2

Domestic Digital Repression and Cyber Peace

Jessica Steinberg, Cyanne E. Loyle, and Federica Carugati

INTRODUCTION

The Chinese government has reportedly detained over a million Muslims in the northwestern region of Xinjiang (Maizland, 2019). The detainees, predominantly of the Uighur ethnic group, are being held in reeducation camps where they are forced to pledge loyalty to the Communist Party of China, renounce Islam, and learn Mandarin (Maizland, 2019). Officials in China purport that these camps are not only used for vocational training, but also cite the need to quell the influence of violent extremism in the Xinjiang population (Maizland, 2019). There are reports of prison-like conditions in these camps, including extensive surveillance, torture (Wen & Auyezov, 2018), and even forced sterilization (Associated Press, 2020). The Uighur population is also under extensive surveillance outside of these detention facilities. Alleged monitoring has included location surveillance through messaging apps such as WeChat, facial recognition technology used at police checkpoints, as well as biometric monitoring (Cockerell, 2019). These technologies are being used by the Communist Party as new digital tools for monitoring and controlling populations deemed threatening to the Chinese state.

Modern digital information and telecommunication technologies (ICTs) have changed the ways in which states and their citizens interact on a variety of fronts, including the provision of goods and services and the production of information and misinformation. As the case of the Uighur population in China suggests, ICTs have also changed the ways in which states address threats from their population. While these kinds of overt, blatant abuses carried out by authoritarian states against ethnic or religious minorities tend to capture much attention, the use of digital technologies for repression is by no means limited to authoritarian states (Dragu & Lupu, 2020). New technologies are shifting the ways in which all states, democratic as well as authoritarian, repress.

While improvements in technology have often been associated with liberation, digital technologies in the hands of governments willing to repress can be a major threat to respect for human rights and freedoms worldwide and, as such, they are

https://doi.org/10.1017/9781108954341.002 Published online by Cambridge University Press

a danger to cyber peace. As defined in the Introduction to this volume, a *positive* cyber peace necessitates respect for human rights and freedoms and the spread of Internet access. These characteristics are threatened by domestic digital repression, which often includes intentionally limiting access to the Internet and cellular communications, and can both constitute and facilitate violations of human rights and freedoms. Our chapter focuses on the changing nature of repression through digital technologies as a risk to cyber peace. Differing from other contributions to this volume (see Chenou & Aranzales, Chapter 5), we explore the domestic side of the interaction between digital technologies and cyber peace. Digital technologies are transforming repression, but we still know very little about this transformation and its long-term impact on state behavior. We believe, however, that understanding the ways in which these technologies are reshaping state power and its relationship to its citizens is necessary to build a more peaceful and freer digital *and* analog world.

In this chapter, we provide a conceptual map of the ways in which ICTs impact state repression. This mapping exercise seeks to identify some initial sites of influence in order to further theorize and empirically evaluate the effects of ICTs on our current understandings of state repression. We begin by outlining a conceptual definition of digital repression informed by the extant literature on state repression. We then derive four constituent components of state repression and trace the impact of ICTs on each of our four components.[1] In conclusion, we discuss how our findings may inform or upend existing theories in the study of state repressive behavior.

1 REPRESSION AND DIGITAL REPRESSION

State repression refers to the actual or threatened use of physical violence against an individual or organization within a state for the purpose of imposing costs on the target and deterring specific activities believed or perceived to be threatening to the government (Goldstein, 1978, p. xxvii). Traditional modes of repression have been conceptualized based on their impact on the physical integrity of groups or individuals, or as restrictions on individual or group civil liberties. Physical integrity violations refer to violations of a person's physical being such as enforced disappearances, torture, or extrajudicial killings. Civil liberties violations include restrictions on press freedoms and information, and freedoms of association, movement, or religious practice.

All states repress, albeit in different ways and for different reasons (Davenport, 2007). Most scholars of state repression view the decision to repress as a rational calculus taken by political authorities when the costs of repression are weighed against its potential benefits (e.g., Dahl, 1966; Goldstein, 1978; Davenport, 2005). When

[1] We note here, but only in passing, that for both authoritarian and democratic governments, the relations with private ICT companies further complicate the strategic calculus. We address this issue below.

https://doi.org/10.1017/9781108954341.002 Published online by Cambridge University Press

the benefits of repression outweigh the costs, then states are likely to repress. The expected benefits of using repression are "the elimination of the threat confronted and the increased chance of political survival for leaders, policies, and existing political-economic relations" (Davenport, 2005, p. 122). In addition, repression may demonstrate strength and deter subsequent threats. Traditional costs of repression, on the other end of the equation, include logistical and monetary costs, as well as potential political costs. The literature on the dissent–repression nexus suggests that while repression may neutralize a threat in the short term, it has the potential to yield to more dissent in the longer term because of a backlash effect to state policies (Rasler, 1996; Koopmans, 1997; Moore, 1998; Carey, 2006). Democratic leaders who use particularly violent forms of repression may be penalized by voters (Davenport, 2005). Furthermore, leaders may suffer external political costs; for example, the international community may sanction leaders for excessive use of force against their civilian populations, or for behaviors that violate international human rights norms (Nielsen, 2013).

The advent of modern digital technologies has ushered in new forms of *digital* repression. Digital repression is the "coercive use of information and communication technologies by the state to exert control over potential and existing challenges and challengers" (Shackelford et al., in this volume, Introduction). Digital repression includes a range of tactics through which states use digital technologies to monitor and restrict the actions of their citizens. These tactics include, but are not limited to, digital surveillance, advanced biometric monitoring, misinformation campaigns, and state-based hacking (Feldstein, 2019). Modes of digital repression map onto the two modes of traditional repression mentioned above, physical integrity and civil liberties violations. Digital repression, while not directly a physical integrity violation, can facilitate or lead to such types of violations. For example, the data gathered by the Chinese state about the Uighur population has aided the government in locating and physically detaining large numbers of Uighurs. Digital repression can constitute both a civil liberties violation in and of itself, and facilitate the violation of civil liberties. For example, by limiting individual access to information and communication, the state violates the rights of citizens to access information. Alternatively, by closely monitoring the digital communications of social movements, states can deter or more easily break up political gatherings and protests. While states regularly gather and rely upon information about their citizens to conduct the work of governing, *digital repression* entails the use of that information for coercive control over individuals or groups that the state perceives as threatening.

As with traditional forms of repression, the use of digital repression can be seen in terms of a cost–benefit calculus on the part of the state. Yet, in the case of digital repression, this calculus is not well understood. Digital technologies impact the ways in which states identify and respond to threats, as well as the resources needed to do so. New technologies also impact the ways in which challengers, citizens, and the international community will experience and respond to the state's behavior,

in turn affecting the costs and benefits of using digital repressive strategies. For example, the costs of digitally monitoring social movement participation through social media may have large upstart costs in terms of infrastructure and expertise. Yet, those initial costs may be offset over future threats. In certain circumstances, digital repression may reduce audience costs associated with traditional forms of repression[2] as these newer forms of repressive behavior may be easier to disguise. Alternatively, if digital repression is hidden from the public, it may be less likely to deter future threats, as challengers may not fully understand the levels of risk involved in challenging the state. In sum, it is likely that digital repression is shifting the cost–benefit analysis of state repression. However, we have yet to adequately theorize how this analysis might differ from, and relate to, a cost–benefit analysis of the use of traditional state repression.

Before we map how ICTs are reshaping state repression, we first place some scope conditions on the set of technologies that are relevant for our inquiry. Within the last decade, scholars have begun to develop frameworks and explore empirical patterns related to digital repression in a still nascent literature.[3] This work has examined a wide range of technologies, strategies, and platforms, including Internet outages (Howard et al., 2011), social media use (Gohdes, 2015), and surveillance technologies (Qiang, 2019). Building on this work, we focus on the technological developments that facilitate two kinds of activities: (1) access to new and potentially diverse sources of information and (2) near instantaneous communication among individual users. While neither of these activities is a fundamentally new use of technology, the volume of information available, the number of individuals that can access and communicate information, and the speed at which exchanges can occur are new. Therefore, we are interested in ICTs that combine cellular technology, the Internet and its infrastructure, the software and algorithms that allow for large-scale data processing, and the devices that facilitate access to the Internet (e.g., computers and smart phones).[4]

As Shackelford and Kastelic (2015) detail, as states have sought to protect critical national infrastructure from cyber threats, they have pursued more comprehensive state-centric strategies for governing the Internet. This has led to the creation of national agencies and organizations whose purpose is to monitor communication and gather data and information about foreign as well as domestic ICT users. This is true for both democracies and autocracies. But whereas we tend to associate democracies with robust legal protections and strong oversight institutions (especially with

[2] Traditional forms of repression impose political costs on the leader when a variety of groups (both domestic and international) observe these forms of repression and respond in ways that penalize the leader.

[3] For example, Deibert et al. (2008); Howard et al. (2011); Dainotti et al. (2011); Gohdes (2015); Rydzak (2015); Hellmeier (2016); Wagner (2018); Deibert (2019); Qiang (2019); and Diamond (2019).

[4] While cellular technology is certainly not new, the widespread use of smartphones allows citizens to make use of cellular technology to access the Internet.

respect to the private sector), we do not need to travel far to find cases of democracies with timid approaches to oversight and protection of individual rights – the obvious example is the US government's reluctance to reign in technology giants such as Apple or Facebook. Once governments gather information about users, they can engage in two kinds of activities that may lead to violations of citizen's rights through either physical integrity or civil liberties violations. First, states can monitor and surveil perceived existing or potential threats. Second, states can limit access to ICTs or specific ICT content for individuals or groups perceived to present a threat to the state. The monitoring of threats and restrictions on threatening behavior are not new behaviors for states. However, digital technologies provide new opportunities for states to exercise control.

2 THE IMPACT OF ICTS ON STATE REPRESSION

We argue that state repression requires four specific components to function effectively. First, a state must have the ability to *identify a threat*. Second, the state must have the *tactical expertise* to address the threat. Third, a state must be able to compel *responsive repressive agents* to address a threat in a specified way. And fourth, the state must have a physical *infrastructure of repression* that facilitates addressing the threat, or at least does not make addressing the threat prohibitively costly. Below we discuss these components of repression and conceptualize the potential impacts of ICTs on each.

2.1 *Threat Identification*

Governments engage in repression in order to prevent or respond to existing or potential threats. The first component of repression, therefore, requires the state to be able to effectively identify and monitor these threats. Identifying and monitoring threats is costly. These costs are largely associated with gathering information which, depending on the nature of the threat, are likely to vary. Costs vary depending on whether the government is responding to an existing and observable threat (such as a protest or riot, or formal political opposition) or whether the government is attempting to detect a potential threat, which could be more difficult to identify.

Threat identification requires that governments have cultural, linguistic, and geographic knowledge (Lyall, 2010). The costs associated with gathering this kind of knowledge vary depending on context (Sullivan, 2012). For example, there are urban/rural dynamics when it comes to threat identification. In some circumstances, it is easier for the state to monitor threats in an urban center, which may be close to the political capital, rather than in the hinterland, where geographic barriers could hinder information collection (Herbst, 2000). Conversely, in other contexts, urban concentrations may make it more costly to identify and isolate a particular threat. The size of a potential threat also impacts the costs of threat identification.

Mass surveillance of the Uighur population, for example, requires the identification and monitoring of approximately twelve million people.

In both traditional forms of state repression and digital repression, information is central to identify existing and potential challenges to the state. Digital technologies offer the possibility of significantly lowering the costs of information collection for the state. The speed and volume with which information can be collected and processed is far greater than with any monitoring or surveillance techniques of the past. Moreover, as Deibert and Rohozinski (2010, p. 44) write, "Digital information can be easily tracked and traced, and then tied to specific individuals who themselves can be mapped in space and time with a degree of sophistication that would make the greatest tyrants of days past envious." Individuals leave digital footprints, online or through cellular communication, with information that ties them to specific beliefs, behaviors, and locations. States can also track a much broader section of the population than was ever previously possible. For example, states threatened by mass mobilization can now closely monitor, in real time, crowd formations with the potential to become mass rallies, allowing police to be put on standby to immediately break up a protest before it grows (Feldstein, 2019, p. 43).

The availability of less overt forms of threat detection may open up new strategic possibilities for governments, shaping their choice among forms of digital repression as well as between digital and traditional repression. For example, it is possible that a state would refrain from using certain monitoring tactics that are visible and attributable to the state, not because they would be useless in identifying a particular threat, but because the government does not want to tip its hand about its repressive capacity. In this circumstance, a government might choose to monitor a population, for example, rather than engage in mass incarceration. Still, digital technologies for threat identification also carry costs. The Xinjian authorities, for example, reportedly budgeted more than $1 billion in the first quarter of 2017 for the monitoring and detention of the Uighur population there (Chin & Bürge, 2017). However, this figure is likely lower than the amount the Chinese state would have spent to construct a comparable system without using digital technologies (Feldstein, 2019, pp. 45–46). Furthermore, once those investments have been made, a form of path dependence is likely to ensure that the new expertise will continue to lead to particular forms or repression (as we discuss in the next section on tactical expertise).

The ability to access more, indeed enormous, amounts of information has the potential to increase the cost of threat identification. In fact, such volume of searchable data raises the challenge of identifying a threatening signal in an ever growing pile of digital noise. The problem, then, is not simply finding a signal, but the possibility that more digital noise could result in biased or wrong signals. Digital surveillance is often a blunter monitoring tool than individual surveillance techniques of the past, given the quantity of digital information which is now available. However, the development of algorithms and reliance on artificial intelligence for sifting through large amounts of information can significantly lower threat identification

costs for states. But such tools, in turn, require new forms of tactical expertise. We discuss this issue in the next section.

2.2 *Tactical Expertise*

Once a threat has been identified, in order to repress effectively the state must have the ability to address the threat. Tactical expertise refers to the actual know-how of repression – that is, the skillsets developed by the state to exert control, ranging from surveillance techniques to torture tactics. A number of studies demonstrate that repressive tactics are both taught and learned (see, e.g., Rejali, 2007). Understanding the tactical expertise of a state when it comes to repression can tell us not only about the ability of the state to repress in the first place, but also about the type of repression the state is most likely to engage in when faced with a particular threat. Each state will have a specific skillset that enables it to repress in certain ways, but not in others. Certain techniques of repression may be unavailable to a state, or they would require the costs of appropriating a new skill. States may or may not be able to incur those costs. For example, states may invest in becoming experts at torture or, instead, they might invest in tools of riot policing. The "coercive habituation" of a state suggests that, if the state has engaged in repression or a type of repression in the past, this lowers the costs of applying the same form of repression in the future (e.g., Hibbs, 1973; Poe & Tate, 1994; Davenport, 1995, 2005). Therefore, the likelihood of becoming proficient at a particular repressive tactic is (at least in part) a function of the state's history of threats and threat perception, as well as the history of the state's response to these threats. We expect states to have varying levels of expertise across a variety of coercive tactics. These levels of expertise are reflected in the training centers, organizational infrastructure, and command structure of particular governmental actors charged with implementing repressive tactics.

Digital repression requires *technological* knowhow or expertise. This might be reflected in the availability of experts trained in information technology, fixed network and mobile technologies, or critical systems infrastructure. Technological expertise ultimately corresponds to the country's reservoir of expert knowledge in the use, maintenance, and control of ICT systems. Given the resource requirements of acquiring this form of expertise in order to implement certain forms of digital repression, some governments may be unable or unwilling to incur the costs of developing the relevant skillset.

The relevant type and level of technological know-how required for digital repression varies based on who a state targets with digital repression, as well as what (if any) content is being restricted. Targets of digital repression can range from individual users to specific groups across specific geographic regions, or the whole country. States can also restrict access to, or publication of, information ranging from single websites to entire platforms or applications. In some cases, states can engage in a wholescale Internet or cellular communications blackout. Targeting individual users, as opposed to large swathes of the population, may be

https://doi.org/10.1017/9781108954341.002 Published online by Cambridge University Press

more costly as it requires a higher level of threat identification, and potentially greater levels of technical and algorithmic expertise. Similarly, targeting a specific website or single platform is often more costly and requires greater technical capacity than enforcing a wholescale Internet blackout.[5] The presence of a "kill switch" in some countries means that the state can easily disrupt telecommunications by creating a network blackout, a crude though often effective form of digital repression. It is more technically difficult, for example, to restrict access to a specific platform such as WhatsApp or Twitter, or to block access for a specific individual or group, especially if targeted individuals have their own technological expertise to develop effective workarounds (i.e., virtual private networks, for example). The target and form of digital repression is therefore influenced by the state's availability and nature of tactical expertise.

2.3 *Responsive Repressive Agents*

Once a threat has been identified and a repressive strategy has been chosen, governments rely on repressive agents to implement that strategy. In general, the leader himself/herself is decidedly *not* the agent of repression. Instead, the state relies on a repressive apparatus. Unpacking the state into a principal (leader) and an agent (the security apparatus), as much of the literature on repression does, is helpful for demonstrating that organizational capacity and power are necessary dimensions of the state's ability to repress. This ability corresponds to the level of centralization, the degree of organization, and the level of loyalty of the repressive agents. The agents of repression are often confined within a set group of organizations that vary by regime and regime type, such as the police, military, presidential security, etc. On rare occasions, state repression can be outsourced to agents not directly under the command of the state, for example, pro-government militias, vigilante groups, or private military contractors. The outsourcing of repression further complicates the issue of ensuring compliance from repressive agents. The state must have the ability to develop these organizations as loyal, responsive agents endowed with the expertise to implement the relevant repressive tactic.

Some forms of digital repression may require fewer repressive agents, simplifying principal-agent issues for repressive states. For example, digital repression might be carried out by a few technical experts within a government agency, or by an automated algorithm. One intuitive possibility is that requiring fewer agents to carry out a repressive action is less costly because of lower coordination costs and gains in efficiency. In the past, mass surveillance required an extensive network of informers. For example, in Poland in 1981, at the height of the Sluzba Bezpieczenstwa's (Security Service) work to undermine the Solidarity

[5] These costs are also likely to vary depending on the website or platform, since many larger companies (Google, for example) have begun to develop their own Internet infrastructure.

movement, there were an estimated 84,000 informers (Day, 2011). New technologies produce the same level of surveillance (or greater) from the work of far fewer people. However, while fewer agents may be easier to coordinate, failure or defection by one among only a few repressive agents may be more costly in comparison to failure by one among thousands.

Online communication and access to digital space further requires a telecommunication company or Internet provider which may be outside of the state's direct control. Though governments often have ownership stakes in these companies, which are seen as a public utility, the companies themselves remain independent actors. The level or ease of control that the state exhibits over the ICT sector varies, thereby shaping how easily the state can compel the sector to engage in repressive behaviors, such as monitoring usage or controlling access. For certain forms of digital repression, governments require greater capacity to compel specific actions on the part of these actors (such as shutting down the Internet, limiting access to specific platforms, limiting broadband access, etc.). The power to compel these actions is determined by government involvement in the sector and by market characteristics (industry structure and the number of actors), as well as existing legal protections – for example, regulations determining whether or when Internet service providers are required to turn over data to the state. In Europe, the General Data Protection Regulation, though aimed primarily at private actors, gives greater control to users over their individual data, and therefore makes it more difficult for governments to obtain access to personal, individual user data. If firms cannot collect it, they cannot be compelled to provide it to governments. In these ways, ICTs have the potential to simultaneously simplify and complicate the state's relationship to its repressive agents, making it difficult to anticipate how ICTs will change the costs of repression in this regard.

2.4 *Infrastructure of Repression*

The capacity to apply repressive pressure in response to an identified threat requires what might be called an *infrastructure of repression*. This infrastructure should be thought of as the physical, geographic, or network characteristics that make it more or less costly (in terms of effort and resources) to engage in repression. At its most basic, repression infrastructure refers to sites of repression, such as prisons and detention facilities. It also refers to the physical environment in which repressive tactics are executed, which include the man-made and natural terrain that shapes the costs of repression (Ortiz, 2007). In civil war literature, many have argued that the existence of a paved road network reduces the government costs of repressing a threat because government vehicles and soldiers can more easily access their targets (Buhaug & Rød, 2006). This result echoes James Scott's discussion of the rebuilding of Paris by Hausmann, which had the explicit goal of constructing a gridded road that government troops could use to more easily reach any part of the city to prevent or put down riots or protests in the aftermath of the French Revolution (Scott, 1998).

https://doi.org/10.1017/9781108954341.002 Published online by Cambridge University Press

The concept of a repressive infrastructure has an intuitive analogue in the digital repressive space due to the physicality of telecommunications. The technologies that facilitate communication and the diffusion and exchange of information require physical infrastructures – the cellular towers, the fiber-optic cables, the data centers, and interconnection exchanges[6] – that are the building blocks of the networks of digital and cellular communication.

Scholars have begun to use the characteristics of a country's Internet technology network of autonomous systems (ASs) and the number of "points of control" to rank and characterize digital infrastructure in terms of the level of control governments can exert over citizen access to telecommunications networks and the data flowing across them (Douzet et al., 2020). Autonomous systems route traffic to and from individual devices to the broader Internet, which in turn is a collection of other ASs. The AS is, therefore, the primary target of regulation, monitoring, and interference by the state. Because most ASs are part of a larger network of systems, the vast majority of Internet traffic flows through a relatively small number of ASs within a country (often between three and thirty).[7] The minimum set of ASs required to connect 90 percent of the IP addresses in a country are called "points of control." The more points of control there are in a country, the more costly it is to regulate or restrict digital communication (both in terms of skills and equipment).

Roberts et al. (2011) have mapped two characteristics of in-country networks: the number of IP addresses (a proxy for individual users) per point of control and the level of complexity of the network within a country (the average number of ASs a user has to go through to connect to the Internet). Countries with more centralized systems and fewer points of control are places in which governments can much more easily exert control over access to the Internet for large portions of the population, and over the data that travel across the network. For example, as of 2011, the Islamic Republic of Iran had only one single point of control, with over four million IP addresses and a low network complexity score, which ensured that the state could easily control the entire Internet. According to Roberts, "in Iran, shutting down each network takes only a handful of phone calls" (Roberts et al., 2011, p. 11). As a result, such systems may require less expertise, less time, and less equipment to obtain and collect data, monitor users, or limit access. The greater the level of control over the infrastructure a state commands, the lower the costs to engage in digital repression.[8]

[6] Also called Internet exchange points (IXP).

[7] There are an estimated four billion Internet users globally, each of whom must connect to the Internet through an AS (of which there are an estimated 60,000 in total).

[8] The infrastructure of digital repression is not, however, an entirely exogenous component of the state's decision to engage in a particular kind of repression. The nature of these network characteristics is not accidental, but often designed to facilitate state control. Referring back to the invention of the Internet, Roberts et al. (2011) note that "the birth of the Internet as the split of ARPANET into two politically distinct networks was an explicitly political decision – intended to allow distinct modes of political control over the distinct networks" (p. 3).

In addition to the network characteristics of the Internet within a country, the infrastructure for digital repression is also characterized by how the majority of individuals communicate and access the Internet. Smart cellular phones are by far the most common devices used to access the Internet, in addition to facilitating voice and text communication. They provide an additional point in the digital infrastructure where states can exert control. For example, states may impose regulations requiring proof of identification in order to obtain a cell phone and sim card. By doing so, they are able to collect large amounts of data about who owns which devices, and thereby monitor individual communications and data (including locational data).

3 NEW THOUGHTS ON DIGITAL STATE REPRESSION AND CYBER PEACE

States repress when the benefits of repression outweigh its costs. But when states repress using digital tools, how does this calculus change? How do digital forms of repression coexist with, or substitute for traditional forms of repression? And how does the combination of traditional and digital forms of repression affect the goal of cyber peace?

These are some of the questions we need to address in order to tackle the complex interactions among domestic state repression, digital technologies, and cyber peace. This chapter does not provide comprehensive answers, but it begins to unpack these interactions. In particular, our contribution is twofold. First, we break down repression into four constituent components, facilitating a conceptualization of repressive actions that cuts across the traditional/digital divide. This framework provides a useful workhorse for advancing research on the empirical patterns of repression. Second, we use this mapping to begin to explore the complex ways in which digital repression can impact each of the four components.

The value of our mapping exercise for scholars and practitioners in the field of cyber peace and cybersecurity emerges most poignantly in the reflections we offer about the tradeoffs between domestic and international security. For example, an Internet architecture that has a single point of control allows for governments to easily control access to the Internet and monitor data traveling over the network, but it also presents a vulnerability to foreign actors who only need to obtain control of, or infiltrate that point of control in order to gain access to domestic networks. This was in fact the case with Iran which, as noted earlier, had a single point of control until 2011. However, in recognition of the potential vulnerabilities to foreign intrusions that this created, Iran has since sought to add complexity to its digital infrastructure (Salamatian et al., 2019). But, as a result, it also had to acquire greater expertise to manage this complexity, developing a broader range of tools to monitor users and control access (Kottasová and Mazloumsaki, 2019). Another issue concerns strategic interdependencies: States may need to rely on international collaborations to carry out repression within their own borders. This problem is

particularly acute given the fact that servers are often housed in data centers outside the country in which most of their users reside.

Our contribution also suggests that some of the core insights in the literature on repression need reconsideration. For example, the literature on repression suggests that while all regime types repress, democracies repress less than autocracies (Davenport, 2007). However, this may not be true in the case of digital repression. Given the importance of the audience costs that we tend to associate with democratic regimes, we might expect democracies to invest and engage more in forms of repression that are more difficult to detect and observe. Perhaps, more interestingly, the existing literature suggests that democracies and autocracies differ with respect to the way they use information, and such differences expose them to different threats (Farrell & Schneier, 2018). This difference may shape the cost–benefit analysis of engaging in certain forms of digital or traditional repression in distinct, regime-specific ways.

Moreover, the repression literature further suggests that under certain conditions state repression may increase rather than eliminate dissent. The dissent–repression nexus may require reexamination in light of how ICTs are reshaping repression. The addition of a new menu of repressive tactics that can be used in conjunction with, or in place of, traditional forms of repression may lead the state to more effectively mitigate or eliminate threats in ways that make them less likely to resurface or produce backlash. This is in part because of the addition of more covert forms of repression that might be less observable and generate fewer grievances down the line.

Finally, the literature suggests that repression requires high levels of state capacity. However, when states repress through computers, and not police and tanks, repression may rely on sectors and skills that we do not currently measure or think of as relevant dimensions of state capacity. In particular, taking a more granular, multidimensional approach to state capacity, with particular attention to the specific capacity to repress, may shed new light on the relationship between generalized state capacity for repression and state capacity for digital repression.

These observations also yield a distinct, methodological question: If digital repression makes preemptive repression more effective, how can we continue to effectively measure repression since we will have many more unobservable cases in which repression preempted the emergence of an observable threat? Although we do not venture to answer this question, we hope that our chapter offers a starting point for a comprehensive analysis of repression in its traditional as well as digital forms.

The ability of states to violate the political and civil liberties of their populations through digital technologies is a direct threat to cyber peace. While often overlooked in our more internationalized discussion of cyber warfare, how states use and misuse digital technologies to monitor and control their populations is a subject that requires much more attention both because it can shape and be shaped by internationalized cyber warfare, and also because it is an important empirical and normative concern in and of itself.

https://doi.org/10.1017/9781108954341.002 Published online by Cambridge University Press

REFERENCES

Associated Press (2020, June 29). China cuts Uighur births with IUDs, abortion, sterilization. The Associated Press. https://apnews.com/article/ap-top-news-international-news-weekend-reads-china-health-269b3de1af34e17c1941a514f78d764c

Buhaug, H., & Rød, J. K. (2006). Local determinants of African civil wars, 1970–2001. *Political Geography*, 25(3), 315–335.

Carey, S. C. (2006). The dynamic relationship between protest and repression. *Political Research Quarterly*, 59(1), 1–11.

Chin, J., & Bürge, C. (2017, December 17). Twelve days in Xinjiang: How China's surveillance state overwhelms daily life. *The Wall Street Journal*. www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

Cockerell, I. (2019, May 9). Inside China's massive surveillance operation. *Wired*. www.wired.com/story/inside-chinas-massive-surveillance-operation/

Dahl, R. A., Ed. (1966). *Political oppositions in western democracies*. Yale University Press.

Dainotti, A., Squarcella, C., Aben, E., Claffy, K., Chiesa, M., Russo, M., & Pescapè, A. (2011, November). Analysis of country-wide internet outages caused by censorship [Manuscript]. Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. Berlin, Germany. https://doi.org/10.1145/2068816.2068818

Davenport, C. (1995). Multi-dimensional threat perception and state repression: An inquiry into why states apply negative sanctions. *American Journal of Political Science* 39(3), 683–713.

Davenport, C. (2005). Understanding covert repressive action: The case of the US Government against the Republic of New Africa. *Journal of Conflict Resolution* 49(1), 120–140.

Davenport, C. (2007). *State repression and the domestic democratic peace*. Cambridge University Press.

Day, M. (2011, October 18). Polish secret police: How and why the Poles spied on their own people. The Telegraph. www.telegraph.co.uk/news/worldnews/europe/poland/8831691/Polish-secret-police-how-and-why-the-Poles-spied-on-their-own-people.html

Deibert, R. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy*, 30(1), 25–39.

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Gross Stein, J. (2008). *Measuring global internet filtering*. MIT Press.

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, 21(4), 43–57.

Diamond, L. (2019). The road to digital unfreedom: The threat of postmodern totalitarianism. *Journal of Democracy*, 30(1), 20–24.

Douzet, F., Pétiniaud, L., Salamatian, L., Limonier, K., Salamatian, K., & Alchus, T. (2020, May 26–28). Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis [Manuscript]. 12th International Conference on Cyber Conflict (CyCon). Tallinn, Estonia.

Dragu, T., & Lupu, Y. (2020). Digital authoritarianism and the future of human rights. *International Organization*. http://yonatanlupu.com/Dragu%20Lupu%20IO.pdf

Farrell, H. J., & Schneier, B. (2018, October). Common-knowledge attacks on democracy. Berkman Klein Center Research Publication. https://cyber.harvard.edu/story/2018-10/common-knowledge-attacks-democracy.

Feldstein, S. (2019). The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy*, 30(1), 40–52.

Gohdes, A. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, 52(3), 352–367.

Gohdes, A. (2020). Repression technology: Internet accessibility and state violence. *American Journal of Political Science*, 64(3), 488–503.
Goldstein, R. J. (1978). *Political repression in modern America from 1870 to the present*. GK Hall & Company.
Hellmeier, S. (2016). The dictator's digital toolkit: Explaining variation in Internet filtering in authoritarian regimes. *Politics & Policy*, 44(6), 1158–1191.
Herbst, J. (2000). *States and power in Africa*. Princeton University Press.
Hibbs, D. A. (1973). *Mass political violence: A cross-national causal analysis*. Wiley.
Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review*, 14(3), 216–232.
Koopmans, R. (1997). Dynamics of repression and mobilization: The German extreme right in the 1990s. *Mobilization: An International Quarterly*, 2(2), 149–164.
Kottasová, I., & Mazloumsaki, S. (2019, November 19). The "internet as we know it" is Off in Iran. Here's why this shutdown is different. *WRAL*. www.wral.com/the-internet-as-we-know-it-is-off-in-iran-heres-why-this-shutdown-is-different/18778492/?version=amp [Accessed: April 20, 2021].
Lyall, J. (2010). Are coethnics more effective counterinsurgents? Evidence from the second Chechen War. *American Political Science Review*, 104(01), 1–20.
Maizland, L. (2019, November 25). China's repression of Uighurs in Xinjiang. Council on Foreign Relations. www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang
Moore, W. H. (1998). Repression and dissent: Substitution, context, and timing. *American Journal of Political Science*, 42(3), 851–873.
Nielsen, R. A. (2013). Rewarding human rights? Selective aid sanctions against repressive states. *International Studies Quarterly*, 57(4), 791–803.
Ortiz, D. (2007). Confronting oppression with violence: Inequality, military infrastructure and dissident repression. *Mobilization*, 12(3), 219–238.
Poe, S., & Tate, C. N. (1994). Repression of personal integrity rights in the 1980s: A global analysis. *American Political Science Review* 88, 853–872.
Qiang, X. (2019). The road to digital unfreedom: President Xi's surveillance state. *Journal of Democracy*, 30(1), 53–67.
Rasler, K. (1996). Concessions, repression, and political protest in the Iranian revolution. *American Sociological Review*, 61(1), 132–152.
Rejali, D. (2007). *Torture and democracy*. Princeton University Press.
Roberts, H., Larochelle, D., Faris, R., & Palfrey, J. (2011). Mapping local internet control. In *Computer communications workshop (Hyannis, CA, 2011), IEEE*.
Rydzak, J. (2015). The digital dilemma in war and peace: The determinants of digital network shutdown in non-democracies [Manuscript]. International Studies Association 57th Annual Convention. Atlanta, GA, United States.
Salamatian, L., Douzet, F., Limonier, K., & Salamatian, K. (2019). The geopolitics behind the routes data travels: A case study of Iran. arXiv. https://arxiv.org/ftp/arxiv/papers/1911/1911.07723.pdf
Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.
Shackelford, S. J., & Kastelic, A. (2015). Toward a State-centric cyber peace: Analyzing the role of national cybersecurity strategies in enhancing global cybersecurity. *NYUJ Legis. & Pub. Pol'y* 18, 895.
Sullivan, C. M. (2012). Blood in the village: A local-level investigation of State Massacres. *Conflict Management and Peace Science*, 29(4), 373–396.

Wagner, B. (2018). Understanding Internet shutdowns: A case study from Pakistan. *International Journal of Communication*, 12(1), 3917–3938.
Wen, P., & Auyezov, O. (2018, November 29). Turning the Desert into Detention Camps. *Reuters*. www.reuters.com/investigates/special-report/muslims-camps-china/