Government and Opposition (2023), 1–23
doi:10.1017/gov.2023.20

Government & Opposition

ARTICLE

How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship

Oliver Schlumberger[1], Mirjam Edel[1], Ahmed Maati[2] and Koray Saglam[1]

[1]Institute of Political Science, Tübingen University, Tübingen, Germany and [2]Technical University of Munich (TUM), School of Social Science and Technology, Hochschule für Politik, Munich, Germany
Corresponding author: Ahmed Maati; Email: ahmed.maati@tum.de

(Received 22 March 2022; revised 13 February 2023; accepted 26 March 2023)

Abstract
While digital technologies have induced profound global transformations, political scientists often lack the analytical tools to grasp their effects on politics. In particular, digitization's impact on dictatorships remains not only empirically understudied, but seriously under-conceptualized. How do new technological possibilities affect autocratic politics? This contribution starts from the inner logic of authoritarianism rather than from technical innovation. It first maps the ways in which autocrats employ various digital technologies to maintain power. This helps us identify seven core areas where dictatorial politics are transformed by the use of new tools. We delineate the key characteristics of these areas of change and conclude that, in their sum, technologically induced transformations significantly alter the nature of dictatorship if and when it is digitized.

Keywords: digital; authoritarianism; transformations; dictatorship; power

The digital revolution's massive impact on politics is undisputed. From tech giants such as Google's or Cambridge Analytica's disruptive political influence to China's 'Great Firewall', evidence abounds that digitization fundamentally changes social textures, political practices and sometimes outcomes.[1] But while some scholars view digitization as a threat to democracy and others see its potential as a pro-democratic tool for mobilization (among many others, see, e.g. Boehme-Neßler 2020; Gil de Zúñiga et al. 2010; Hindman 2009; Howard and Hussain 2011; Zuboff 2019), the impact of the digital on authoritarianism has been studied far less than its impact on democracy (notable exceptions are discussed below).

It is common wisdom that in modern dictatorships, rulers 'must contend with the omnipresent threat of overthrow' (Frantz 2018: 104).[2] But while it is well established that dictators aim at perpetuating power,[3] it is far less clear how to fully grasp the political impact of digitization in such authoritarian environments of power maintenance, and how this might change the overall face of authoritarianism. We address this gap by presenting an analytical framework for the study of digital dictatorship that helps us better understand how digital technologies influence political processes and outcomes under authoritarianism, and how these transformations make digitized 21st-century dictatorship distinct from the ways authoritarianism has traditionally been viewed. Future research should hence not only examine changes *in* authoritarianism, but also the macropolitical regime *type* dimension (changes *of* authoritarianism).

A new framework for analysis: why and how?

After initial euphoria about digitization's democratic potential, more and more contributions now examine how autocrats instrumentalize digital technologies. Gerasimos Tsourapas (2020) and Steven Feldstein (2021) hint at digitally enabled domestic and transnational repression, while Sergei Guriev and Daniel Treisman (2019) describe how 'informational autocrats' base their rule on the manipulation of information (instead of on terror or ideology). Seva Gunitsky (2015) focuses on how social media help autocrats bolster legitimacy and gain more accurate information about their population, thereby acquiring some of the functions routinely ascribed to autocratic elections. Espen Rød and Nils Weidmann (2015) demonstrate how the internet is used as a 'repression technology' in autocracies, and Xu Xu (2020) finds that increased digital surveillance leads to more targeted repression, which in turn reduces the dictator's costs of co-optation. Others have studied the impact of new technologies on variables such as regime duration or the likelihood of protests (Frantz et al. 2020; Kendall-Taylor et al. 2020; Maerz 2016).

These are important contributions, and we still need more comparative and case-based empirical studies. Yet, there is a growing awareness that this emerging literature, its merits notwithstanding, lacks the theoretical embeddedness necessary to systematically relate findings about the usage of digital technologies (1) to the strategic ends of authoritarian regimes, and (2) to the transformational political effects of such new technologies. Nor does studying individual aspects of digitization necessarily tell us whether and in what respect the *nature* of authoritarianism transforms.

This latter question is pertinent as it remains unanswered because existing research has not operated on the level of abstraction that would allow to confer a locus to each of the contributions within the emerging broader research agenda. While Eda Keremoğlu and Nils Weidmann (2020) rightly lament the lack of a theoretically embedded framework for analysis, our contribution provides just that. Thus, this article neither represents another piece of empirical research nor does it provide a comprehensive literature review of the emerging field. Rather, we provide a framework that enables us to better assess how digital technologies influence political processes and outcomes in autocracies.

In contrast to the recent suggestion to structure the field according to which techniques dictators employ – that is, by focusing on the new epiphenomenon of the digital (Keremoğlu and Weidmann 2020) – we hold that the link between the digital and the dictator needs to be analysed from the other end, that is: to start from what we know about dictatorship. Only by considering the dictator's overarching logic of power maintenance that guides policies can we comprehend

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

why and *to what effect* dictators[4] employ *what means* to stay in power. Unlike a tool-centred approach, the holistic perspective adopted here enables scholars to make statements about what exactly is changing in the nature of politics on a political (not technical) level. On that basis, it can also stimulate theory-building by linking new observations to existing knowledge about autocracies. By starting from the logic of authoritarian rule, digitization becomes clear as an intervening variable rather than being mistaken for an independent in some causal vacuum. The goal is thus to white-balance new technological developments with authoritarianism as classically defined by Juan Linz (1964, 1975); the starting point for structuring the field thus needs to be 'seeing like an autocrat', not 'seeing like a technocrat'.

We first outline the dictator's agenda of power maintenance on a meta level. This step is based on, but does not explicitly review, the vast recent literature on authoritarianism.[5] Most generally, dictators want: (1) to be informed as perfectly as possible, that is to *know* about what their societies and elites (i.e. their 'subjects')[6] do or plan; (2) to *influence* their subjects' *behaviour* to achieve compliance so that it does not threaten their rule; and (3) to *manipulate* their subjects' *beliefs* so that their rule appears legitimate – which, if successful, is automatically conducive to (2).[7] Second, we move down to the meso level of technological innovation to empirically identify and categorize the new digital tools in the hands of dictators while simultaneously linking them to the latter's agenda of power maintenance. Finally, we white-balance these first two steps and thereby identify seven core areas of political (as opposed to technical) change. We claim that these areas of transformation may be constitutive (though not necessarily exhaustive) for the emerging research agenda on digital dictatorship.[8] Each of these areas is classic in the comparative study of politics and contains at least one original hypothesis to invite fresh scholarly debate in what has become a major new field of research.

In sum, autocracies will be digitally transformed in ways that likely go beyond a mere 'authoritarian upgrading' (Heydemann 2007) or incremental modifications of authoritarian practices.[9] Rather, we witness changes on the conceptual level of regime characteristics. The idea that technology can be a defining element of political rule is not new. Carl Friedrich and Zbigniew Brzezinski (1956), for instance, defined totalitarianism as, inter alia, monopolistic control over mass media, a feature peculiar to modernity. This nexus between (autocratic) political rule and technological requisites that condition the former is important because certain regime types cannot exist without specific technologies. We argue that today we witness no less than such a technologically induced transformation of political rule in authoritarianism. As such, this is not unique, but it is historic (see boxes 'technological innovation' in Figure 1 below).

The dictator's perpetual agenda: power maintenance

The following builds on broad and largely uncontested insights that research on authoritarianism has unearthed, rather than on any particular theoretical approach or school of thought, because the aim is to provide a general framework for analysing digitized and digitizing dictatorship with global applicability. Theoretically, the stability of authoritarian regimes has been convincingly analysed as based on

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

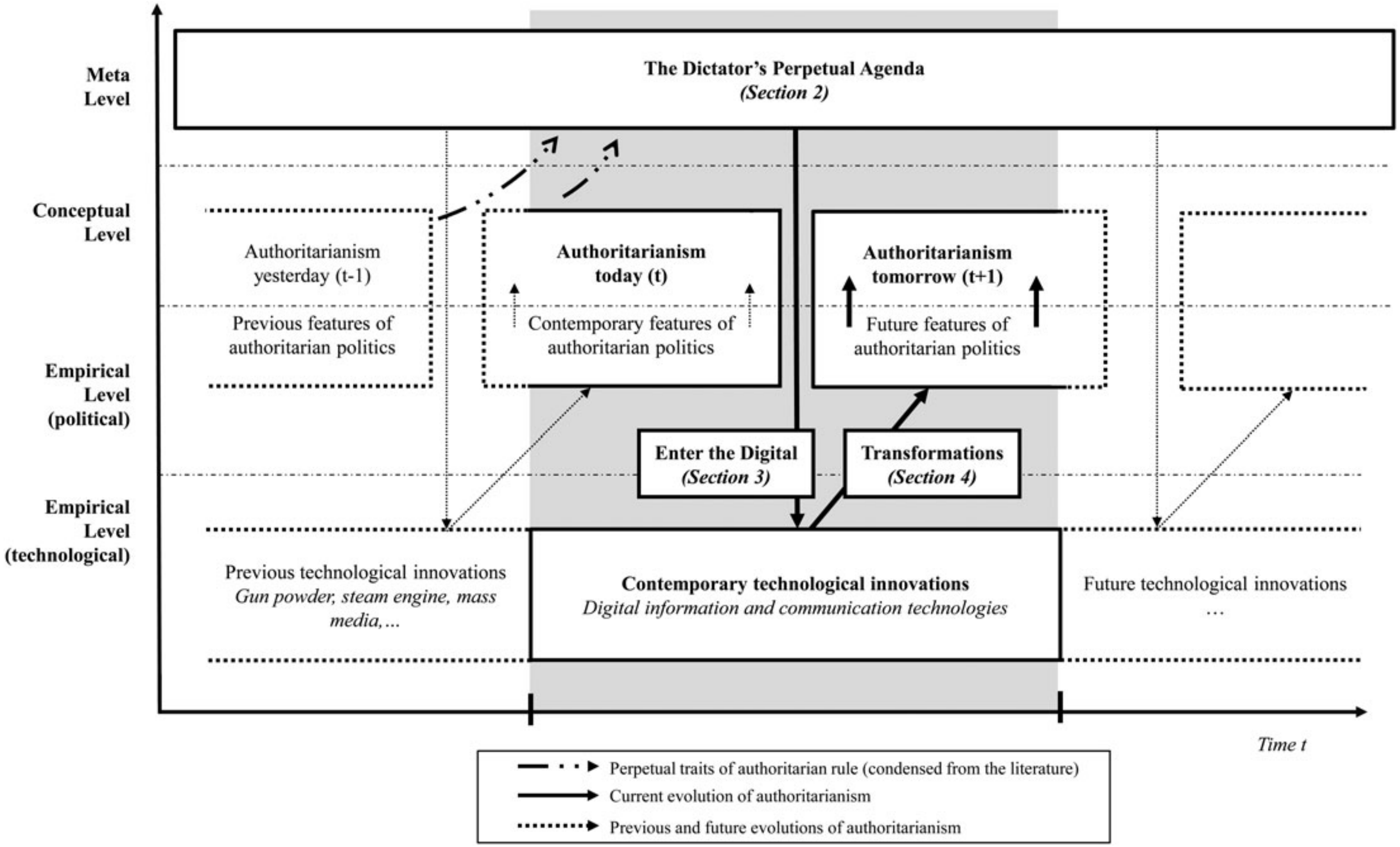
Meta Level
Conceptual Level
Empirical Level (political)
Empirical Level (technological)
The Dictator's Perpetual Agenda
(Section 2)
Authoritarianism yesterday (t-1)
Previous features of authoritarian politics
Authoritarianism today (t)
Contemporary features of authoritarian politics
Authoritarianism tomorrow (t+1)
Future features of authoritarian politics
Enter the Digital
(Section 3)
Transformations
(Section 4)
Previous technological innovations
Gun powder, steam engine, mass media, …
Contemporary technological innovations
Digital information and communication technologies
Future technological innovations
…
Time t
Perpetual traits of authoritarian rule (condensed from the literature)
Current evolution of authoritarianism
Previous and future evolutions of authoritarianism

Figure 1. The Dictator's Perpetual Agenda

legitimacy, repression and co-optation (Gerschewski 2013). But most research on authoritarianism rests on a yet more general implicit assumption: the dictators' desire to retain power – and in order to retain power, dictators need to eliminate threats, real or perceived.[10] To that end, they seek to *control their subjects* through various strategies, ranging from openly coercive strategies, positive and negative (material and non-material) incentives for compliance, divisive tactics, propagandistic rhetoric, ideology or intimidation, to name but a few.[11] One can now link the classical pillars of legitimation, repression and co-optation to general authoritarian objectives: co-optation and repression directly stem from the objective of *influencing behaviour*. Aspirations to generate legitimacy originate from dictators' desires to *influence the beliefs* of their subjects. To pursue their agenda, autocrats thus need to do three things: they must (1) *know* about potential threats, rivals, grievances and the effectiveness of their strategies. To address threats, they need (2) to *influence the behaviour* of their subjects; and, simultaneously, (3) to *influence their beliefs*.[12]

First, dictators need to gather as much information as possible on subjects in order to recognize threats. To control and manipulate behaviour and beliefs effectively, accurate knowledge about who potential challengers are and what they plot is essential. *Knowing* (what people think, do, or plan) is thus a basic requisite that logically precedes the control and manipulation of behaviour and beliefs. Most 'strategies of knowing' focus on identifying opponents and finding out what they do or plan. Strategies to assess prevailing beliefs more accurately traditionally include elections as 'opinion barometers'. Once information is available, incumbents dissect, analyse and interpret it to respond appropriately to challenge(r)s.

To pre-empt threats, incumbents *directly influence people's behaviour*. Most prominently, they do so through repression: by restricting unwanted activities physically or legally, or by raising the costs of contention. *Repression* thus entails negative incentives and sanctions. But autocrats also set positive incentives for compliance by offering avenues of *co-optation* to selected groups. Divide-and-rule strategies combine positive and negative incentives. They aim at fragmenting potentially threatening opponents so that competing groups keep each other at bay. Thereby, dictators can prevent or eliminate threats but sometimes they act too late or inexactly – which hints at another important path to control behaviour.

Less open than directly controlling and manipulating behaviour, but potentially more effective, is to control narratives that shape subjects' beliefs. By altering and controlling narratives, authoritarian regimes render the populace oblivious to its oppression. In academic terms, such manipulation intervenes in the causal chain and in turn causes behavioural changes. Ideally, orders become unnecessary when compliance becomes voluntary. Nobody contending for power would reduce the costs of repression and, ultimately, of power maintenance. In an autocratic utopia where all people always believed the regime's narratives, coercive apparatuses would be superfluous.

We differentiate between 'constructive' and 'destructive' means to influence beliefs and opinions. First, the construction of narratives occurs in two forms: either governments create and perpetuate narratives themselves (through

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

Table 1. The Dictator's Perpetual Agenda

Control subjects					
Know		Influence beliefs		Influence behaviour	
Collecting information	Processing information	Constructive: through creation and promotion of narratives	Destructive: through discrediting and censoring narratives	Negative incentives and sanctions (mostly repression)	Positive incentives (mostly co-optation)

Source: Authors' own compilation.

propagandistic speeches, state-owned media etc.) or they promote pre-existing narratives by selectively sharing content. By promoting a certain picture of reality, such as by granting pro-regime news more coverage in regime-controlled media, autocrats can marginalize undesired narratives. But they also actively engage in campaigns that produce false 'news' and 'alternative facts' that deliberately create regime-orchestrated (untrue) narratives. Second, incumbents have 'destructive' means to marginalize undesired information and counter-narratives: the production and proliferation of content is restricted via *censorship* of the various media. If it has already spread, unwanted information is *discredited* in public statements and regime-controlled media, or their producer (e.g. an opposition group or army general) is defamed to render the source untrustworthy (Table 1).

Enter the digital

Dictators remain, as always, interested in controlling their subjects, but digitization provides them with a plethora of new opportunities to pursue their goals of *knowing*, *influencing beliefs* and *influencing behaviour*.[13] Contrary to others, we explicitly broaden the view beyond the 'internet' and 'social media'. Digital technologies also include advanced digital devices and programs that, assisted by automatized machine-learning, allow for digitization, analysis and response by the regime. This section provides a comprehensive screening of the digital techniques most commonly used by dictators and illustrates their respective – often multiple – purposes; we thereby show how they relate to the dictator's power-maintenance agenda.

Techniques to know

These are digital techniques for gathering and analysing information. While we separate the two analytically, they are usually employed iteratively: the analysis of information usually leads to better collection and vice versa.[14]

Gathering information

Dictators use four sets of digital techniques to collect information: (1) obtaining user data from service providers, for example through respective legislation; (2) installing additional hardware (data probes, surveillance cameras and other eavesdropping devices) in public spaces, on terminal devices or on the infrastructure such as national gateways;[15] (3) obtaining data directly from users, either through

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

deceptive means or by users voluntarily revealing information through interaction with specific digital applications (e.g. entertainment services, emails or websites) or through interaction with official government websites; and (4) malware and hacking.

First, internet service providers (ISPs) are subject to local laws and forced to provide data to authorities if requested. This applies to all countries, but in most autocracies, legal processes are not independent of the dictator's power-maintenance agenda, and privacy rights remain unenforceable. Data thus acquired contain basic information, such as the frequency of visits to specific websites, but can be more detailed if the service provider uses hardware data probes (see below). Information is also requested from international companies such as Facebook, which argues that it 'responds to government requests for data in accordance with applicable law and [its] terms of service'. Between January and June 2019 alone, Facebook responded positively to over 85 data requests by authoritarian regimes, among them Jordan (Facebook 2019).

Second, hardware eavesdropping components are implanted in digital devices such as smartphones to surveil the in- and outbound traffic of that device. These hardware components are either designed specifically for surveillance (e.g. spy microchips) or manipulated to also serve the purpose of surveillance, for example when sim cards and GPS locators are used to collect information about users' locations and activity. Data probes are hardware components that are installed on national internet cables connected to government-owned servers. They screen all internet traffic passing through the national network and store all thus surveilled internet data on large government servers to be later analysed by computer programs. Russia uses such probes as part of its surveillance program SORM-3 (Lewis 2014).

Third, autocrats also deceive users through phishing campaigns to steal their identities, such as login credentials for social media, email or bank accounts. State officials send links that direct users to fake websites that resemble legitimate or known ones. Entered usernames and passwords are then stored on a government server.

Moreover, dictators have also learned how to incentivize users, that is, to either force users to accept specific cookie settings or browser certificates and actively share their personal and/or device information, or by luring them, sometimes via private companies that subsequently share the data they collect with autocratic regimes, into voluntary sharing such information. For example, the Kazakh regime attempted to force all internet users to install a government browser certificate that allows the government to see the interaction between digital devices and websites unencryptedly (Mozilla 2019). By digitizing government services, governments can create centralized data banks of their citizens that digitally code all bureaucratic steps that individuals take and, in extreme cases, record every daily action of targeted individuals. These are also data sources that are used – for example, in Chinese provinces where social credit systems have been implemented to inform a digitally assisted assessment of subjects from the standpoint of the Chinese regime (Kostka and Antoine 2020; Xu et al. 2022).[16] Online entertainment programs on social media can also be used to gather information.

Fourth, malware and hacking are the most sophisticated and intrusive techniques of data gathering. Spyware collects information from users' devices and

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

sends it to a government server. One infamous example is a program named Pegasus. The Israel-based NSO Group Technologies claims that it sells the program exclusively to law-enforcement agencies (Kenyon 2019). Unsurprisingly, CitizenLab reports that various authoritarian regimes have used the program to target political dissidents. Like other malware programs, Pegasus copies files from the victims' device and sends them via the internet to a server accessible to the surveillance agency. It is also able to delete files and to destroy the infected device. Without the user noticing, malware programs can switch on cameras and microphones on end-user devices, turning them into live spying machines (Cannings et al. 2017).

Analysing information

Authoritarian regimes analyse information with computer programs that can access, sort and analyse the vast amount of data gathered. Some software, such as SolarWinds NetFlow Traffic Analyzer, is commercially available. The capacity of such analysis programs to process data is impressive, and opaque, as the algorithms produced and sold to dictatorships – also by Western companies – are often dual-use technologies. Algorithms developed for identifying cancer cells, for instance, can also be used for face recognition.

Second, regimes also program social media bots to analyse, detect and collect content that regimes deem critical. These algorithms can spot, screen and report critical posts, pages and users, but are also used for additional purposes in digitized dictatorships (more below).

Finally, autocrats use techniques that are not particularly 'digital' to analyse 'big data'. Innovations in psychometrics have allowed Cambridge Analytica to analyse data gathered from over 50 million Facebook users to – among other things – craft personalized voting campaigns. The analysis relied on Facebook profile information, including 'likes' to specific pages and posts, to create personality profiles.

Techniques to influence behaviour

New ways of collecting and analysing information are not ends in themselves, but they allow the autocrat to decide on the choice of digital (and non-digital) techniques to influence behaviour.

Digital repression

While dictators routinely use digitally collected information to repress subjects in the offline world (Kendall-Taylor et al. 2020: 108), this section focuses on techniques of digital repression – that is, techniques of repression targeting digital devices or platforms, regardless of whether this extends to the offline world or not.

Dictators use two techniques to repress digitally. First, they deny users access to online services such as social media profiles, personal or corporate websites or specific communication platforms. Authoritarian regimes utilize their jurisdiction over service providers and pressure international companies to block or delete specific accounts, services or websites. Alternatively, autocrats can deny access to websites and services by blocking access to their IP addresses from within national borders, or digitally attack specific websites in so-called denial-of-service (DOS) attacks.[17] Russia, for instance, domestically blocked Telegram after the latter had refused to provide the state with all encrypted conversations (Dans 2018).

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

Second, dictators target specific individuals and organizations with malware computer programs that destroy devices or steal sensitive data (e.g. private photos) to repress opponents across borders. Malware programs often overlap with surveillance programs (spyware), which also have a transnational reach. A case in point is, again, Pegasus, which has been used to destroy subjects' digital devices outright.

Digital co-optation

The most prominent examples in this area are China's social credit systems. In provinces where such systems are in place, citizens' scores are tied to a virtual account for each person.[18] The score reflects the gross evaluation of an individual's activities. Information surveilled and analysed includes offline behaviour through public surveillance cameras in combination with face recognition, but also online behaviour that is comprehensively surveilled because clients are forced to use accounts that are tied to their individual social credit account. This score, in turn, not only reflects behaviour, but also determines behaviour, as certain privileges must be earned, such as bank credit (including terms and conditions like interest rates), permission to travel internationally, permission to fly, permission to access social media, and even to access the internet as such (Drinhausen and Brussee 2021; Kostka and Antoine 2020; Xu et al. 2022). The range of positive incentives for compliant behaviour is thus very broad and includes most of what subjects consider modern life (Data Justice Lab 2020 gives a complete list). It is true that these systems are not yet implemented across all Chinese provinces equally and coherently; they still require human agency, and do not (yet) result in one coherent central data set that could be analysed in real time. Yet, the existing systems demonstrate the technical capacities that autocrats can utilize for surveillance and for granting or withholding rights and privileges (Drinhausen and Brussee 2021). As to its effects, thus, it makes sense to conclude that in the eyes of the subject, it is the political leadership who grants the benefits of modern life and for which it can expect gratitude and compliance in return – while they can be withdrawn from ungrateful subjects.

Techniques to influence beliefs

Pro-regime propaganda

One way to establish pro-regime narratives digitally is to use traditional propaganda techniques on government-owned websites. Apart from the important information-gathering function discussed above, another reason why authoritarians digitize public services is that e-governance can not only carry propaganda messages, but also serves to promote a legitimizing image of advanced regime performance (output legitimacy). By advancing e-governance, autocracies legitimize their rule by painting a digital façade of participation and responsiveness (Maerz 2016). Unsurprisingly, thus, authoritarian regimes invest particularly heavily in e-governance – but for reasons very different from international donor intentions. Another way is to employ social media bots to create and spread pro-regime narratives. These bots pretend to be humans on social media. They comment, like, post and share content. Russia, China and the Middle East are but some of the locations where 'bot armies' are extensively used to spread regime propaganda (see Jones 2022; Oxford Internet Institute 2021).

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

As Russian interference in the 2016 US elections demonstrated, target audiences of digital propaganda campaigns are not exclusively domestic. National and international digital disinformation campaigns include the creation of fake news through bots or trolls (humans who create content of the aforementioned sort) not only to influence opinions and beliefs, but also to instil scepticism about truth more generally.

Censorship and discreditation

One core feature of authoritarianism is the restriction of 'access to alternative sources of information'.[19] Digital technologies allow autocrats to censor online content more effectively and less expensively than manual censorship. Digital censorship includes, first, the cooperation of online service providers to remove content and pages deemed critical by the regime and, second, the direct blocking of websites, as happened to Wikipedia in Turkey because it had informed about corrupt government officials. Third, bots also censor online content. These algorithms can be programmed to automatically detect and block webpages that contain critical keywords or content. The Chinese Great Firewall combines numerous algorithms to filter and block critical content automatically (Arthur 2012).

Social media bots can also be programmed to defame and discredit opponents, as well as to influence news coverage. Bahrain, for instance, employed such bots during the 2011 uprisings to 'troll' posts and pages of political opponents (Jones 2019).

The most drastic digital censorship is to shut down the internet altogether, regionally or nationally, to prevent international audiences from getting information about regime crackdowns on opposition. When, in 2019/2020, the Iranian regime killed over 1,000 people in a crackdown on demonstrations, it was hardly covered by international media, nor did it trigger political reactions as it was conducted during an ordered internet shutdown.

As with information gathering and processing, dictators' capacities to control national and substantially influence international public discourse have vastly increased with digitization; accordingly, so have their abilities to influence what their subjects believe.

Trade-offs between the various strategies where the use of one might undermine the other have existed before digitization and continue to exist. But such trade-offs seem to be ameliorated by digitization in various ways. For instance, while one might think that more effective censorship of public discourse would deprive regime leaders from useful information, the opposite seems more likely because, while 'public' discourse is censored, digital technologies enable rulers to access potential dissidents' private discourses on all levels of electronic and offline communication.[20]

Transformations of political dynamics in authoritarian regimes

We now discuss how digital tools affect the dictator's perpetual agenda. Only when viewed against the backdrop of literature on authoritarianism does it become clear, however, that many of the integral elements of authoritarianism are affected by digitization. If we understand 'political regime' as 'the formal and informal organization of the centre of political power, and of its relations with the broader society'

(Fishman 1990: 428), digital transformations affect not only the 'three pillars' of 'authoritarian stability' (Gerschewski 2013), but important core features of how regimes form, are composed and institutionalize, including state–society relations. Their effects thus transcend incremental enhancements of existing dictatorial ruling strategies and capacities.

This section discusses seven key areas where digitization transforms authoritarianism because of regimes' unprecedented abilities to collect and analyse information about subjects, and to influence the latter's beliefs and behaviour. For each, we provide testable hypotheses on how politics is transformed by the dictatorial use of digital tools. While these areas of transformation are not necessarily exhaustive, they are common fields in research on authoritarianism. Their discussion helps in assessing more precisely on what level and to what extent political transformations occur due to technological innovation, and how this influences the overall face of dictatorship.

1: New elite actors and partially reconfigured regime composition

Operating the new tools requires higher levels of technical expertise from regime agents. Domestically, new 'cyber elites' are already emerging (see also transformation 2, below), while, at least in the short run, regimes also rely on foreign commercial services to install, maintain and operate their tools. Some of the traditional elites' importance will decline because digital technologies increasingly assume their tasks. Simultaneously, the more digitized autocracies become, the more cyber elites will gain in influence. For instance, directors of security services' surveillance directorates, formerly in command of huge bodies of informants, may be marginalized as the collection and real-time analysis of big data are performed by self-learning algorithms, the administration of which the old guard of elites cannot perform due to lack of digital expertise. Fewer and very differently qualified personnel are now needed in extremely sensitive positions, and such new elites may also be recruited internationally (see also transformation 7 below). Agents of digital repression, co-optation and propaganda already occupy a prominent place in newly installed institutions (more below). Beyond such formal positions, elites are also reshuffled in more informal and secret positions. In any case, these reconfigurations in the composition of, and power dynamics within, autocratic elites can impact authoritarian politics in important ways. Changes in the relative importance of some elites and changes in elite circles that can access and control information might impact intra-elite composition and coordination, and possibly create new challenges to the rulers (e.g. principal–agent issues).

So far, little research has examined these changes, nor how they fit into existing theories of autocratic elite coordination, formation or recruitment. It remains for future research to investigate the sociopolitical and economic ramifications of such changes to elite composition/configuration in authoritarian regimes – especially since some major works on authoritarianism view elite coordination and power dynamics as pivotal in understanding the politics of authoritarian regimes (stability).

2: Institution-building and -reconfiguration

Large data-gathering and data-analysing techniques can reduce or erode previous functions of more traditional dictatorial political tools. For instance, public opinion

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

is continuously screened and known by dictators when they employ sophisticated data analysis programs. Rulers then no longer need to rely on elections as a barometer of public opinion, and we concur with Gunitsky (2015: 43) that with a 'potential *substitute* for unfair elections', such institutions lose part of their function.

When autocratic institutions change functions as dictatorships digitize, it represents important institutional shifts. We therefore expect autocracies competent in digital surveillance to rely less on elections for finding out about their population's political preferences. Such losses of function could lead us, prima facie, to assume a decrease in the frequency or importance of elections in authoritarianism, but they also serve purposes other than testing regime popularity.[21]

Digital capabilities can also supplant existing dictatorial tools. Enhanced surveillance capacities enable autocrats, in combination with bot armies and other defamation and control instruments, to better predict voting behaviour. If Cambridge Analytica became infamous for digitally distorting democratic elections, it would be naive to assume that autocrats would not apply similar strategies to influence and control votes at home. The electoral process hence becomes more predictable for authoritarians and yet less promising for oppositional forces. This might motivate autocrats to rely even more on elections for generating legitimacy and could thus lead to an increase in their frequency or centrality. The increasing popularity that pseudo-democratic elements such as referenda enjoy among modern autocrats seems to point in this direction.

Institutional change beyond elections includes, for instance, new political institutions established as reaction to technological change. Examples are the 2013-founded Chinese 'Cyberspace Administration' that reports directly to the president (Polyakova and Meserole 2019: 3), the Iranian 'Cyberspace Supreme Council', established in 2012 and staffed mostly with security personnel (Reporters Without Borders 2020), or the various bodies for supervising new processes of e-governance that most autocracies have recently established, and which are staffed, inter alia, with the above-mentioned new cyber elites. As discussed above, e-governance not only enhances autocrats' 'performance legitimacy' but also enables them to engage in 'imitative institution-building' when they establish democratic-looking façades (Albrecht and Schlumberger 2004). Yet, imitative institution-building might become less important in digital dictatorships. We therefore hypothesize (a) the emergence of new, now functionally necessary dictatorial institutions, and (b) a change in the nature, functions and potentially also shape of existing 'imitative' institutions' that mimic their democratic counterparts.

3: The intension of political rule: reconfigured state–society relations

While the consequences of a new digital public sphere are debated (Schäfer 2016), the distinction between the public and private spheres becomes blurred. Where private activities, preferences and conversations increasingly take place digitally, regime capacities to penetrate private life increase. The more the private takes place online (e.g. via social media or messenger services), the more it becomes at least susceptible to 'publicization', and ultimately part of the public sphere.

The depth to which society can now be digitally penetrated is unprecedented, and the intensity of 'knowing' and, subsequently, manipulating beliefs and

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

behaviour exceeds even what 20th-century dictators could have dreamed of. Big data analyses give incumbents the power of real-time mass surveillance and, simultaneously, of targeting an almost unlimited number of individuals more specifically. This leads to a thorough reconfiguration of state–society relations: whereas rulers remain in opacity, subjects become more transparent than ever. Oppositional activity is often detected in the planning stages before it occurs – because incumbents *know*.[22] In many dictatorships, incumbents now implement tools of digital surveillance to pre-empt open contestation. With digital surveillance perfected, we will hence see fewer mass demonstrations.

Some argue societies would counteract by likewise acquiring digital skills and thus creating new challenges to autocrats (Hobbs and Roberts 2018). Yet, this view fundamentally ignores the qualitative imbalance in power resources between societies and dictators in which the asymmetry between the two allows the latter not only to control but also to determine the digital possibilities of societal forces. While opposition movements do have learning capacities, these invariably depend on the regime-installed hardware to which access is controlled by incumbents, and on the regime's monopoly to control access to software. Ultimately, therefore, opposition is thus much more restricted and has fewer opportunities to coordinate than before digitization. This point has been empirically confirmed in a large-n study by Weidmann and Rød (2019, chs 5 and 6), who call it the 'protest-reducing effect of internet technology' (Weidmann and Rød 2019: 155). It is our framework that explains the causes behind that increasing imbalance.

While it is still too early to predict exactly how contentious politics will further evolve, this is one central theme to understand state–society relations in 21st-century dictatorships. What is certain today is that digital techniques have empowered authoritarian incumbents much more than their societal opponents. While popular movements have been able to make use of digital techniques to mobilize, such opportunities vanish rapidly as authoritarians become more digitally capable than most still were in the 2000s and 2010s when the room for online contention was still large. In the 2019 Hong Kong protests, the Telegram-based organization among participants was highlighted. But it was only in combination with a new type of offline protest tactic ('be like water') that authorities had a hard time in handling protesters. This is just one example of how activities in the online and offline world blend. Such innovative crossings are likely to become more prevalent in the future, as might be opponents' tactical withdrawal into the analogue world when digital surveillance becomes omnipresent (as long as there are physical spaces that are not covered by real-time facial recognition and CCTV). Clandestine acts of resistance then likely outpace open political opposition or visible activism.

4: The reconfiguration of coalitions and micro-steered co-optation

New tools of digital co-optation alter the ways of authoritarian coalition-building. Co-optation of either particularly loyal followers or of would-be opponents has now become much more individualized. Traditionally, different collectivities (i.e. classes, segments or elite groups) are both the building blocks and main beneficiaries of authoritarian coalitions and their welfare provision (Eibl 2020; Slater 2010). E-governance and social credit systems individualize both the criteria for inclusion

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

into authoritarian social pacts and the benefits of social welfare. Instead of including or excluding societal segments, incumbents can target specific individuals based on their (online) behaviour as 'social-credit scores can determine the results of applications for personal loans, jobs, visas, and more' (Qiang 2019: 59). Given this ability to fine-tune inclusion and exclusion independently of group identities, regime coalitions as well as the relationship between different elite segments might look different in the future.

Even basic citizenship rights become contingent on subjects' 'well-behaviour' (theoretical reflections: Heydemann 2020). We expect the widespread use of reward–punishment systems such as China's social credit system to affect the ways authoritarian coalitions evolve and are sustained. For some regimes, such systems will reduce the costs of rule by narrowing down the group of beneficiaries as exclusive benefits (and costs) can be delivered with surgical precision to the intended individual recipient instead of to larger groups. Other regimes might diversify their coalitions to include individuals from different societal segments rather than by co-opting larger groups. This may increase loyalty and leader–elite-cohesion, thus further reducing threats to the regime (see transformation 3 above). We assume that resource-rich authoritarian regimes might tend to keep previous elite coalitions intact whereas resource-poor autocracies might narrow down such coalitions more quickly.

5: The frequency, forms and targeting of repression

With the spread of bots, digital attacks and malware, authoritarian regimes enjoy an unprecedented ability to know about their population, censor information and destroy opponents' digital devices. This allows digitized dictators to fine-tune and target repression. First, the regimes' ability to know enables them to better identify threats and employ repression with surgical precision, as Feldstein (2021) convincingly illustrates. Second, regimes can censor and destroy regime-critical content more easily, more systematically and more precisely. We discussed Bahrain's use of social media bots to censor critics as well as China's Great Firewall. Such measures enable the targeting of specific critical content instead of enacting bans of entire social media, let alone a total internet shutdown (a Syrian routine in the 2000s). Furthermore, as India and South Africa, albeit democracies, demonstrate, regimes are today able to shut down the internet or to throttle the bandwidth in a very targeted manner (Farries 2019: 13), which effectively blocks avenues for opponents' coordination.

The consequences of such repression deserve closer attention. Intuitively, more targeted repression seems to reduce both its undesired side-effects and its costs (Feldstein 2021) and would increase regimes' willingness to repress. Yet, we also noted that autocrats today better pre-empt opponents from gathering and even coordinating. The International Network of Civil Liberties Organizations reports the extent to which the governments of Kenya, Russia and Hungary use digital surveillance to curb protests before they are even called for (Farries 2019: 8) – which in turn helps avoid the large-scale repression that would be necessary if such protests materialized. When domestic mass contention becomes thus less frequent (transformation 3), so does potential international damage to the regimes' legitimacy. Dictators increasingly 'shy away from overt and highly visible forms of coercion

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

and turning to subtler techniques that are less likely to spark outrage and condemnation' (Frantz 2018: 120), and the cause for that might well lie in the vastly increased levels of 'knowing' that allow for more targeted repression, if necessary at all.

6: Legitimacy and informational agnosticism

In the analogue age, readers had a choice between, say, the state's official gazette and alternative newspapers that could deviate from the regime's official narrative within 'accepted lines'. Readers were usually aware of whose voice they were exposed to. Digital tools to influence beliefs fundamentally blur this distinction between pro-regime and regime-critical information sources because non-governmental information channels are systematically infiltrated (Kelly et al. 2013: 4). Information looks as if it is derived from a diversity of sources while in fact it consists of different regime-initiated discourses. For incumbents, it is not necessary to allow only one voice to speak. They just need to sow enough disinformation to make the opposition appear slightly less legitimate than the regime.[23] For example, during the 2011 Bahraini uprising, social media bots retweeted and posted pro-regime narratives without officially belonging to the regime (Jones 2013: 78–79). Even before bots became ubiquitous, Russia initiated and financed private 'brigades' to change online narratives (Polyanskaya et al. 2003). The Chinese regime forges 448 million social media comments a year to 'distract the public and the change the subject' away from controversial political issues (King et al. 2017).

With regimes creating and disseminating their own 'truths' through, among other things, social media, dictators have drastically expanded their capacity not only to obscure the origin of news and narratives, but also to render citizens structurally unable to identify the source of 'information' they consume or to judge its trustworthiness. Thus, confounded subjects cannot know what news to trust nor whether rulers protect or manipulate them. Deeply manipulated rationales of knowing lead to equally distorted rationales of obedience – which might, in turn, transform how the Weberian belief in legitimacy itself is garnered.

Moreover, ignorance about who stands where leaves potential dissidents within masses and elites uncertain about their relative strength, rendering collective action less likely. This is a qualitative break from anything seen in earlier times, and it might become *the* tool to create almost perfect ignorance about truth and falsehood. As psychologists have demonstrated since the 1960s, this pushes subjects not only into a state of ignorance about reality, but into political apathy and carelessness about the origin of the news they are fed. Mutually exclusive narratives translate into a general suspicion against media, even in democracies. Such authoritarian practices intentionally work against the very concepts of truth and reality; among subjects, they create not only an informational gap, but also informational agnosticism. This is particularly frightening because 'access to alternative sources of information' (Dahl 1971: 3) is a core requisite for democratic contestation. Where citizens are unable to discern the very source of their information, they lack the prerequisites of forming an independent opinion. We hypothesize, therefore, that digitized authoritarians will successfully broaden the base of those who buy their narratives and yet more successfully marginalize critics. The decisive point is not whether citizens are convinced of the truthfulness of regime narratives. The

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

uncertainty instilled upon society is enough for most to not engage in searching for truth because 'truth', under these conditions, cannot be known anyway.[24] This enhances the dictator's ability to manipulate beliefs while simultaneously decreasing prospects for democratization.

7: The extension of political rule: the transnational reach of power

Digitized dictatorship changes the features and the scope of political rule, both in its intension (see transformation 3), but also in its extension. The latter becomes clear when we look at what traditionally constituted national borders. All three 'pillars of stability' (Gerschewski 2013) today routinely transgress borders much more quickly and at less cost than ever before, adding a transnational dimension to the transformations discussed under transformations 4 to 6.

A case in point is the remote surveillance of opponents abroad: agents are no longer needed to spy on exiled opposition leaders. The case of London-based Saudi satirist Almasarir exemplifies this.[25] In many cases, this digitally enhanced capacity to know, in turn, enhances the capacity to physically repress in the offline world and instils fear among regime critics. Some question whether this successfully silences all critics (Pan and Siegel 2020; Roberts 2020), but empirics suggest that the existing power gap between dictators and their critics increases to benefit the former (King et al. 2013; see transformation 3 above). Azeri journalist Khadija Ismayilova was secretly filmed in her home and blackmailed with the material before it was spread online, ultimately leading to her arrest (Reporters Without Borders 2018: 10). The unprecedented ability to surveil critics anywhere intimidates exiled opposition. Rwandan deputy Faustin Rukondo, targeted by a WhatsApp Pegasus attack in 2019, felt 'paranoid and scared' (Tidy 2019). We hypothesize that authoritarian regimes, alongside increasing transnational surveillance capacities, also increase their capacities to repress targets abroad.

Digital tools of repression thus enable autocrats to better target and silence even exiled opponents (Dalmasso et al. 2018). Rukondo was not only internationally surveilled, but the same Pegasus malware also destroyed files on his mobile phone (Tidy 2019). Private Russian agencies directly tied to the president orchestrate troll armies that attack targets worldwide, as with Finnish journalist Jessikka Aro or during Emanuel Macron's campaign for the French presidency in 2017 (Reporters Without Borders 2018: 23–24). State-sponsored online harassment and hate speech against critics are also well documented (Michaelsen 2020) and acknowledged by international organizations such as the European Council.

Beyond surveillance and repression, co-optation also increasingly occurs transnationally. One example is the recruitment of international tech experts of questionable ethics, often hired on a one-off basis, but sometimes also lured into long-term contracts with autocracies. Different from the international advisers whom dictators have always had, such experts are located at the most sensitive points of domestic security infrastructures, which could result in ramifications on the inner dynamics of authoritarianism. Furthermore, rulers' efforts at legitimizing their hold on power increasingly target not only a domestic audience, but international ones too. Alongside elaborate disinformation campaigns through traditional state-controlled international media (such as *Russia Today* or *Sputnik*

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

News), new media have been particularly successful in spreading favourable 'news' about autocracies abroad. This allows dictators to paint a positive picture of their regimes to domestic and international audiences alike. The international delegitimization and defamation of rivals and adversaries are closely related. Dictatorial great powers such as Russia perceived the world to be in a state of cyber war about (mis-) information even before the war in Ukraine, aiming at internal and external legitimation (the 'Gerassimov Doctrine'). However absurd the 'news' that troll firms disseminate might seem, they likely find followers who multiply their messages and create echo chambers so that uncertainty about truth is propelled even beyond national borders.

Taken together, then, digitization significantly transforms the political process in various dimensions.[26] Each of these areas awaits more systematic empirical research that we hope to encourage by the discussion and hypotheses presented here. Overall, we can safely state that digitization makes autocracies faster in their responses to threats, quicker and more targeted in both surveillance and repression, and more versatile in the creation of tailor-made 'truths' for targeted audiences – in brief: authoritarianism on steroids. All this points to what Steven Heydemann (2007) called 'authoritarian upgrading'. But the whole can be more than the sum of its components. We are convinced that the combined weight of these transformations amounts to more than just changes in degree. By contrast, we argue that above and beyond the discussed transformations of the political process – that is, in the sphere of politics – we also witness transformations that affect regime type – that is, polity. We conclude this article by suggesting that digitization produces a kind of political rule that, while dictatorial, also differs in important respects from authoritarianism as classically defined.

A technologically induced transformation of authoritarian politics

Condensed from the existing literature on authoritarianism, but in contrast to most contributions on digitized dictatorships, we started our argument from the 'dictator's agenda' in studying dictatorships instead of from the technological side. Proceeding thus enabled us to treat digital innovation in ruling techniques as the intervening variable it is. Technical innovation provides autocrats with new tools – tools they not only embrace but actively develop in order to better pursue their political goals, and which strongly impact on the way autocratic politics work. Thus, while the goals of authoritarianism remain constant, the means by which dictators pursue them are fundamentally transformed in ways that rapidly increase dictators' capabilities of controlling, surveilling and manipulating the attitudes and behaviour of their societies – despite all societal or oppositional efforts to the contrary. This is because resources available to societal forces are to a large extent determined by regimes' exclusive power over hardware and regulations that circumscribe the availability of digital means of resistance available to oppositional forces.

The seven core areas of transformation identified above can be understood as an analytical frame that helps both in locating current and encouraging future research within the broader field of digitized dictatorships, and in identifying areas where future research is particularly desirable. But change might not stop here: the

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

combined impact of these transformations leads to profound changes not only to the process of how authoritarian politics – including politics aimed at authoritarian stability – functions, but in consequence also to the very nature of authoritarianism. Far from a distant techno-sceptical dystopia, the Chinese case demonstrates just how different from authoritarianism as traditionally defined (see Linz 1964: 1975) new, digitized autocracies can already look today. While, for reasons that go beyond the scope of this contribution, we do not share Larry Diamond's (2019) view of a 'postmodern totalitarianism' on the horizon, empirical trends in the direction of a more total than ever control and surveillance are evident. Further research should therefore not only focus on transformations *in* authoritarian politics, but also broaden the view and include the possible transformation *of* authoritarianism as a distinct regime type as well.

Acknowledgements. We would like to thank Erica Frantz, Marlies Glasius, Joseph Wright, Andreas Schedler, Nils Weidmann, Maria Josua, Žilvinas Švedkauskas and Chonlawit Sirikupt for valuable comments on previous versions of the text, and Victoria Wang for great research assistance.

Notes

[1] We distinguish between digitization as the technical process of an electronification of communication, information and control; and digitalization as the processes this technological change triggers on the social, economic and political levels. Digitalization, then, refers to the broader effects caused by an ever-widening use of digital technologies (Urbach and Röglinger 2019). 'Digital technologies' comprise all technologies that produce or process digitized information. They differ qualitatively from analogue technologies in three ways: (1) they are reprogrammable; (2) the information they produce and process are in universally machine-readable formats; and (3) digital technologies are self-referential in their innovativeness, i.e. digital innovations require digital devices (Yoo et al. 2010).

[2] We use dictatorship, like autocracy, as a generic term to refer to any non-democratic political regime. Below, we follow Linz, who defines 'authoritarianism' by four characteristics: (1) limited, non-responsible political pluralism; (2) absence of large-scale political mobilization from above (except in some specific circumstances), with political apathy instead; (3) absence of an elaborate guiding ideology, but with mentalities instead; (4) an exercise of political rule within 'formally ill-defined, but actually quite predictable' limits (see Linz 1975: 264). For an empirical definition of totalitarianism, see Friedrich and Brzezinski (1956).

[3] Obviously, this assumption only approximates reality as humans always pursue more than one goal at any one point in time. But in authoritarianism research, it has proven useful to take the dictator's quest for regime survival and power maintenance as a starting premise.

[4] While authoritarian regimes are not monolithic, and no individual always controls everything, 'dictator' is a placeholder that refers to the regime elite's perspective as a collective actor.

[5] For a good recent overview, see Schlumberger and Schedler (2020).

[6] Our framework encompasses all domestic actors who can pose threats to authoritarian regimes. Throughout this article, we use the term 'subjects' to refer to both societal/mass actors as well as to representatives of the (politically relevant) elites (PRE). For a fuller discussion see note 10.

[7] Some might argue that, logically, beliefs are ahead of behaviour as the former leads to the latter, but for the dictator to organize compliance, the former is much more ambitious and difficult to achieve; we therefore discuss the three goals in the order mentioned above.

[8] While we do acknowledge the importance of the international dimension of digital dictatorship, and while our analytical frame also facilitates future explorations into that dimension, it is beyond the scope of this article to include it systematically here.

[9] What Heydemann refers to as 'upgrading' has brought about incremental change in the past and concerns the invention of new tactics or strategies. In contrast, what we refer to here as qualitative, transformative change involves not only new strategies but also the accessibility and broad employment of new technology and impacts on both regime policies and the very nature of regimes. We also visualize this in the bottom part of Figure 1.

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

10 One actor-centred rational-choice strand of literature (such as, e.g. Acemoglu, Robinson, Bueno de Mesquita, Przeworski or, in the study of dictatorship, Svolik) has modelled contentious actor constellations in dictatorships as a 'dual threat' to leaders: a horizontal threat from politically relevant elites, and a vertical threat from societal actors ('masses'). The assumption then is that leaders would use distinct strategies to counter each. Yet, this modelling of only three actors (leader–elite–masses) seems simultaneously too little differentiated and not encompassing (see also Schedler 2013: 34–35). As indicative evidence suggests, many (if not most) digital strategies of power maintenance such as, e.g. full-range real-time surveillance, are applied similarly to both elites and masses.

However, the main reason why we do not follow this particular actor-centred approach is that such constellations are not the same across all dictatorships. If a regime 'determines who has access to political power, and how those who are in power deal with those who are not', then such constellations by definition cannot be assumed to be uniform across regime types and subtypes, and indeed empirically, they differ in important respects not only across regime subtypes, but also across time, space, motivations, militancy, group identity, coherence etc.

Because our framework aims at applicability to all regime subtypes, we must avoid delving into the meso level of various possible actors, their varying constellations and the respective threats that emanate from them in this contribution. We thus choose to not follow the view of a 'dual threat', but instead build our analytical framework by following Gerschewski's broader approach, which, moreover, allows us also to incorporate structural rather than only actor-related factors.

11 On democratic leaders entertaining similar desires and on authoritarian practices in democracies, see note 14.

12 These three components of the power-maintenance agenda are interrelated and, in part, even endogenous to one another. Nonetheless, for the purpose of this article, we treat them as distinct, non-hierarchized elements of power maintenance.

13 Actors in democracies, too, engage in digitally enabled authoritarian practices (see, e.g. Glasius 2018). But in democracies, control and surveillance are structurally constrained by basic civil liberties (privacy rights), in combination with political guarantees such as an independent judiciary (rule of law). While authoritarian practices in democracies constitute flaws of the system, they are integral to the modus operandi of dictatorships. Consequently, in democracies, scandals such as the one in 2018 with Cambridge Analytica or the NSA in 2013 result in public debates, new legislation for data protection and/or lawsuits.

14 This is particularly visible in face-recognition technology that simultaneously collects and analyses information.

15 Gateways are entry points that connect devices outside a network with devices inside a national network and facilitate their communication.

16 These systems are operated on a provincial level and include private and public operators with varying degrees of sophistication and extent – all ultimate authority to control private sector operations, however, lies with the regime. Other than in Western contexts where Google and other large companies could be said to de facto control access to the data they collect, ultimate 'allocation of values' in places like China is firmly in the hands of the top regime elite, not of any private company. Moreover, it is clear that the Chinese regime is working hard to integrate and streamline hitherto separate systems of assessing individuals' behaviour (Drinhausen and Brussee 2021). This bears fruit, as could be seen, for instance, during the COVID pandemic when police-operated 'talking drones' were used across various provinces to, first, digitally identify, and second, directly address subjects through the drones, telling them to wear face masks or to stay at home (see, e.g. D'Amore 2020).

17 Internet bots repetitively and simultaneously connect to the victim's server and thereby bring down the whole service by exhausting its capacity, as China did against Telegram during the 2019/20 protests in Hong Kong.

18 China, by far the most advanced digital dictatorship with its social credit systems, delineates a conceivable ideal type – and thus is a suitable example when contemplating trends. Note that we do not claim that all dictatorships, including China, are able or willing to fully establish such an ideal type. Still, the ambition to control, surveil and manipulate digitally is present in virtually all dictatorships that experiment with the purchase and development of digital power-maintenance tools. While China highlights the current scope of tools available to the digital dictator, other dictatorships rather install piecemeal digitization and so far focus on specific dimensions they deem particularly important for their own survival. Likely, we will see different 'digital profiles' emerge among the universe of digitizing dictatorships. Our illustrations here stem from across the world to ensure that our framework and conclusions are not based on any particular case.

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

19 Note that this is one of Dahl's 'eight institutional guarantees' in his definition of polyarchy (Dahl 1971: 3).
20 Moreover, as one anonymous reviewer suggested, technological innovation can also bring synergy effects such as in China, where regime-initiated discourse influences belief formation in ways conducive to citizens' willingness to voluntarily provide private information and comply with surveillance policies.
21 On why dictators hold elections when results are known *ex ante*, see, e.g. Gandhi and Przeworski (2006).
22 This does not mean that no errors occur. Apart from human miscalculations, certain types of errors are innate in the digital tools themselves (e.g. misidentification of individuals by recognition software). Yet, such errors become fewer through machine learning in self-optimizing systems.
23 We thank Marlies Glasius for hinting this point to us.
24 This psychological effect is long known. Saloojee and Dagli (2000: 903–4), for instance, report on collusion within the US tobacco industry in the 1950s when reports about smoking as a health hazard emerged. In an internal memo, the colluders strategized, 'doubt is our product. Spread doubt over strong scientific evidence and the public won't know what to believe …. It's enough to foster and perpetuate the illusion of controversy in order to muddy the waters.'
25 Saudi security forces had hacked Almasarir's phone with the Pegasus spyware. For similar cases, see Middle East Monitor (2019).
26 These seven areas can interact: new or altered forms of repression potentiate the transnational reach of authoritarianism; new cyber elites can dilute or highlight the importance of different security agencies (institutions), and reconfigured regime coalitions surely affect state–society relations and contentious politics, which in turn impacts on forms of repression, and so on. Digital technologies' ability to simultaneously serve several elements of dictators' perpetual agenda gives dictators an edge in steering these interactions to their favour.

References

Albrecht H and Schlumberger O (2004) Waiting for Godot: Regime Change without Democratization in the Middle East. *International Political Science Review* **25**(4), 371–392. https://doi.org/10.1177/0192512104045085.

Arthur C (2012) China Tightens 'Great Firewall' Internet Control with New Technology. *Guardian*, 14 December, www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control.

Boehme-Neßler V (2020) *Digitizing Democracy: On Reinventing Democracy in the Digital Era – A Legal, Political and Psychological Perspective*. New York: Springer International Publishing.

Cannings R et al. (2017) An Investigation of Chrysaor Malware on Android. *Google Online Security* blog, 3 April, https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html.

Dahl RA (1971) *Polyarchy*. London: Yale University Press.

Dalmasso E, et al. (2018) Intervention: Extraterritorial Authoritarian Power. *Political Geography* **64**, 95–104. https://doi.org/10.1016/j.polgeo.2017.07.003.

D'Amore R (2020) 'Yes, This Drone is Speaking to You': How China Is Enforcing Coronavirus Rules. *Global News*, 11 February, https://globalnews.ca/news/6535353/china-coronavirus-drones-quarantine/.

Dans E (2018) The Kremlin vs. Telegram: What's Really Going On with the Messaging Service in Russia? *Forbes*, 19 April, www.forbes.com/sites/enriquedans/2018/04/19/the-kremlin-vs-telegram-whats-really-going-on-with-the-messaging-service-in-russia/.

Data Justice Lab (2020) Data Harm Record. https://datajusticelab.org/data-harm-record/.

Diamond L (2019) The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism. *Journal of Democracy* **30**(1), 20–24. https://doi.org/10.1353/jod.2019.0001.

Drinhausen K and Brussee V (2021) China's Social Credit System in 2021 – From Fragmentation towards Integration. *China Monitor Report*. Mercator Institute for China Studies (MERICS), https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration.

Eibl F (2020) *Social Dictatorships: The Political Economy of the Welfare State in the Middle East and North Africa*. Oxford: Oxford University Press.

Facebook (2019) Facebook Transparency – Jordan – Requests for User Data. Meta Transparency Center, https://transparency.facebook.com/government-data-requests/country/JO/jan-jun-2019.

Farries E (2019) *Spying on Dissent: Surveillance Technologies and Protest*. Report, Geneva: International Network of Civil Liberties Organizations (INCLO), https://policehumanrightsresources.org/spying-on-dissent-surveillance-technologies-and-protest.

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

Feldstein S (2021) *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. New York: Oxford University Press.

Fishman RM (1990) Rethinking State and Regime: Southern Europe's Transition to Democracy. *World Politics* **42**(3), 422–440. https://doi.org/10.2307/2010418.

Frantz E (2018) *Authoritarianism: What Everyone Needs to Know*. Oxford: Oxford University Press.

Frantz E, Kendall-Taylor A and Wright J (2020) Digital Repression in Autocracies. *Users Working Paper Series* 2020:27. University of Gothenburg: V-Dem Institute, https://162.242.252.160/media/filer_public/18/d8/18d8fc9b-3ff3-44d6-a328-799dc0132043/digital-repression17mar.pdf.

Friedrich CJ and Brzezinski ZK (1956) *Totalitarian Dictatorship and Autocracy*. Cambridge, MA: Harvard University Press.

Gandhi J and Przeworski A (2006) Cooperation, Cooptation, and Rebellion under Dictatorships. *Economics and Politics* **18**(1), 1–26. https://doi.org/10.1111/j.1468-0343.2006.00160.x.

Gerschewski J (2013) The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes. *Democratization* **20**(1), 13–38. https://doi.org/10.1080/13510347.2013.738860.

Gil de Zúñiga H et al. (2010) Digital Democracy: Reimagining Pathways to Political Participation. *Journal of Information Technology & Politics* **7**(1), 36–51. https://doi.org/10.1080/19331680903316742.

Glasius M (2018) What Authoritarianism Is … and Is Not: A Practice Perspective. *International Affairs* **94** (3), 515–533. https://doi.org/10.1093/ia/iiy060.

Gunitsky S (2015) Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. *Perspectives on Politics* **13**(1), 42–54. https://doi.org/10.1017/S1537592714003120.

Guriev S and Treisman D (2019) Informational Autocrats. *Journal of Economic Perspectives* **33**(4), 100–127. https://doi.org/10.1257/jep.33.4.100.

Heydemann S (2007) Upgrading Authoritarianism in the Arab World. *Analysis Paper* 13. Washington: Sabian Center for Middle East Policy at the Brookings Institution, www.brookings.edu/research/upgrading-authoritarianism-in-the-arab-world/.

Heydemann S (2020) Rethinking Social Contracts in the MENA Region: Economic Governance, Contingent Citizenship, and State–Society Relations after the Arab Uprisings. *World Development* **135,** 105019. https://doi.org/10.1016/j.worlddev.2020.

Hindman MS (2009) *The Myth of Digital Democracy*. Princeton: Princeton University Press.

Hobbs WR and Roberts ME (2018) How Sudden Censorship Can Increase Access to Information. *American Political Science Review* **112**(3), 621–636. https://doi.org/10.1017/S0003055418000084.

Howard PN and Hussain MM (2011) The Role of Digital Media. *Journal of Democracy* **22**(3), 35–48. https://doi.org/10.1353/jod.2011.0041.

Jones MO (2013) Social Media, Surveillance and Social Control in the Bahrain Uprising. *Westminster Papers in Communication and Culture* **9**(2), 68–92. https://doi.org/10.16997/wpcc.167.

Jones MO (2019) Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis. *International Journal of Communication* **13**(2019), 1389–1415.

Jones MO (2022) *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. London: Hurst Publishers.

Kelly S et al. (2013) Freedom on the Net 2013: A Global Assessment of Internet and Digital Media. Freedom House Report, https://freedomhouse.org/report/freedom-net/2013/despite-pushback-internet-freedom-deteriorates.

Kendall-Taylor A, Frantz E and Wright J (2020) The Digital Dictators: How Technology Strengthens Autocracy. *Foreign Affairs*, March/April, www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

Kenyon M (2019) Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes. *Citizen Lab*, 1 April, https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes.

Keremoğlu E and Weidmann NB (2020) How Dictators Control the Internet: A Review Essay. *Comparative Political Studies* **53**(10–11), 1690–1703. https://doi.org/10.1177/0010414020912278.

King G, Pan J and Roberts ME (2013) How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review* **107**(2), 326–343. https://doi.org/10.1017/S0003055413000014.

King G, Pan J and Roberts ME (2017) How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review* **111**(3), 484–501. https://doi.org/10.1017/S0003055417000144.

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

Kostka G and Antoine L (2020) Fostering Model Citizenship: Behavioral Responses to China's Emerging Social Credit Systems. *Policy & Internet* **12**(3), 256–289. https://doi.org/10.1002/poi3.213.

Lewis JA (2014) Reference Note on Russian Communications Surveillance. *Center for Strategic & International Studies*, 18 April, www.csis.org/analysis/reference-note-russian-communications-surveillance.

Linz J (1964) An Authoritarian Regime: Spain. In Allardt E and Littunen Y (eds), *Cleavages, Ideologies and Party Systems: Contributions to Comparative Political Sociology*. Helsinki: Academic Bookstore, pp. 291–341.

Linz J (1975) Totalitarianism and Authoritarian Regimes. In Polsby NW and Greenstein F (eds), *Handbook of Political Science*. Reading: Addison-Wesley, pp. 291–341.

Maerz SF (2016) The Electronic Face of Authoritarianism: E-Government as a Tool for Gaining Legitimacy in Competitive and Non-Competitive Regimes. *Government Information Quarterly* **33**(4), 727–735. http://doi.org/10.1016/j.giq.2016.08.008.

Michaelsen M (2020) The Digital Transnational Repression Toolkit, and Its Silencing Effects. Freedom House Special Report, https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.

Middle East Monitor (2019) Spyware Developed in Israel Used by Saudis to Hack London-Based Dissident. 29 May, www.middleeastmonitor.com/20190529-spyware-developed-in-israel-used-by-saudis-to-hack-london-based-dissident/.

Mozilla (2019) Mozilla Takes Action to Protect Users in Kazakhstan. *Mozilla* blog, 21 August, https://blog.mozilla.org/blog/2019/08/21/mozilla-takes-action-to-protect-users-in-kazakhstan.

Oxford Internet Institute (2021) Social Media Manipulation by Political Actors Now an Industrial Scale Problem Prevalent in over 80 Countries – Annual Oxford Report. https://www.oii.ox.ac.uk/news-events/news/social-media-manipulation-by-political-actors-now-an-industrial-scale-problem-prevalent-in-over-80-countries-annual-oxford-report.

Pan J and Siegel AA (2020) How Saudi Crackdowns Fail to Silence Online Dissent. *American Political Science Review* **114**(1), 109–125. https://doi.org/10.1017/S0003055419000650.

Polyakova A and Meserole C (2019)Exporting Digital Authoritarianism: The Russian and Chinese Models. Policy brief, 27 August. Washington, DC: Brookings Institution. www.brookings.edu/research/exporting-digital-authoritarianism/

Polyanskaya A, Krivov A and Lomko I (2003) Big Brother's Virtual Eye – A Research Approach. *Vestnik Online* **9**(320). https://web.archive.org/web/20191219182655/http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm.

Qiang X (2019) President XI's Surveillance State. *Journal of Democracy* **30**(1), 53–67. https://doi.org/10.1353/jod.2019.0004.

Reporters Without Borders (2018) *Online Harassment of Journalists – Attack of the Trolls*. Report, Paris: Reporters sans frontières, https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf.

Reporters Without Borders (2020) RSF Unveils 20/2020 List of Press Freedom's Digital Predators. *Reporters Without Borders*, 21 March, https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators.

Roberts ME (2020) Resilience to Online Censorship. *Annual Review of Political Science* **23**, 401–419. https://doi.org/10.1146/annurev-polisci-050718-032837.

Rød EG and Weidmann NB (2015) Empowering Activists or Autocrats? The Internet in Authoritarian Regimes. *Journal of Peace Research* **52**(3), 338–351. https://doi.org/10.1177/0022343314555782.

Saloojee Y and Dagli E (2000) Tobacco Industry Tactics for Resisting Public Policy on Health. *Bulletin of the World Health Organization* **78**(7), 902–910.

Schäfer MS (2016) Digital Public Sphere. In Mazzoleni G et al. (eds), *The International Encyclopedia of Political Communication*. Chichester: Wiley, pp. 322–328.

Schedler A (2013) *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. Oxford: Oxford University Press.

Schlumberger O and Schedler T (2020) Authoritarianism and Authoritarianization. In Badie B, Morlino L and Berg-Schlosser D (eds), *The SAGE Handbook of Political Science, Vol. 2, Comparative Politics*. London and Thousand Oaks, CA: Sage, pp. 712–729.

Slater D (2010) *Ordering Power: Contentious Politics and Authoritarian Leviathans in Southeast Asia*. New York: Cambridge University Press.

Tidy J (2019) I was a Victim of the WhatsApp Hack. *BBC News*, 31 October, www.bbc.com/news/technology-50249859.

https://doi.org/10.1017/gov.2023.20 Published online by Cambridge University Press

Tsourapas G (2020) Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics. *International Studies Review* **23**(3), 616–644. https://doi.org/10.1093/isr/viaa061.

Urbach N and Röglinger M (2019) Introduction to Digitalization Cases: How Organizations Rethink Their Business for the Digital Age. In Urbach N and Röglinger M (eds), *Digitalization Cases*. New York: Springer International Publishing, pp. 1–12.

Weidmann N and Rød EG (2019) *The Internet and Political Protest in Autocracies*. Oxford: Oxford University Press.

Xu X (2020) To Repress or to Co-Opt? Authoritarian Control in the Age of Digital Surveillance. *American Journal of Political Science* **65**(2), 309–325. https://doi.org/10.1111/ajps.12514.

Xu X, Kostka G and Cao X (2022) Information Control and Public Support for Social Credit Systems in China. *Journal of Politics* **84**(4), 2231–2245. https://doi.org/10.17169/REFUBIUM-36075.

Yoo Y, Henfridsson O and Lyytinen K (2010) Research Commentary – The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research. *Information Systems Research* **21**(4), 724–735. https://doi.org/10.1287/isre.1100.0322.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Cite this article: Schlumberger O, Edel M, Maati A, Saglam K (2023). How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship. *Government and Opposition: An International Journal of Comparative Politics* 1–23. https://doi.org/10.1017/gov.2023.20