movement repression. *Sociol Theory* **21**, 44–68 (2003).
20. C. J. Jenkins, C. M. Eckhert, Channeling black insurgency: Elite Patronage and professional social movement organizations in the development of the black movement. *Am. Sociol. Rev.* **51**, 812–829 (1986).
21. J. D. McCarthy, D. W. Britt, M. Wolfson, The Institutional channeling of social movements by the state in the United States. *Res. Soc. Move. Conflicts Change* **13**, 45–76 (1991).

22. L. H. Ong, "Thugs-for-Hire": Subcontracting of state coercion and state capacity in China. *Perspect. Polit.* **16**, 680–695 (2018).
23. J. Boykoff, Limiting dissent: The mechanisms of state repression in the USA. *Soc. Move. Stud.* **6**, 281–310 (2007).
24. E. Keremoğlu, N. B. Weidmann, How dictators control the internet: A review essay. *Comp. Pol. Stud.* **53**, 1690–1703 (2020).
25. D. L. Cingranelli, D. L. Richards, The Cingranelli and Richards (CIRI) human rights data project. *Hum. Rights Q.* **32**, 401–424 (2010).
26. N. B. Weidmann, E. G. Rød, *The Internet and Political Protest in Autocracies* (Oxford Univ. Press, 2019).
27. J. Pan, A. A. Siegel, How Saudi crackdowns fail to silence online dissent. *Am. Polit. Sci. Rev.* **114**, 109–125 (2020).
28. Human Rights Watch. *Azerbaijan* (2021); https://hrw.org/europe/central-asia/azerbaijan [cited 2021 June 15].
29. L. Anceschi, The persistence of media control under consolidated authoritarianism: Containing Kazakhstan's digital media. *Demokratizatsiya* **23**, 277–295 (2015).
30. M. Lynch, After Egypt: The limits and promise of online challenges to the authoritarian Arab State. *Perspect. Polit.* **9**, 301–310 (2011).
31. C. Fuchs, Societal and ideological impacts of deep packet inspection internet surveillance. *Inf. Commun. Soc.* **16**, 1328–1359 (2013).
32. K. E. Pearce, A. Hajizada, No laughing matter humor as a means of dissent in the digital era: The case of authoritarian Azerbaijan. *Demokratizatsiya* **22**, 67–85 (2014).
33. M. Michaelsen, *The Digital Transnational Repression Toolkit, and Its Silencing Effects* (Freedom House, 2020).
34. D. M. Moss, Transnational repression, diaspora mobilization, and the case of the Arab spring. *Soc. Probl.* **63**, 480–498 (2016).
35. D. M. Moss, The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora. *Globalizations* **15**, 265–282 (2018).
36. L. Dencik, A. Hintz, Z. Carey, Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. *New Media Soc.* **20**, 1433–1450 (2018).
37. J. Earl, H. McKee Hurwitz, A. Mejia Mesinas, M. Tolan, A. Arlotti, This protest will be tweeted: Twitter and protest policing during the Pittsburgh G20. *Inf. Commun. Soc.* **16**, 459–478 (2013).
38. J. P. Walsh, C. O'Connor, Social media and policing: A review of recent research. *Sociol. Compass* **13**, e12648 (2019).
39. J. Earl, A. Schussman, Cease and desist: Repression, strategic voting and the 2000 U.S. presidential election. *Mobilization* **9**, 181–202 (2004).
40. J. Earl, Controlling protest: New directions for research on the social control of protest. *Res. Soc. Move. Conflicts Change* **25**, 55–83 (2004).
41. S. Sobieraj, *Credible Threat: Attacks Against Women Online and the Future of Democracy* (Oxford Univ. Press, 2020).
42. S. Scott, *Fake Geek Girls: Fandom, Gender, and the Convergence Culture Industry* (New York Univ. Press, 2019).
43. A. Massanari, #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Med. Soc.* **19**, 329–346 (2017).
44. M. E. Miller, Google takes down maps made by Thai right-wingers targeting free speech activists, in *Washington Post* (2021).
45. J. L. Beyer, *Expect Us: Online Communities and Political Mobilization* (Oxford Univ. Press, 2014).
46. D. Gilbert, Anonymous is now doxxing Q-Anon supporters: "We gonna wreck you", in *Vice* (2018).
47. M. H. Peckham, New Dimensions of social movement/countermovement interaction: The case of scientology and its internet critics. *Can. J. Soc.* **23**, 317–347 (1998).
48. R. J. Deibert, *Reset: Reclaiming The Internet For Civil Society* (House of Anansi, 2020).
49. S. Kargar, A. Rauchfleisch, State-aligned trolling in Iran and the double-edged affordances of Instagram. *New Media Soc.* **21**, 1506–1527 (2019).
50. H. Beaumont, Revealed: Pipeline company paid Minnesota police for arresting and surveilling protesters, in *The Guardian* (2021).
51. R. Klemko, A small group of sleuths had been identifying right-wing extremists long before the attack on the Capitol, in *Washington Post* (Washington, D.C., 2021).
52. R. Deibert, J. Palfrey, R. Rohozinski, J. L. Zittrain, *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (MIT Press, 2011).
53. S. Anstis, S. Chan, A. Senft, R. Deibert, *Annotated Bibliography Dual-Use Technologies* (2019 September 5); https://citizenlab.ca/2019/09/annotated-bibliography-dual-use-technologies-network-traffic-management-and-device-intrusion-for-targeted-monitoring/.
54. J. Penney, S. Mckune, L. Gill, R. J. Deibert, Advancing human-rights-by-design in the dual-use technology industry. *J. Int. Affairs* **71**, 103–110 (2018).
55. S. Hankey, D. Ó. Clunaigh, Rethinking risk and security of human rights defenders in the digital age. *J. Human Rights Prac.* **5**, 535–547 (2013).
56. D. M. Moss, Repression, response, and contained escalation under "Liberalized" authoritarianism in Jordan. *Mobilization* **19**, 261–286 (2014).
57. B. Qin, D. Strömberg, Y. Wu, Why does China allow freer social media? Protests versus surveillance and propaganda. *J. Econ. Perspect.* **31**, 117–140 (2017).
58. X. Xu, To Repress or to Co-opt? Authoritarian control in the age of digital surveillance. *Am. J. Polit. Sci.* **65**, 309–325 (2021).
59. S. Gunitsky, Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspect. Polit.* **13**, 42–54 (2015).
60. R. Deibert, Cyberspace under siege. *J. Democracy* **26**, 64–78 (2015).
61. M. E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton Univ. Press, 2018).
62. A. R. Gohdes, Repression technology: Internet accessibility and state violence. *Am. J. Polit. Sci.* **64**, 488–503 (2020).
63. J. A. Kerr, Information, security, and authoritarian stability: Internet policy diffusion and coordination in the former Soviet Region. *Int. J. Commun.* **12**, **21**, (2018).
64. E. Snowden, *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'* (The Guardian, 2013).
65. B. Gellman, A. Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, in *Washington Post* (Washington, D.C., 2013).
66. J. Menn, Spy agency ducks questions about 'back doors' in tech products, in *Reuters* (2020).
67. S. Owen, Monitoring social media and protest movements: Ensuring political order through surveillance and surveillance discourse. *Soc. Ident.* **23**, 688–700 (2017).
68. G. Borradaile, B. Burkhardt, A. LeClerc, Whose tweets are surveilled for the police: An audit of a social-media monitoring tool via log files, in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Barcelona, Spain, Association for Computing Machinery, 27th-30th January 2020), pp. 570–580.
69. American Civil Liberties Union, *Stingray Tracking Devices: Who's Got Them?* (2018); https://aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them [cited 2021 June 20].
70. C. Izant, *Stingray Surveillance: Legal Rules by Statute or Subsumption?* (Harvard National Security Journal, 2016).
71. J. Earl, D. Cunningham, *See No Evil, Hear No Evil, Police No Evil* (Lawfare Blog, 2021).
72. K. E. Pearce, Democratizing kompromat: The affordances of social media for state-sponsored harassment. *Inf. Commun. Soc.* **18**, 1158–1174 (2015).
73. J. Scott-Railton, A. Hulccop, B. A. Razzak, B. Marczak, S. Anstis, R. Deibert, *Dark Basin: Uncovering a Massive Hack-For-Hire Operation* (University fo Toronto, 2020).
74. T. Maurer, *Cyber Mercenaries* (Cambridge Univ. Press, 2018).
75. R. Deibert, The road to digital unfreedom: Three painful truths about social media. *J. Democracy* **30**, 25–39 (2019).
76. S. Zuboff, Big other: Surveillance capitalism and the prospects of an information civilization. *J. Inform. Technol.* **30**, 75–89 (2015).
77. E. Zuckerman, Cute cats to the rescue? Participatory media and political expression, in *From Voice to Influence: Understanding Citizenship in a Digital Age*, A. Danielle, S. L. Jennifer, Eds. (University of Chicago Press, 2015), pp. 129-154.
78. R. J. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (McClelland & Stewart, 2013).
79. J. E. Bromwich, D.Victor, M. Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says* (New York Times, 2016).
80. B. Marczak, J. Scott-Railton, s. McKune, B. A. Razzak, R. Deibert, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab Research Report No. 113 (University of Toronto, 2018).
81. Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus* (Amnesty International, 2021).
82. S. Feldstein, *The Global Expansion of AI Surveillance* (Carnegie Endowment for International Peace, 2019).
83. M. Marquis-Boire, B. Marczak, C. Guarnieri, J. Scott-Railton, *For Their Eyes Only: The Commercialization of Digital Spying* (Citizen Lab at the University of Toronto, 2013).
84. J. Scott-Railton, B. Marczak, C. Guarnieri, M. Crete-Nishihata, *Bitter Sweet Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links* (Citizen Lab, Univ. of Toronto, 2017).
85. J. Chen, Y. Xu, Why do authoritarian regimes allow citizens to voice opinions publicly? *J. Polit.* **79**, 792–803 (2017).
86. M. Jiang, H. Xu, Exploring online structures on chinese government portals: Citizen political participation and government legitimation. *Soc. Sci. Comp. Rev.* **27**, 174–195 (2009).
87. J. Chen, J. Pan, Y. Xu, Sources of authoritarian responsiveness: A field experiment in China. *Am. J. Polit. Sci.* **60**, 383–400 (2016).
88. J. Pan, K. Chen, Concealing corruption: How Chinese officials distort upward reporting of online grievances. *Am. Polit. Sci. Rev.* **112**, 602–620 (2018).
89. J. L. Stevens, B. I. Spaid, M. Breazeale, C. L. Esmark Jones, Timeliness, transparency, and trust: A framework for managing online customer complaints. *Bus. Horiz.* **61**, 375–384 (2018).

90. G. A. Gorry, R. A. Westbrook, Winning the internet confidence game. *Corp. Reput. Rev.* **12**, 195–203 (2009).
91. P. K. Mowbray, A. Wilkinson, H. H. M. Tse, Strategic or silencing? Line Managers' repurposing of employee voice mechanisms for high performance. *British J. Manage.* 10.1111/1467-8551.12469 (2021).
92. J. Field, J. Chelliah, Social-media misuse a ticking time-bomb for employers. *Human Resource Manage. Int. Digest* **20**, 36–38 (2012).
93. M. Ristolainen, J. Kukkola, Chapter 3 - Closed, safe and secure – the Russian sense of information security, in *Emerging Cyber Threats and Cognitive Vulnerabilities*, V. Benson and J. McAlaney, Es. (Academic Press, 2020), pp. 53–71.
94. M. Kravchenko, Russian anti-extremism legislation and internet censorship. *The Soviet Post-Soviet Rev.* **46**, 158–186 (2019).
95. D. Butler, A. Kucukgocmen, *Turkey Approves Social Media Law Critics Say Will Silence Dissent* (Reuters, 2020).
96. Reuters, *China Makes First Use Of Law Banning Defamation Of National Heroes* (Reuters, 2018).
97. Human Rights Watch. *How India's Archaic Laws Have A Chilling Effect On Dissent* (2016 May 24); https://hrw.org/news/2016/05/24/how-indias-archaic-laws-have-chilling-effect-dissent.
98. F. Liang, V. Das, N. Kostyuk, M. M. Hussain, Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy Internet* **10**, 415–453 (2018).
99. G. Kostka, China's social credit systems and public opinion: Explaining high levels of approval. *New Media Soc.* **21**, 1565–1593 (2019).
100. J. Pan, *Welfare for Autocrats: How Social Assistance in China Cares for Its Rulers* (Oxford Univ. Press, Incorporated, 2020).
101. J. Earl, Private Protest? *Inf. Commun. Soc.* **15**, 591–608 (2012).
102. W. L. Youmans, J. C. York, Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *J. Commun.* **62**, 315–329 (2012).
103. D. Kreiss, S. C. McGregor, Technology firms shape political communication: The work of Microsoft, Facebook, Twitter, and Google with campaigns during the 2016 U.S. Presidential Cycle. *Polit. Commun.* **35**, 155–177 (2018).
104. G. P. L. Chong, Cashless China: Securitization of everyday life through Alipay's social credit system—Sesame Credit. *Chinese J. Commun.* **12**, 290–307 (2019).
105. J. Pan, How market dynamics of domestic and foreign social media firms shape strategies of internet censorship. *Problems of Post-Communism* **64**, 167–188 (2017).
106. R. Wintrobe, *The Political Economy Of Dictatorship* (Cambridge Univ. Press, 2000).
107. L. Blaydes, *State of Repression* (Princeton Univ. Press, 2018).
108. M. W. Svolik, *The Politics Of Authoritarian Rule* (Cambridge Univ. Press, 2012).
109. M. K. Dimitrov, J. Sassoon, State security, information, and repression: A comparison of communist Bulgaria and Ba'thist Iraq. *J. Cold War Stud.* **16**, 3–31 (2014).
110. M. K. Dimitrov, Internal government assessments of the quality of governance in China. *Stud. Comparative Int. Dev.* **50**, 50–72 (2015).
111. H. Romerstein, Disinformation as a KGB Weapon in the Cold War. *J. Intell. Hist.* **1**, 54–67 (2001).
112. E. Pontikes, G. Negro, H. Rao, Stained Red: A study of stigma by association to blacklisted artists during the "Red Scare" in Hollywood, 1945 to 1960. *Am. Sociol. Rev.* **75**, 456–478 (2010).
113. C. Gläßel, K. Paula, Sometimes less is more: Censorship, news falsification, and disapproval in 1989 East Germany. *Am. J. Polit. Sci.* **64**, 682–698 (2020).
114. P. Lorentzen, China's strategic censorship. *Am. J. Polit. Sci.* **58**, 402–414 (2014).
115. Y. Zhao, Understanding China's media system in a world historical context, in *Comparing Media Systems Beyond the Western World*, D. C. Hallin and P. Mancini, Eds. (Cambridge Univ. Press, 2012), pp. 143–176.
116. K. Munger, R. Bonneau, J. Nagler, J. A. Tucker, Elites tweet to get feet off the streets: Measuring regime social media strategies during protest. *Polit. Sci. Res. Methods* **7**, 815–834 (2019).
117. M. Adena, R. Enikolopov, M. Petrova, V. Santarosa, E. Zhuravskaya, Radio and the rise of the Nazis in Prewar Germany. *Quart. J. Econ.* **130**, 1885–1939 (2015).
118. B. Qin, D. Strömberg, Y. Wu, Media bias in China. *Am. Econ. Rev.* **108**, 2442–2476 (2018).
119. D. Stockmann, M. E. Gallagher, Remote control: How the media sustain authoritarian rule in China. *Comp. Pol. Stud.* **44**, 436–467 (2011).
120. J. Mcmillan, P. Zoido, How to subvert democracy: Montesinos in Peru. *J. Econ. Perspect.* **18**, 69–92 (2004).
121. A. R. Gohdes, Pulling the plug: Network disruptions and violence in civil conflict. *J. Peace Res.* **52**, 352–367 (2015).
122. J. A. Rydzak, A total eclipse of the net: The dynamics of network shutdowns and collective action responses, in *School of Government and Public Policy* (University of Arizona, 2018).
123. P. N. Howard, S. D. Agarwal, M. M. Hussain, The dictators' digital dilemma: When do states disconnect their digital networks?, in *Issues in Technology Innovation* (The Center for Technology Innovation at Brookings, 2011).
124. B. Wagner, Authoritarian practices in the digital age: Understanding internet shutdowns: A case study from Pakistan. *Int. J. Commun.* **12**, 22 (2018).
125. T. Freyburg, L. Garbe, Authoritarian practices in the digital age: Blocking the bottleneck: Internet shutdowns and ownership at election times in Sub-Saharan Africa. *Int. J. Commun.* **12**, 21 (2018).
126. N. Hassanpour, Media disruption and revolutionary unrest: Evidence from Mubarak's quasi-experiment. *Polit. Commun.* **31**, 1–24 (2014).
127. M. Cabanatuan, *Bart Admits Halting Cell Service To Stop Protests* (SFGate, 2011).
128. T. Riski, *In Purge of Extremists, Facebook Removes Page of Portland Protest Organizers* (Willamette Week, 2020).
129. S. Ingber, *Facebook Bans White Nationalism And Separatism Content From Its Platforms* (NPR, 2019).
130. S. Kalathil, T. C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Brookings Institution Press, 2010).
131. N. B. Weidmann, A closer look at reporting bias in conflict event data. *Am. J. Polit. Sci.* **60**, 206–218 (2016).
132. G. King, J. Pan, M. E. Roberts, How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *Am. Polit. Sci. Rev.* **111**, 484–501 (2017).
133. R. Clayton, S. J. Murdoch, R. N. M. Watson, *Ignoring the Great Firewall of China* (Springer Berlin Heidelberg, 2006).
134. J. Knockel, C. Parson, L. Ruan, R. Xiong, J. Crandall, R. Deibert, *We Chat, They Watch How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus* (Citizen Lab, 2020).
135. J. Knckek, L. Ruan, M. Crete-Nishihata, Measuring decentralization of chinese keyword censorship via mobile games, in *7th USENIX Workshop on Free and Open Communications on the Internet (FOCI 17)* (USENIX Association, 2017).
136. J. Knockel, R. Xiong, *(Can't) Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats* (The Citizen Lab, Toronto, 2019).
137. J. Knockel, L. Ruan, M. Crete-Nishihata, *Keyword Censorship in Chinese Mobile Games* (The Citizen Lab, Toronto, 2017).
138. M. Kenyon, *An Analysis Of Censorship In Chinese Open Source Projects* (The Citizen Lab, Toronto, 2018).
139. G. King, J. Pan, M. Roberts, How censorship in China allows government criticism but silences collective expression. *Am. Polit. Sci. Rev.* **107**, 326–343 (2013).
140. J. Adler, The public's burden in a digital age: Pressures on intermediaries and the privatization of internet censorship. *J. Law Policy* **20**, (2011).
141. J. Earl, J. L. Beyer, The dynamics of backlash online: Anonymous and the Battle for WikiLeaks. *Res. Soc. Move. Conflicts Change* **37**, 207–233 (2014).
142. M. Michaelsen, Authoritarian practices in the digital age: Transforming threats to power: The international politics of authoritarian internet control in Iran. *Int. J. Commun.* **12**, 21 (2018).
143. J. D. Ronald, The geopolitics of internet control, in *Routledge Handbook of Internet Politics* (Routledge, 2008).
144. B. Marczak, N. Weaver. J. Dalek, R. Ensafi, D. Fifield, S. McKune, A. Rey, J. Scott-Railton, R. Deibert, V. Paxson, *China's Great Cannon* (Citizen Lab, 2015).
145. V. Asal, J. Mauslein, A. Murdie, J. Young, K. Cousins, C. Bronk, Repression, education, and politically motivated cyberattacks. *J. Global Sec. Stud.* **1**, 235–247 (2016).
146. P. M. Lutscher, N. B. Weidmann, M. E. Roberts, M. Jonker, A. King, A. Dainotti, At home and abroad: The use of denial-of-service attacks during elections in nondemocratic regimes. *J. Confl. Resolut.* **64**, 373–401 (2020).
147. P. Perrine, Social media and state repression: The case of VKontakte and the anti-garbage protest in Shies, in Far Northern Russia. *First Monday* **26**, 10.5210/fm.v26i5.11711 (2021).
148. G. Yang, Social dynamics in the evolution of China's internet content control regime, in *Routledge Handbook of Media Law* (Routledge, 2012).
149. C. Shu, *Reddit Replaces Its Confusing Shadowban System With Account Suspensions* (2015 November 11); https://techcrunch.com/2015/11/11/reddit-account-suspensions/.
150. Bastlynn, *Shadowban* (2015); https://drupal.org/project/shadowban.
151. N. Villeneuve, *Search Monitor Project: Toward a Measure of Transparency* (Citizen Lab, Toronto, 2008).
152. M. Jiang, The business and politics of search engines: A comparative study of Baidu and Google's search results of Internet events in China. *New Media Soc.* **16**, 212–233 (2014).
153. J. Nicas, R. Zhong, D. Wakabayashi, *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China* (New York Times, 2021).
154. A. Leber, A. Abrahams, A storm of tweets: Social media manipulation during the gulf crisis. *Rev. Middle East Stud.* **53**, 241–258 (2019).
155. Y. Lu, J. Pan, Capturing Clicks: How the Chinese government uses clickbait to compete for visibility. *Polit. Commun.* **38**, 23–54 (2021).
156. J. Earl, R. James, E. Ramo, S. Scovill, Protest, activism, and false information, in *The Routledge Companion to Media Disinformation and Populism*, H. Tumber, S. Waisbord, Eds. (Taylor & Francis Group, 2021), pp. 290-301.

157. M. Alizadeh, J. N. Shapiro, C. Buntain, J. A. Tucker, Content-based features predict social media influence operations. *Sci. Adv.* **6**, eabb5824 (2020).
158. R. DiResta, K. Shaffer, B. Ruppel, D. Sullivan, R. Matney, R. Fox, J. Albright, B. Johnson, *The Tactics & Tropes of the Internet Research Agency* (United States Senate Select Committee on Intelligence: Washington, D.C., 2018).
159. A. Arif, L. G. Stewart, K. Starbird, Acting the part: Examining information operations within #blacklivesmatter discourse. *Proc. ACM Hum. Comput. Interact.* **2**, 1–27 (2018).
160. Y. M. Kim, J. Hsu, D. Neiman, C. Kou, L. Bankston, S. Y. Kim, R. Heinrich, R. Baragwanath, G. Raskutti, The Stealth Media? Groups and targets behind divisive issue campaigns on facebook. *Polit. Commun.* **35**, 515–541 (2018).
161. C. A. Bail, B. Guay, E. Maloney, A. Combs, D. S. Hillygus, F. Merhout, D. Freelon, A. Volfovsky, Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017. *Proc. Natl. Acad. Sci.* **117**, 243–250 (2020).
162. A. Badawy, E. Ferrara, K. Lerman, Analyzing the digital traces of political manipulation: The 2016 Russian Interference Twitter Campaign, in *Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (Barcelona, Spain, IEEE, 28th-31st August 2018).
163. A. Hulcoop, J. Scott-Railton, P. Tanchak, M. Brooks, R. Deibert, *Tainted Leaks: Disinformation And Phishing With A Russian Nexus* (Citizen Lab, 2017).
164. F. B. Keller, D. Schoch, S. Stier, J. H. Yang, Political astroturfing on twitter: How to coordinate a disinformation campaign. *Polit. Commun.* **37**, 256–280 (2020).
165. E. Treré, The dark side of digital politics: understanding the algorithmic manufacturing of consent and the hindering of online dissidence. *IDS Bulletin* **41**, 127–138 (2016).
166. J. C. Ong, J. V. A. Cabañes, When Disinformation studies meets production studies: Social identities and moral justifications in the political trolling industry. *Int. J. Commun.* **13**, 20 (2019).
167. R. Lewis, A. Marwick, Taking the red pill: Ideological motivations for spreading online disinformation, in *Understanding and Addressing the Disinformation Ecosystem* (Annenberg School for Communication: University of Pennsylvania, 2017), pp. 18–22.
168. Y. Benkler, R. Faris, H. Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford Univ. Press, 2018), pp. 462.
169. Z. Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (Yale Univ. Press, 2017).
170. C. Davenport, D. A. Armstrong, Democracy and the violation of human rights: A statistical analysis from 1976 to 1996. *Am. J. Polit. Sci.* **48**, 538–554 (2004).
171. C. Davenport, *State Repression and the Domestic Democratic Peace* (Cambridge Univ. Press, 2007).
172. E. Frantz, A. Kendall-Taylor, J. Wright, *Digital Repression in Autocracies* (The Varieties Of Democracy Institute, 2020).
173. R. E. Litan, A. M. Rivlin, Projecting the economic impact of the internet. *Am. Econ. Rev.* **91**, 313–317 (2001).
174. J. Rydzak, M. Karanja, N. Opiyo, Internet Shutdowns in Africa: Dissent does not die in darkness: Network shutdowns and collective action in African countries. *Int. J. Commun.* **14**, 24 (2020).
175. C. Davenport, Multi-dimensional threat perception and state repression: An inquiry into why states apply negative sanctions. *Am. J. Polit. Sci.* **39**, 683–713 (1995).
176. V. Boudreau, Precarious regimes and matchup problems in the explanation of repressive policy, in *Repression and Mobilization*, C. Davenport, H. Johnston, C. Mueller, Eds. (University of Minnesota Press, 2005), pp. 33–57.
177. D. McAdam, *Political Process and the Development of Black Insurgency, 1930-1970* (University of Chicago Press, 1982).
178. D. della Porta, Social movements and the state: Thoughts on the policing of protest, in *Comparative Perspectives on Social Movements*, D. McAdam, J. D. McCarthy, M. N. Zald, Eds. (Cambridge Univ. Press, 1996), pp. 62–92.
179. D. W. Hill, Z. M. Jones, An empirical evaluation of explanations for state repression. *Am. Polit. Sci. Rev.* **108**, 661–687 (2014).
180. R. Nordås, C. Davenport, Fight the Youth: Youth bulges and state repression. *Am. J. Polit. Sci.* **57**, 926–940 (2013).
181. E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs, 2011).
182. E. Chenoweth, M. J. Stephan, *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict* (Columbia Univ. Press, 2011).
183. R. Koopmans, Dynamics of repression and mobilization: The German extreme right in the 1990s. *Mobilization* **2**, 149–164 (1997).
184. J. L. Beyer, J. Earl, Backfire Online: Studying reactions to the repression of internet activism, in *The Paradox of Repression and Nonviolent Movements*, L. R. Kurtz, L. A. Smithey, Eds. (Syracuse Univ. Press, 2018), pp. 102-142.
185. M. E. Roberts, Resilience to online censorship. *Annu. Rev. Polit. Sci.* **23**, 401–419 (2020).
186. W. R. Hobbs, M. E. Roberts, How sudden censorship can increase access to information. *Am. Polit. Sci. Rev.* **112**, 621–636 (2018).
187. Y. Chen, D. Y. Yang, The impact of media censorship: 1984 or Brave new world? *Am. Econ. Rev.* **109**, 2294–2332 (2019).
188. K. D. Hyun, J. Kim, The role of new media in sustaining the status quo: Online political expression, nationalism, and system support in China. *Inf. Commun. Soc.* **18**, 766–781 (2015).
189. G. T. Marx, Thoughts on a neglected category of social movement participant: The Agent Provocateur and the Informant. *Am. J. Sociol.* **80**, 402–442 (1974).
190. D. Cunningham, Understanding state responses to left- versus right-wing threats. *Soc. Sci. Hist.* **27**, 327–370 (2003).
191. D. Cunningham, *There's Something Happening Here: The New Left, the Klan, and FBI Counterintelligence* (University of California Press, 2004).
192. D. Cunningham, The patterning of repression: FBI counterintelligence and the new left. *Soc. Forces* **82**, 209–240 (2003).

Acknowledgments

Funding: J.E., T.V.M., and J.P. received no funding in support of this research. **Author contributions:** J.E. took the lead in organizing this collaboration. All other authors contributed equally to writing and revising this article. **Competing interests:** J.E. and T.V.M. declare that they have no competing interests. J.P. declares that she has received honoraria from Meta for participating in Facebook News Integrity Expert Circle workshops. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials.

Submitted 17 August 2021
Accepted 18 January 2022
Published 9 March 2022
10.1126/sciadv.abl8198