Network Topology Facilitates Internet Traffic Control in Autocracies

Eda Keremoğlu[1*], Nils B. Weidmann[1],
Alexander Gamero-Garrido[2], Esteban Carisimo[3],
Alberto Dainotti[4], Alex C. Snoeren[5]

[1]Department of Politics and Public Administration, University of Konstanz,
Universitätsstr. 10, 78457 Konstanz, Germany

[2]Khoury College of Computer Sciences, Northeastern University
360 Huntington Ave, Boston, MA 02115, United States

[3]Department of Computer Science, Northwestern University
2233 Tech Drive, Evanston, IL 60208, United States

[4]School of Computer Science, Georgia Institute of Technology
266 Ferst Dr., Atlanta, GA 30332, United States

[5]Department of Computer Science and Engineering, University of California San Diego
9500 Gilman Drive, La Jolla, CA 92093, United States

[*]To whom correspondence should be addressed:
E-mail: eda.keremoglu-waibler@uni-konstanz.de

Abstract

Recent years have seen an increase in governmental interference in digital communication. Most research on this topic has focused on the application level, studying how content is manipulated or removed on websites, blogs or social media. However, in order for governments to obtain and maintain control of digital data flows, they need to secure access to the network infrastructure at the level of Internet service providers. In this paper, we study how the network topology of the Internet varies across different political environments, distinguishing between control at the level of individual Internet users (access) and at a higher level in the hierarchy of network carriers (transit). Using a novel method to estimate the structure of the Internet from network measurements, we show that in autocratic countries, state-owned (rather than privately-owned) providers have a markedly higher degree of control over transit networks. We also show that state-owned Internet providers often provide Internet access abroad, with a clear focus on other autocratic countries. Together, these results suggest that in autocracies, the network infrastructure is organized in a way that is more susceptible to the monitoring and manipulation of Internet data flows by state-owned providers both domestically and abroad.

Significance Statement

Most research on autocratic control of the digital information environment has focused on social media and website content. However, information control is more effective when governments can influence how data is transmitted over the underlying network infrastructure. Our study investigates how this infrastructure is set up in autocracies and democracies, and which role government-owned Internet providers play. We find that first, in autocratic countries, government-owned providers retain a much more central role as domestic *transit* carriers, which relay data flows from the country to the global Internet. Second, in many autocracies, Internet *access* is provided by state-owned providers from other autocratic countries, which illustrates international patterns of collaboration between these countries.

Introduction

On April 30, 2022, several weeks after the Russian invasion of Ukraine, the Kherson district in Eastern Ukraine experienced a complete Internet shutdown. When service returned a day later, Internet traffic was routed through Rostelecom, Russia's main and state-owned Internet provider (*1*). This incident is only one of the latest in a series of moves to make Russian-occupied areas in Ukraine part of the Russian Internet (*2*). It illustrates that governmental control over Internet traffic flows remains a fundamental concern in particular for autocratic regimes, presumably to retain opportunities to interfere with digital communication (*3*).

This governmental interference can happen in different ways (*4*). The blocking of access to particular websites (*5*) or even the shutdown of the entire domestic Internet (*6, 7*) constitute extreme forms of Internet control; more subtle techniques include censorship of content deemed unacceptable (*8*) or the spread of misinformation (*9*). For most of these tactics, close collaboration with Internet providers is necessary. Existing research has revealed much about these observable manifestations of governmental interference. So far, however, we know little about whether the underlying Internet topology in autocracies is set up to facilitate governmental incursions in cyberspace. This article leverages new data to study how Internet topology differs between autocracies and democracies. In particular, we focus on the role of state-owned Internet providers, which can be an effective way for governments to influence and control communication flows on the domestic Internet, but also abroad.

Two groups of networks in the Internet infrastructure play a key role in carrying traffic: *(i)* access providers and *(ii)* transit and backbone providers. An *access* network connects individuals to the Internet at large, typically in the form of fixed broadband or high-speed cellular networks. *Transit* providers are responsible for connecting customer access networks to the rest of the Internet; some transit providers are rather large and serve as the "core" or backbone of the Internet, including so-called tier-1 providers. While access networks are a critical surveillance point, the structure of transit networks underpinning the modern Internet may be equally consequential in determining the exposure to interference in a country's traffic. Therefore, our focus is not solely on the access networks, but on end-to-end infrastructure. In all these types of networks, governments' engagement in the Internet service business would give them direct capabilities to observe and tamper with Internet traffic. In fact, state involvement in service provision is frequent, with governments owning majority stakes in domestic Internet providers in 123 countries globally (*10*). However, what is their influence on Internet traffic?

Results

In a first analysis, we examine the influence of domestic providers across democracies and autocracies. Providers keep records of users or households, which allows for a simple matching of (possibly suspicious) data traffic to individuals. Therefore, we would expect control over *access* providers to be particularly important for autocratic governments. To measure the influence these access providers have on domestic traffic, we use the share of domestic IP addresses owned by the respective provider (*11*). We combine these data with a second dataset by (*10*) to identify state-owned providers.

In Figure 1 (Panel A), we plot the relative influence of domestic access providers across different regime types. The plot shows that counter to common expectations, the type of political regime is not necessarily a predictor of the state's monopoly of the address space. For instance, Uruguay and Cuba (which have regimes classified as democracy and autocracy, respectively) both have state-sanctioned monopolies (ANTEL and ETECSA). Regression models controlling for potential confounders confirm this (see Section 4.1 in the Supporting Information). This analysis shows that there is no difference in the fraction of address space controlled by state and non-state providers in autocracies while in democracies, state-owned providers are significantly less involved in access provision (Figure 1, Panel B). In Section 5 in the Supporting Information, we check that these results are robust to the use of alternative democracy indicators, a reduced sample and a different assignment of providers to countries.

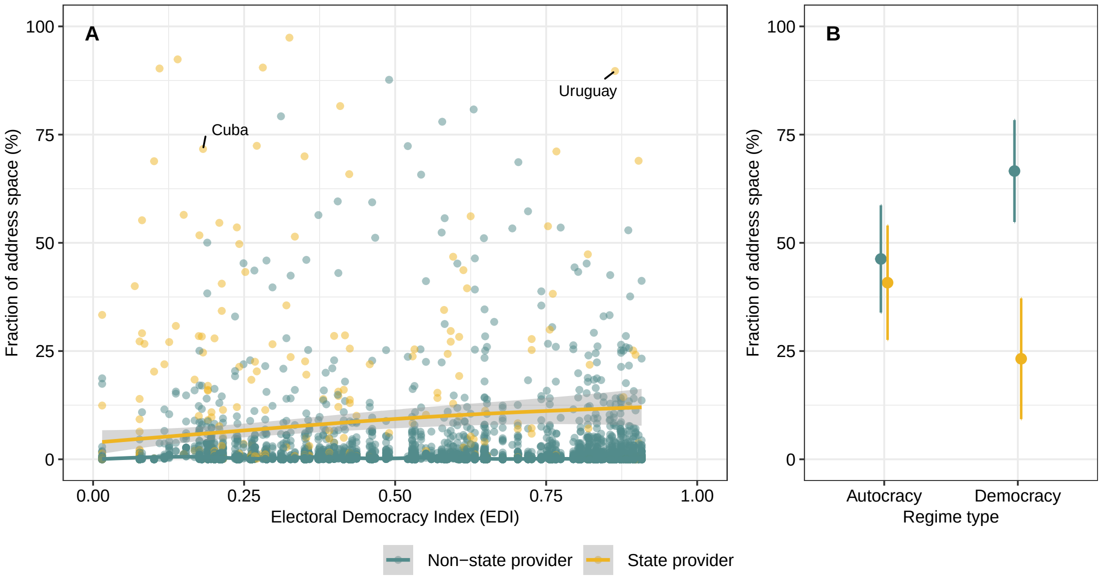

Figure 1: **A.** Fraction of address space serviced by individual domestic state (yellow) vs. non-state providers (green), for non-democratic (low values of the Electoral Democracy Index, left) and democratic countries (right). **B.** Predicted fraction of address space serviced by all domestic state vs. non-state providers based on regression results in Section 4.1 in the Supporting Information (Model 4). Binary regime type indicator derived from the Electoral Democracy Index (*12*).

An alternative, and likely more efficient, way to monitor and interfere with Internet traffic is to control data traffic at the level of *transit* providers. For governments attempting to regulate digital flows of information, controlling the underlying infrastructure as a transit provider can vastly expand the potential to control the functionality and content of online communication. As transit networks are often unaccountable to consumers, they create opportunities for government surveillance and censorship without facing political backlash. Further, transit networks can serve multiple access networks (both fixed and wireless) simultaneously, allowing for the creation of a centralized observation or manipulation point. We measure the degree to which state-owned transit providers influence transit flows using a new dataset compiled by (*13*). The dataset improves on earlier attempts (*14*) by quantifying the capabilities of a transit network to observe or selectively tamper with a country's inbound traffic. Our analyses of transit influence comprise a sample of 75 countries. We provide more details on the sample of countries and the data generation, and assess possible sampling bias in the Supporting Information.

Figure 2 (Panel A) plots the transit influence of domestic providers across the range of democracies and autocracies. Two autocracies, Cameroon and Uzbekistan, operate highly influential and state-owned transit networks: *Camtel* and *Uzbektelekom*. These operators provide international connectivity to a significant fraction of their respective country's users. In general, compared to other (non-state) domestic transit providers, the influence of state-owned providers is particularly high in autocracies (Panel A, left), while it decreases in the democratic countries in the sample (Panel A, right). A statistical analysis with different controls confirms this result (Figure 2, Panel B): In autocracies, state-owned domestic providers have a much higher combined influence on domestic Internet traffic as compared to non-state providers, a difference we do not see in democracies. These analyses suggest that authoritarian governments maintain a high level of control over the domestic Internet traffic not as access providers, but rather as transit traffic carriers.

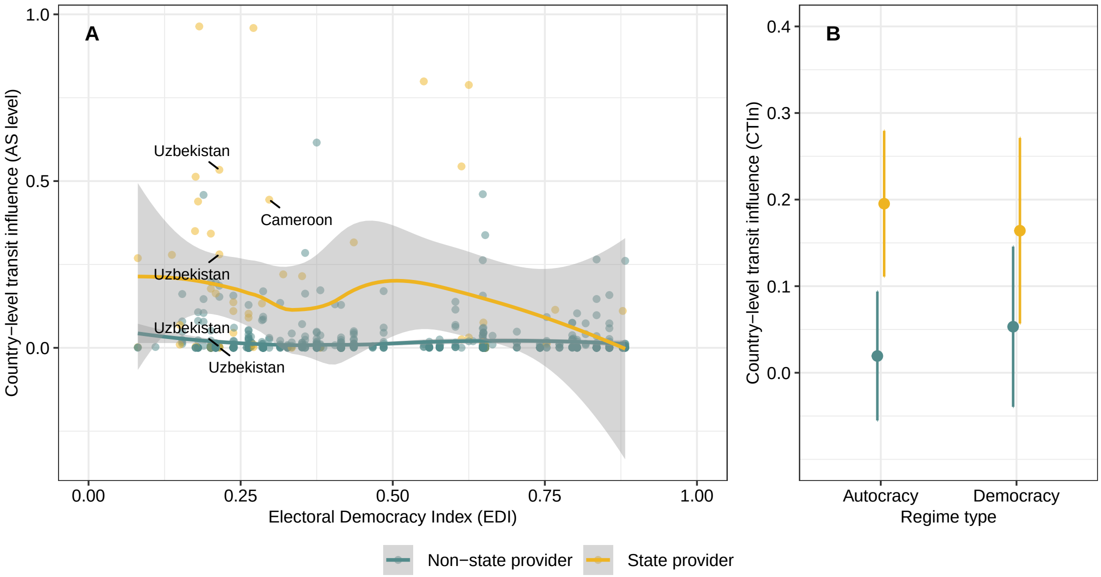

Figure 2: **A.** Country-level transit influence (CTI) of individual domestic state (yellow) vs. non-state providers (green), for non-democratic (low values of the Electoral Democracy Index, left) and democratic countries (right). CTI estimates the relative prevalence of a particular network on Internet routes serving a country and ranges from 0 to 1, with higher values denoting higher prevalence on routes that reach a higher number of IP addresses. **B.** Predicted average country-level transit influence (CTIn) of domestic state vs. non-state providers in democratic and non-democratic countries, based on regression results in Section 4.2 in the Supporting Information (Model 4). CTIn is the combined transit influence, ranging from 0 to 1, of the group of all individual state-owned vs. non-state providers. Binary regime type indicator derived from the Electoral Democracy Index (*12*). Robustness tests for this analysis provided in Section 5 in the Supporting Information.

Our analysis so far has focused only on the domestic influence of Internet providers. However, many providers operate internationally. While their influence at the transit level is negligible (in our sample, the country-level median transit influence is only 0.0006), in many countries, foreign access providers control a significant share of the

Internet access (global average: 25.7%, autocracies: 27.5%, democracies: 24%). These providers have considerable control over Internet traffic as a form of international influence. We therefore focus on access service provision at the level of individual Internet users in the subsequent analyses.

In Figure 3 (Panel A), we visualize the extent to which state-owned providers control access abroad, distinguishing between the different regime types *(i)* where these providers come from (x-axis) and *(ii)* where they operate (y-axis). The plot shows that the operation of state-owned providers from autocratic countries concentrates largely on other autocracies (most of the dots cluster at the left bottom), where these providers are highly influential (thus the larger dots). The United Arab Emirates is a case in point. Three of its state-owned providers operate in Gabon, Mauritania and Morocco, respectively, where the share of access they control is high, ranging from 50 to 67%. Using again regression analysis to back up these descriptive results (Figure 3, Panel B), we confirm that foreign access providers operating in autocracies are almost exclusively located in other autocratic countries. This shows that the international operation of access providers follows a political logic. State-owned providers from some autocratic countries are highly influential in other autocracies, thus creating clusters of autocratic cooperation in the Internet infrastructure.

For pervasive and effective use of Internet communication, it is necessary that governments maintain control over data flows on the Internet, independently of what service or application they are used for. In this paper, we have documented considerable differences in the topology of the Internet infrastructure across democratic and autocratic countries. Using a new method to estimate the influence of Internet providers on the data traffic between users and the global Internet, we have shown that in particular in autocratic countries, the Internet infrastructure is set up such that domestic state-owned

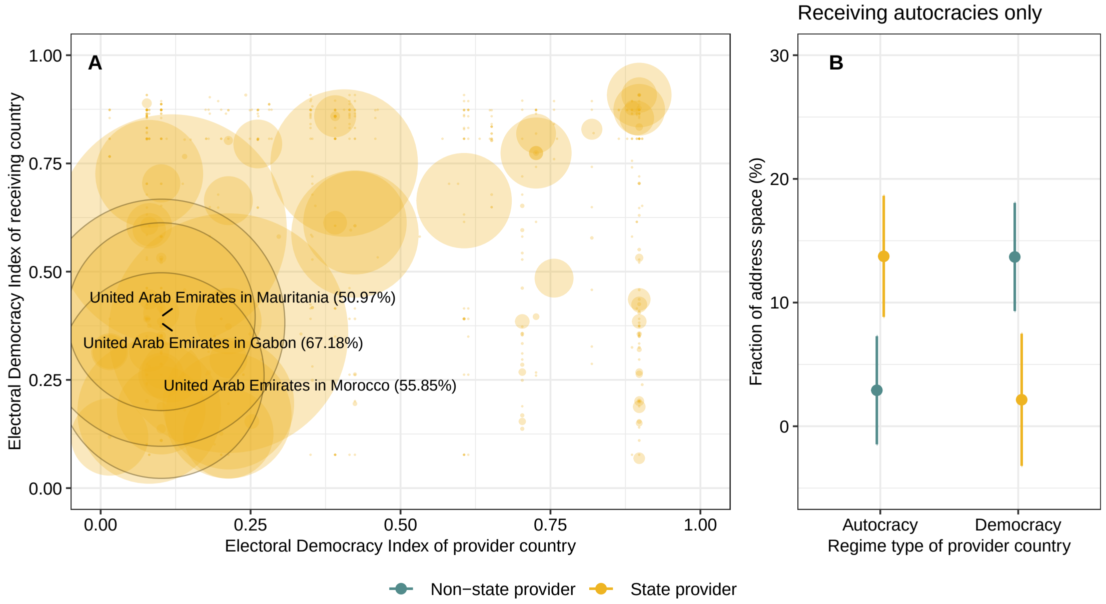

Figure 3: **A.** Address space serviced by individual state-owned access providers from democratic and non-democratic countries (x-axis), ordered by the level of democracy of the country where the service is provided (y-axis). The size of yellow dots represents the share of address space serviced by individual providers. **B.** Predicted aggregate address space originated by all state (yellow) vs. non-state (green) access providers in other autocracies only. Figure based on regression results in Section 4.3 in the Supporting Information (Model 4). Binary regime type indicator derived from the Electoral Democracy Index (*12*). Robustness tests in Section 5 in the Supporting Information.

Internet providers retain a much greater level of control over transit Internet traffic. These features of the network topology can vastly expand the opportunities for non-democratic governments to monitor sensitive information, censor critical content, and disrupt digital communication domestically. Our results also reveal increasing potential of governmental Internet control across state borders. While democracies and autocracies rely on foreign access providers to a similar extent, we find that many state-owned providers from autocratic countries operate preferably in other autocratic countries, thus creating clusters of technological cooperation between non-democratic countries.

Discussion

Our study has important implications for research and ICT policy. First, to gain a better understanding of the political role of the internet, researchers need to take into account the network topology and different ways in which service providers operate in it. More sophisticated, less observable means of potential influence may work even more to the advantage of governments to avert threats to their rule during liberation struggles (*15*). Along these lines, existing work on digital interference at the application layer needs to be supplemented with analyses of the underlying network topology, to better understand who can control (and potentially manipulate) the data traffic these applications are based on. Second, while international providers from democratic states need to be aware of their political impact and assess their abilities to influence traffic in non-democratic states, our results also show that their influence may be limited. As our results have shown, we see a close technological cooperation evolve between autocratic countries at the level of Internet service provision. With state-owned autocratic providers operating in other autocratic countries, potentially differing standards of privacy and anonymity can be avoided, thus sustaining autocratic rule through international partnerships.

Nevertheless, our focus on state ownership only addresses one aspect of an autocratic government's potential to control the digital information environment. In addition to the direct means we assess in our study, governments exert considerable control also over private firms that operate under the state's jurisdiction, which provides them with additional, indirect means of interfering with network traffic (*16*). Focusing on China, research has shown that the political environment is an important factor to consider when market dynamics and the location of firms shape how autocrats exert influence via private domestic firms. Following (*17*), this could make customers serviced by those providers still vulnerable to influence. China is not an outlier; requiring non-state providers to comply with repressive governmental regulations is a common practice also in many other autocracies, such as Russia, Saudi Arabia or the UAE (*16*). As a result, our analysis that focuses on ownership as a direct means of control produces a conservative estimate of the extent to which states can interfere with digital communication, which in reality may be more severe.

Acknowledgements

Funding: Eda Keremoğlu and Nils B. Weidmann acknowledge financial support from the German Research Foundation DFG (Project #402127652). Alexander Gamero-Garrido and Alberto Dainotti were partially supported by National Science Foundation (NSF) grants CNS-1705024 and CNS-2202288. Alexander Gamero-Garrido was supported in part by a Northeastern Future Faculty Fellowship and a Ford Foundation Postdoctoral Fellowship. Alexander Gamero-Garrido and Alex C. Snoeren acknowledge separate support from the National Science Foundation (NSF) through grant CNS-1629973. The authors do not have any real or apparent conflicts of interest. **Author contributions:** E.K.: Conceptualization of the study and execution of the analyses, creation of the visualizations, writing, editing. N.B.W.: Conceptualization of the study, writing, editing. A.G.: Generation of the transit influence estimates, writing. E.C.: Collection of the AS ownership data, writing. A.D.: Editing, commenting. A.C.S.: Commenting. **Competing interests:** The authors declare no competing interests. **Data and materials:** The data and R code required to replicate the results of the statistical analyses are available at https://doi.org/10.7910/DVN/59BX4J.

References and Notes

1. A. Satariano, S. Reinhard, How Russia took over Ukraine's Internet in occupied territories, New York Times (2022). August 9. Available at `https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html`.

2. R. Fontugne, K. Ermoshina, E. Aben, *2020 IFIP Networking Conference (Networking)* (IEEE, 2020), pp. 809–814.

3. H. V. Milner, *Comparative Political Studies* **39**, 176 (2006).

4. E. Keremoğlu, N. B. Weidmann, *Comparative Political Studies* **53**, 1690 (2020).

5. W. R. Hobbs, M. E. Roberts, *American Political Science Review* **112**, 621 (2018).

6. A. R. Gohdes, *American Journal of Political Science* **64**, 488 (2020).

7. T. Freyburg, L. Garbe, *International Journal of Communication* **12**, 3896 (2018).

8. G. King, J. Pan, M. E. Roberts, *American Political Science Review* **107**, 326 (2013).

9. D. Freelon, C. Wells, *Political Communication* **37**, 145 (2020).

10. E. Carisimo, A. Gamero-Garrido, A. C. Snoeren, A. Dainotti, *Proceedings of the 21st ACM Internet Measurement Conference*, IMC '21 (Association for Computing Machinery, New York, NY, USA, 2021), pp. 687–702.

11. A. Dainotti, *et al.*, *IEEE/ACM Transactions on Networking* **22**, 1964 (2014).

12. M. Coppedge, *et al.*, *V-Dem [Country–Year/Country–Date] Dataset v12*, Varieties of Democracy (V-Dem) Project, https://doi.org/10.23696/vdemds22 (2022).

13. A. Gamero-Garrido, *et al.*, *International Conference on Passive and Active Network Measurement* (Springer, 2022), pp. 645–674.

14. T. Freyburg, L. Garbe, V. Wavre, *The Review of International Organizations* (2022). DOI: 10.1007/s11558-022-09483-z.

15. J. Earl, T. V. Maher, J. Pan, *Science Advances* **8**, eabl8198 (2022).

16. R. Deibert, *Journal of Democracy* **26**, 64 (2015).

17. J. Pan, *Problems of Post-Communism* **64**, 167 (2017).

18. RouteViews (2019). Available at `http://www.routeviews.org/routeviews/`.

19. RIPE Routing Information Service (RIS) (2019). Available at `https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris`.

20. Netacuity (2020). Available at `http://info.digitalelement.com/`.

21. RIR Delegation Files (2019). Available at `https://ftp.ripe.net/pub/stats/ripencc/`.

22. The World Factbook. Available at `https://www.cia.gov/the-world-factbook/field/internet-users/country-comparison`.

23. CAIDA AS-Relationships (2019). Available at `http://data.caida.org/datasets/as-relationships/`.

24. M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, K. Claffy, *ACM IMC* (2013).

25. A. Dhamdhere, C. Dovrolis, *ACM Internet Measurement Conference (IMC)* (2008).

26. E. Agbaraji, F. Opara, M. Aririguzo, *IJAET* **2**, 315 (2012).

27. I. Livadariu, A. Elmokashfi, A. Dhamdhere, *e-Infrastructure and e-Services for Developing Countries*, V. Odumuyiwa, O. Adegboyega, C. Uwadia, eds. (Springer International Publishing, Cham, 2018), pp. 345–351.

28. S. D. P. Affairs, Statistics and trends: Ipv6 deployment in latin america and the caribbean 2016-2020 (2021). Available at `https://www.lacnic.net/`

innovaportal/file/3052/1/estadisticas-y-tendencias-el-despliegue-de-ipv6-en-lac-2016-2020-en.pdf.

29. A. Lodhi, N. Larson, A. Dhamdhere, C. Dovrolis, k. claffy, *ACM CCR* (2014).

30. A. Dainotti, *et al.*, *IEEE Journal on Selected Areas in Communications* **34**, 1862 (2016).

31. B. van Dijk, Orbis Overview (2014). Available at https://www.bvdinfo.com/en-us/our-products/data/international/orbis.

32. International Monetary Fund, State-owned enterprises: The Other Government (2020). Available at https://www.imf.org/~/media/Files/Publications/fiscal-monitor/2020/April/English/ch3.ashx.

33. A. Lührmann, M. Tannenberg, S. I. Lindberg, *Politics and Governance* **6**, 60 (2018).

34. D. Kaufmann, A. Kraay, M. Mastruzzi, *Hague Journal on the Rule of Law* **3**, 220 (2011).

35. World Bank, World Development Indicators. Available at https://data.worldbank.org.

36. United Nations Statistics Division, Standard country or area codes for statistical use (m49) (2022). Available at https://unstats.un.org/unsd/methodology/m49.

37. M. G. Marshall, T. R. Gurr, *Polity 5. Political Regime Characteristics and Transitions, 1800-2018. Dataset Users' Manual*, Center for Systemic Peace (2020).

Supporting Information

Supporting Text

Figs. S1 to S5

Tables S1 to S11