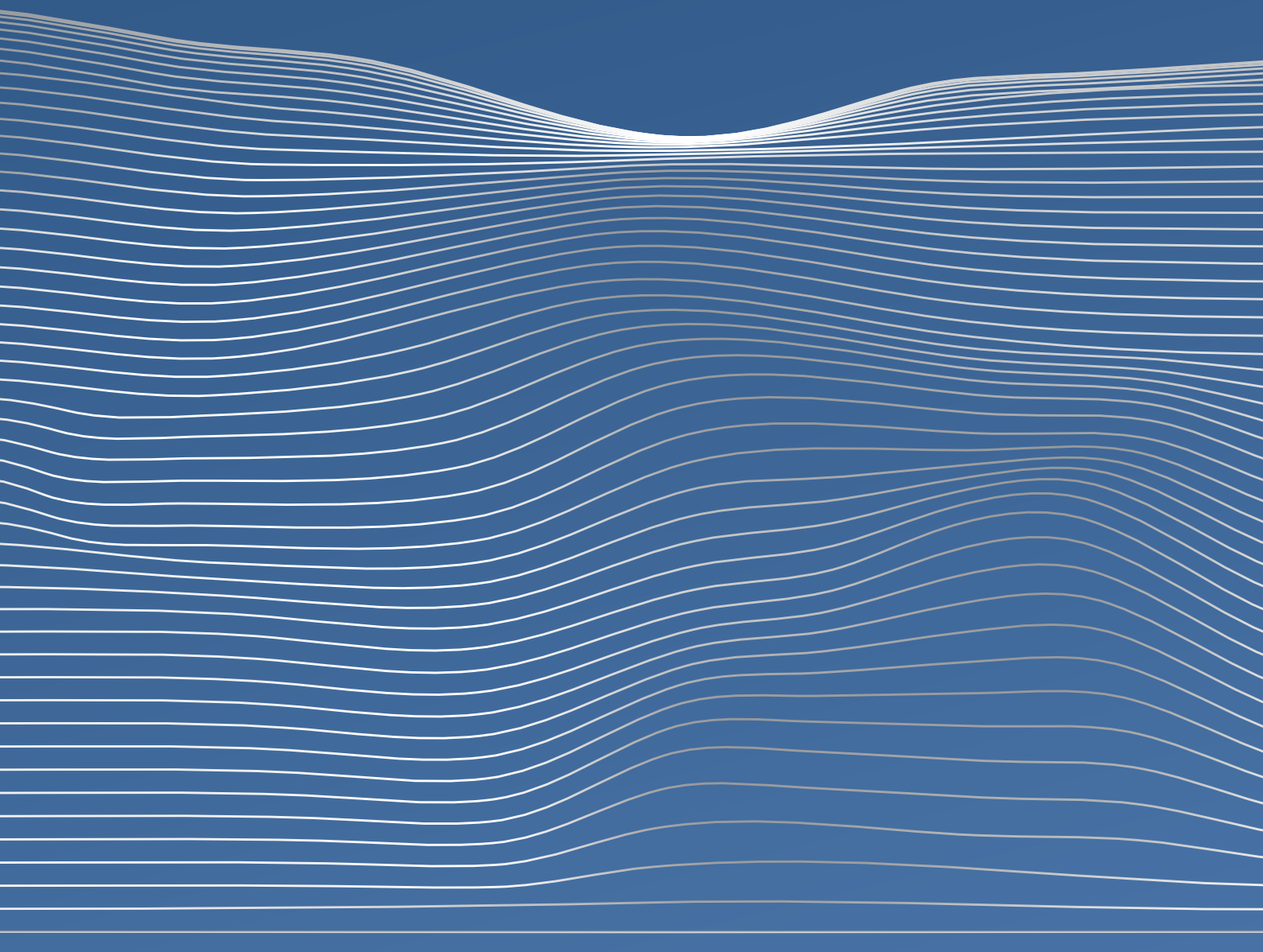
FORUM 2000

Policy paper

Global Cooperation of Democracies in the Digital Realm

Trisha Ray
Jan Hornat



Acknowledgment

The authors would like to thank Maria Kaplina, Junior researcher of the Forum 2000 Foundation, for research assistance.

Introduction

The incremental "digitalization" of human lives has accelerated exponentially in the past decade. Everyday professional and personal activities are increasingly connected to operations in the "digital realm", a multi-layered space encompassing software (online applications, artificial intelligence etc.), hardware (mobile phones, computers, tablets, and other Internet-enabled devices) and the network of services that connect individual human beings, businesses and governments virtually. Needless to say, the flipside is that the digital realm may be exploited for various malign purposes – either by private actors and creators of digital products, who are willing to break ethical barriers for profit-seeking and also by governments, who employ the new technologies to more effectively monitor and sway their own – and foreign – populations.

In the exploitation of the digital realm lies a challenge particularly for liberal democratic societies. The relative openness of their governments, economies and societies toward the outside world in terms of trade of goods and services, as well as ideas and communication, makes them particularly vulnerable to malicious attacks and influence, especially by foreign entities.

The following paper focuses mostly on the possibilities of multilateral cooperation of democracies in the face of challenges emanating from what is often being labeled as digital authoritarianism, i.e. the use of the digital tools by authoritarian states to surveil and control their own populations (inward-looking); and further their political power, undermine democratic systems and narratives along the way (outward-facing). However, we must be aware that even liberal democracies themselves can be tempted to adopt tools similar to those of digital authoritarians in order to reach political goals - thereby becoming threats to the upholding of fundamental human rights. To understand how and why democracies should cooperate in the digital realm, we shall first map the specific challenges that democratic systems face from digital authoritarianism.

Identifying the challenges in the digital realm

Digital services and platforms, either headquartered in authoritarian states or directly operated by them, pose a threat to the core principles of democratic societies. The toolbox of digital authoritarianism is expanding and becoming more accessible.

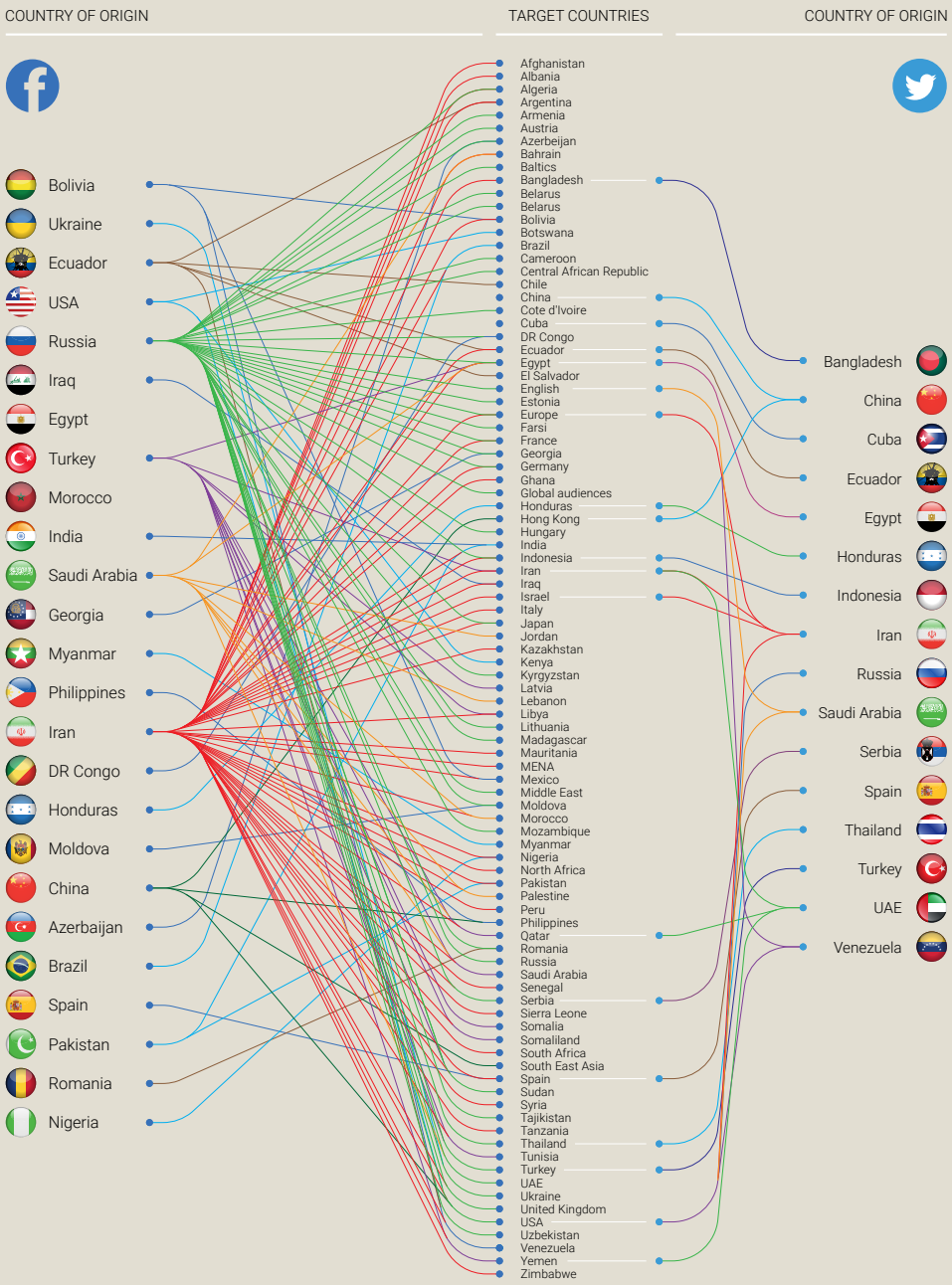
A rising challenge for liberal democracies lies in the illiberal uses of Artificial Intelligence (AI) to track, police, and exclude certain social groups and minorities. The development of facial recognition software targeting China's Uyghur minority [1] has raised alarm bells, and despite global backlash, new applications continue to be piloted [2]. Repression of populations is facilitated by easily available surveillance technologies that employ AI to track real or potential dissidents and unwanted civil society leaders in real-time. These uses are also no longer restricted to mainland China's borders: at least 75 countries in the world have adopted AI-enabled surveillance technologies, with China being a key provider. [3] [4] Hand-in-hand with the tracking of regime opponents goes the prospect of censorship, which again takes place in real-time and can potentially silence any information deemed as a threat by the political elites before it gains a larger audience. Shutdowns of information flows are increasingly common and even affect digital platform users not based in authoritarian states. [5] Social media platforms headquartered in authoritarian states and linked to their government's agendas deliberately censor critical speech and coverage of certain issues, while hosting fake news and disinformation, thereby skewing the debate and manipulating public opinion on a global scale. [6] [7] This can also take the form of account takedowns (see Image 1), organized harassment and mass reporting. In June 2020, for instance, Twitter disclosed a list of state-linked information operations it had identified and acted upon. [8] This included 23,750 accounts, along with 150,000 amplifier accounts linked to PRC's information operations targeting Hong Kong. [9]

Even if Internet users take precautionary measures against being tracked and traced by foreign governments, authoritarian regimes are apt at using digital espionage and cyber operations to access sensitive data about individuals. [10] Legal recourse, including rights to privacy and robust data protection regulations, are weak in the digital authoritarian regimes. This problem becomes even more acute if a democratic state's data flows through infrastructure designed and built by vendors based in authoritarian regimes. This question has been explicitly debated in the case of the implementation of 5G networks and the viability of permitting Chinese company Huawei to provide the technology. Though experts agree that providers of 5G infrastructure may abuse their position and access any Internet traffic, this, of course, applies to all providers and not just those from authoritarian states. [11] As a consequence, the issue has a tendency to become securitized and politicized, thereby sowing discord among publics in democratic states. [12]

Authoritarian states themselves, being anxious about foreign interference in their domestic digital realms, often advocate for "cyber sovereignty" while eroding the rights of their online populations, further isolating their online spaces from global discourse. [13] However, we must note that the narrative of "sovereignty" is not the sole domain of authoritarian regimes. An impending "balkanization" of the Internet, where each state closely monitors traffic within their jurisdiction, could eventually lock millions of people in repressive digital autocracies, which would be more effective at the control of population than any political system in the past.

FIGURE 2 - FACEBOOK AND TWITTER ACCOUNT TAKEDOWNS

COUNTRIES DEPLOYING COMPUTATIONAL PROPAGANDA - HIGHEST FACEBOOK SPEND FROM TOP



Source: Authors' evaluations based on data collected. **Note:** Facebook column is organized by highest spend. Data based on Facebook and Twitter takedowns where state actors were attributed by the platforms. This does not include takedown data where non-state actors were attributed.

Image 1: Social media account takedown requests by country, Oxford Internet Institute

Why should democracies work together in responding to the challenges?

Liberal democracies have arguably the most at stake when facing the possible threats of authoritative practices in the digital realm. The set of values undergirding democratic societies centers around the autonomy and rights of the individual, which are curbed under digital authoritarianism. Given the openness of these democratic societies, malign actors in the digital realm can sow discord through the manipulation of news and narratives among target populations, leading to the weakening of social cohesion and even anomie. However, on the part of democracies worldwide, we can hardly speak of a unified and common approach to dealing with challenges emanating from the digital realm. Indeed, there are diverging interests that have to do both with specific political and social contexts, but also with the political strength of domestic technology firms that are more or less successful in resisting regulation and governance schemes proposed by their governments.

For instance, even the practice of the principles of free speech differs considerably from country-to-country, shaped by historical, social and political contexts. South Korea maintains strict legal guidelines on online election coverage and prohibits content that may sway the outcome of an election. [14] Its Supreme Court even considers a range of offensive or misleading speech acts during an election on social media a crime. On the other hand, the US Supreme Court has long held the view that Internet regulations must be "narrowly tailored." [15] This means that in order to pass the court's scrutiny, the US government must show that any legal speech restrictions "are valid provided that they are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information." On this basis, the Supreme Court, successively struck down laws designed to protect children from online pornography, on the grounds that they were not the least restrictive method of achieving the set goal.

Agreeing on the definition of online free speech, setting the fine line between censorship and social protection or even intervening in the free global market to disqualify certain providers of 5G technologies from public tenders may turn out to be an impossible task among democracies. Still, common threats have served well historically in assembling coalitions of unlikely partners that eventually lead to convergences of interests. In a similar vein, the threats emanating from the digital realm and its co-opting by authoritarian regimes need to be kept in the public discourse, so that democratic societies exert pressure on their governments to conduct practical steps to face the challenges. Indeed, the listed challenges are security threats – both in the sense of physical and ontological security – and thereby their securitization is warranted. The appeal for democracies to cooperate in the response to these challenges can serve as a rallying call that will aid in overcoming the diverging interests and present a united front against possible encroachments on democratic values and freedoms.

The previous section mentioned the way authoritarian regimes deploy the narrative of "cyber sovereignty" to espouse protectionist, repressive and illiberal models for the internet. However, democracies across Europe, Africa and South Asia have espoused their

own versions of cyber sovereignty, centering around "taking back control" of the Internet from technology giants, securing data flows and leveraging them for development. [16] Similarly, digital authoritarianism is not exclusive to authoritarian regimes: democracies must also be alert to its rise within their own borders. It is crucial that democracies strike the balance between the rights of the individual and the security of the state in fighting disinformation, foreign surveillance and other challenges in the digital realm. The Pegasus Project demonstrated just how vulnerable democracies are to these tendencies. While surveillance is a regular feature of states around the world, a key element in security and stability, a baseline of transparency and due process are equally critical for democracies. [17] A political democracy may incrementally move into digital authoritarianism while maintaining the formal appearance of a democratic system - unless its citizens and watchdog groups are vigilant to monitor and reverse such a development.

As the digital realm is not only a source of challenges and threats but promises to bring more equity to social interactions and benign influences on human lives, democratic states have to step in with sound ethical visions for governing the digital sphere to reap its benefits.

Existing initiatives and efforts

The idea of cooperation between democracies to better cope with challenges to human rights and freedoms that may arise with the adoption of new technologies in the digital realm is not new. Initiatives with this particular objective in mind exist, but vary in scope, political ambition and prominence. On the multilateral level, the Organisation for Economic Co-operation and Development (OECD) has launched its Going Digital project in 2017. The initiative "aims to help policymakers better understand the digital transformation that is taking place and develop appropriate policies to help shape a positive digital future." It has produced, for instance, a Going Digital Toolkit and the OECD Principles on Artificial Intelligence, which promotes AI that is innovative and trustworthy and that respects human rights and democratic values. [18] [19] The EU, for its part, has also been rallying member states to create their own AI strategies that meet the criteria of trustworthy and democratic AI technologies. [20] In June 2020, the UN Secretary-General's High-Level Panel on Digital Cooperation has issued a Roadmap for Digital Cooperation, where it particularly focuses on the concept of digital human rights and the International Telecommunications Union (ITU) organizes a high-level annual summit titled AI for Good. [21] [22]

Democratic states have also attempted to form coalitions for the exchange of experience and joining efforts in tackling digital challenges. The informal grouping of the ten "leading digital governments", dubbed Digital Nations, is a successful effort of democratic states to share knowledge on digital governance. [23] With annual summits and a number of working groups focusing on issues related to AI and digital identity, it plays an important role in sharing best practices and advancing the principles of democratic use of digital technologies. The loose partnership of the United States, India, Japan and Australia - the so-called QUAD - has also established a cooperation pillar "on the critical technologies of the future", establishing a working group to facilitate cooperation on international standards and innovative technologies. Some states push the agenda forward with their individual efforts - Denmark, for instance, has been focusing its foreign policy on the issues connected with the challenges in the intersection of tech, democracy and human rights and will host a global Tech for Democracy conference in November 2021. [24] [25]

The initiatives of research institutions, think-tanks and foundations should also not be overlooked. Harvard's Belfer Center holds the Defending Digital Democracy Project, which aims to develop strategies, tools, and recommendations to protect democratic processes and systems. [26] The German Marshall Fund has created the Digital Innovation and Democracy Initiative to work against the misuse of new technologies by developing strategies that advance innovation and strengthen democratic values. [27]

This is not an exhaustive list of ongoing initiatives aiming to unite democracies to jointly face the challenges of the digital (see Appendix) - more such efforts are appearing as we speak and some experts are indeed calling for the digital technology agenda to be a priority in US President Joe Biden's much-anticipated Summit for Democracy. [28]

Bolstering the cooperation of democracies in the digital realm

Policy and investment coordination

In international relations, coordination is often deemed as a solution to collective problems that arise when actors maintain divergent immediate interests but share long-term goals. Coordination of policy in the digital realm among democracies may help settle various differences in approaches and lead to increased convergence. Moreover, a coordinated approach to regulation and governance of emerging technologies will not only make markets in democracies more comprehensive, predictable and transparent for tech companies introducing and developing new products, but also for consumers. Such coordination could concentrate on export and import controls of digital surveillance technologies and AI software or regulating the use of blockchain technology.

Investment policy coordination could be a particularly viable way of strengthening cooperation among democracies in the digital realm, and in turn serve specific goals of technological advancement. Coordination of investment could lead to the rationalization of the allocation of resources and an effective division of labor in research, development and innovation. Such coordination could eventually lead to the pooling of resources to invest in financially intense projects or those that increase the security and resilience of democratic societies, such as increasing cybersecurity, detecting AI-generated "deep fakes" or examining new, potentially unbreakable encryption methods based on quantum mechanics. [29]

The coordination of investments could also involve the embedding of certain (ethical) standards in the new technologies being developed with public investments. For instance, the High-Level Expert Group on Artificial Intelligence (AI HLEG) set up by the European Commission produced Policy and Investment Recommendations for Trustworthy AI, which included the proposition that the EU Commission "work with European financial institutions ... to develop investment guidelines that take into account the Ethics Guidelines", which were also produced by the AI HLEG. [30] [31] In practice, this could mean that investments into new AI technologies could be conditioned on meeting predefined ethical criteria and other standards (such as gender equality) that meet the EU's narrative of a human-centered and trustworthy AI. This may be a way for funders and investors to steer AI technology development in a rights-respecting direction on a broader level. Although the approach of tying the availability of public investments with normative goals may be less acceptable in democracies outside the European Union, it can serve as an example of how to set standards on technologies in the digital realm globally.

Socialization

Sustained coordination of policies and investment among the democracies may require more regular contact through international fora and specific multilateral agencies that focus on issues related to the digital realm. However, since the creation of a new international secretariat that would coordinate the cooperation of democracies in the digital realm is unlikely and if there is a lack of political will and capacity to move forward with more significant levels of coordinated action, civil society should fill this void. [32] As challenges emanating from the digital realm concern all citizens of democratic states, non-governmental organizations should increasingly forge domestic and transnational activities around these issues and help maintain and spread the debates over difficult questions arising from the adoption of new technologies in the public realm.

The intersection of applying new technologies and sustaining democratic freedoms should form part of any debate on the future of democracy. Civil society organizations can play a key role in mediating contact and some level of coordination among officials responsible for digital agendas from different countries. Various studies have shown that intense contact with peers leads to greater convergence of preferences and conformity - this effect, often labeled as socialization, is a crucial added value of all international discussion fora that facilitate informal exchanges of opinions, experience and visions among scholars, government officials and the general public. Engaging governmental officials, who are tasked with implementing or developing policies related to the digital realm, from all levels of governmental institutions and across a number of democracies in discussions about democracy, will enable successive socialization and diffusion of shared norms and values. [33]

Standard-setting

Standard-setting in the digital realm remains in a state of flux, however, there are ongoing processes at international and regional forums, like the UN GGE and the OEWG on cybersecurity, the Global Commission on the Stability of Cyberspace, the Global Partnership on Artificial Intelligence, UNESCO's Information for All Programme and several more identified in this paper. [34] [35] [36] [37] [38] Similarly, a number of governance mechanisms for data flows have emerged, including the EU's General Data Protection Regulation (GDPR), APEC's Cross Border Privacy Rules (CBPR), the African Union's Convention on Cyber Security and Personal Data, the Osaka Track's Data Free Flow with Trust (DFFT) and several more based on function and sector. [39] Data governance at the national level varies as well along the spectrum of regulated flows, from supervised to restrictive.

Aside from attempting to establish a baseline of democratic principles within existing processes, standard-setting is also a part of emerging mechanisms on the cyber resilience, including in supply-chains, disinformation, cyber security and more. Of note are growing narratives and processes around 'trusted supply chains', including for 5G technologies. [40] India's National Security Council, for instance, issued a directive to create a list of trusted telecom vendors, culminating in the launch of the "Trusted Telecom" portal in June 2021, accessible to registered telecommunication operators. [41]

The European Union similarly launched a 5G Cybersecurity Toolbox with risk mitigation measures. Building shared criteria for trustworthy vendors could help close the loop on building the cyber resilience of democracies against a range of authoritarian threats. Standard-setting also concerns AI technologies and the possible biases contained

in algorithms. While we discussed the issue of intentionally biased uses of AI above, unintentional biases are a pertinent issue as well. Even when developers actively seek to avoid any prejudice in their systems, smart algorithms can perpetuate and exacerbate existing patterns of discrimination in the society and bias can "creep" into an AI-based system. For instance, a team of software engineers at Amazon realized in 2015 that an AI program they built to review the resumes of job applicants discriminated against women for technical roles. [43] It has also been reported that an artificial intelligence tool used in courtrooms across the United States to predict future crimes and to help make decisions about pretrial release and sentencing - the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) - was biased against defendants of color. [44] Without some level of transparency of algorithms and some exposure of machine-learning input data, artificial intelligence-based systems cannot be entrusted with automated decision-making. [45]

Promoting, for example, ethical guidelines for AI-based systems operating in the wealthy markets of democratic states can help shape the ethical standards globally. It is crucial that any processes of standard-setting integrate discussions on democratic ethics and norms, by promoting core principles like due process, digital rights and sufficient legal recourse.

Democracy by Any Other Name: Working with Emerging and Developing Nations

A key talking point in anti-democracy narratives perpetuated by authoritarian regimes is that democracy promotion is a strongly Western agenda, with the United States as its primary flag-bearer. [46] It is important not to dismiss these points outright as contrarian or ill-advised as they do reflect widely held anxieties -- well-founded in history -- about the imposition of Occidental values and power relations on non-Western states and societies. [47] A narrative shift acknowledging this history is already under way, as terms like "alliance of the like-minded" enter the diplomatic and geopolitical lexicon. [48]

Linking to all the other categories in this policy brief is the need to engage consistently with non-Western democracies and non-democracies to avoid the creation of standards that fail because they are not adopted widely. As the sub-section on standard-setting also mentions, agreement upon core principles and rights in the digital space need not be under the politicized banner of democracy promotion. More effort must also be dedicated in terms of research and engagement at forums to study debates around approaches to digital spaces outside of the usual fenced-off "club of democracies".

Conclusions and policy recommendations

As the digital realm grows through our social fabrics and increasingly impacts human relationships and interactions in a positive manner, we must be aware of the challenges it poses for the fundamental freedoms and rights democratic that societies have fought for in the last decades and centuries. Though the possible malign implications of new digital technologies are too broad to encompass all in the presented paper, we have aimed to spell out the basic contours of the threats democracies may face in the coming years and how they can cooperate to pool resources and jointly tackle these challenges.

Digital authoritarianism is a disturbing dystopia from the perspective of democratic states, but societies in democracies must not be coddled by the assumption that it is only an issue faced by societies in authoritarian states. As a number of cases have demonstrated, even democratic governments may be lured by the efficiency of targeted surveillance and algorithms providing technical decisions and advice to governing authorities. The cooperation of democracies in hedging against challenges in the digital realm should also be considered as a means, not an end in itself. The ultimate goal of such cooperation is to agree upon common principles and standards of use of new technologies and then diffuse them (i.e. through socialization) amongst semi-democratic and non-democratic states as well.

The following recommendations for the cooperation of democracies in the digital realm are addressed to various stakeholders - not only governments and multilateral organizations, but also to think-tanks and civil society organizations (CSOs), who need to play a pivotal role in monitoring the activities of governments across the board.

- The Biden administration's planned Summit of Democracies should include a focus on the challenges posed by emerging technologies for democracy - discussions should center not only on the threats emanating from "digital authoritarians", as such challenges are easier to detect, but on how democracies themselves are already denying fundamental rights in the initial implementation of technologies in their governing structures
- Debates about digital challenges to democracy should be "mainstreamed" into all discussions about the future of democracy, human rights and freedoms - this mainly concerns public fora and CSOs that engage in efforts aimed at educating the public about these topics
- Democratic governments should -- through multilateral platforms like the OECD or the UN -- establish a code of conduct for governments in the sphere of surveillance. The concept of "ethical surveillance" could help democracies and private technology companies understand the boundaries of personal data collection. These principles should also ensure that the sale of surveillance technologies by companies based in democratic nations meets baseline "tests" of necessity and proportionality.
- There is a pressing need to harmonize the patchwork of data protection frameworks -- implemented or proposed. Furthermore, the revitalization of a DFFT-like process should be inclusive of the deliberation stage. The case of South Africa, India and Indonesia (viz the Osaka Declaration on DFFT) presents a cautionary tale on the risks of an exclusionary process that does not acknowledge the equitable growth imperatives of developing countries. [49]
- The EU and the US should move toward establishing the proposed Transatlantic Agreement on Artificial Intelligence, ideally including more democratic stakeholders. [50]
- As this paper's survey of initiatives in the "digital democracies" space found, research and therefore agenda-setting power is concentrated in a handful of Atlantic countries. It is also worth noting the importance of diversified sources of funding for think tanks and universities in all geographies. [51] [52] In this context, the establishment of a global fund for research on the implications of digital technologies for democracies and its linkages with equitable development and inclusive growth, that prioritizes underrepresented countries and communities would greatly benefit the richness of the debate.

Appendix

Table of notable initiatives of democracies cooperating in the digital realm

Name	Category	Description	Sector	Source
Global Digital Policy Incubator – FSI - Stanford university	Digital norms (Legislation)	The goal is to inspire policy and governance innovations that reinforce democratic values, universal human rights, and the rule of law in the digital realm. Collaboration hub for the development of norms, guidelines, and laws that enhance freedom, security, and trust in the global digital ecosystem.	Academia	https://cyber.fsi.stanford.edu/gdpi/global-digital-policy-incubator-mission
Accelerating the pace of ICT in Government	IT transformation strategies	When: 20 January 2022, London The agenda is to champion technical brilliance in Government, bringing together over 500 senior technology and transformation leaders from both central and local government, and the wider public sector. Providing access to expert speakers and pioneering case studies, it will give insight into how the public sector can incorporate best-practice and IT transformation strategies.	Civil society	https://government-ict.co.uk/
The Digital Services Act and Digital Markets Act	Digital Services and Market	The goal is to create a single set of new rules applicable across the whole EU. To create a safer digital space in which the fundamental rights of all users of digital services are protected, to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally	Government	https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
The OGP Global Summit (Open Government Partnership)	Artificial intelligence, Data rights and privacy	When: December 13-17, 2021, virtually Data rights and privacy: working on the standards, Internet access and control, Responsible and ethical AI and open algorithms, tackling challenges of disinformation and "fake news", protecting freedom of association, protecting freedom of expression, defending human rights defenders.	Civil society	https://www.opengovpartnership.org/about/
Virtual Global Conference	Digital industry	When: October 27-28, 2021 Agenda: Reuters MOMENTUM unites the global technology community to build a better society and advanced economy. The 2-day virtual program is based around four key strategic pillars: society, economy, sustainability, trust and ethics.	Civil society	https://reutersevents.com/events/momentum/conference-agenda.php
Digital Democracy	Technology and Digital rights	Digital Democracy helps our partners achieve transformative change and works toward a world where all people can participate in decisions that govern their lives. USA-based, helps the governments-partners.	Civil society	https://www.digital-democracy.org/mission/
QUAD (Quadrilateral Security Dialogue)	Digital Security	Strategic dialogue platform between the United States, Japan, Australia and India that is maintained by talks between member countries.	Government	https://mea.gov.in/press-releases.htm?dtl/33601/First+Quad+Leaders+Virtual+Summit
East Asia Institute - EAI	Digital Civil Society	South Korea Democracy Storytelling project on democratic cooperation.	Civil society	http://www.eai.or.kr/new/en/pub/view.asp
Decoding #Digital Democracy in Africa	Digital Civil Society	A collaboration with the Digital Civil Society Lab of Stanford University. Analysis on everything from fake news to internet shutdowns, and the role of Facebook to the fight for digital rights.	Civil society/ Academia	http://democracyinafrica.org/wp-content/uploads/2021/06/Decoding-Digital-Democracy-Booklet_Final_loRes-2_WITHEDIT.pdf

The Global Partnership on Artificial Intelligence (GPAI)	Artificial intelligence	GPAI is a multistakeholder initiative working toward responsible development, deployment and use of AI. It's 15 founding members are Australia, Canada, France, Germany, India, Italy, Japan, Mexico, New Zealand, the Republic of Korea, Singapore, Slovenia, the United Kingdom, the United States and the European Union. Brazil, Netherlands, Poland and Spain joined in December 2020.	Government	https://gpai.ai/
Supply Chain Resilience Initiative (SCRI)	Security, trade	The SCRI was formally launched in April 2021 by India, Japan and Australia, with the aim of diversifying supply chains and lines of investment, including for digital technologies. The initiative is aimed at bringing together like-minded nations to cooperate on these issues.	Government	http://goingdigital.oecd.org/ https://www.oecd.org/going-digital/ai/principles/
Roadmap for Digital Cooperation	Security, Digital rights and privacy	In June 2020, the UN Secretary-General's High-Level Panel on Digital Cooperation has issued this Roadmap, where it particularly focuses on the concept of digital human rights.	Government	https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf
Summit – AI for Good	Artificial intelligence	Based on the Roadmap for Digital Cooperation, International Telecommunications Union (ITU) organizes a high-level annual summit. AI for Good is presented as a year round digital platform where AI innovators and problem owners learn, build and connect to help identify practical AI solutions to advance the United Nations Sustainable Development Goals.	Government/ Civil society	https://aiforgood.itu.int/
Digital Nations	Technology and Digital rights	It is an international forum of leading digital governments. The collective goal is to harness the potential global power of digital technology and help one another to become even better digital governments, faster and more efficiently through sharing and learning from each other. Each participant agrees to lead by example and contribute with its expertise on a non-binding, voluntary basis.	Government	https://www.leadingdigitalgovs.org/
Defending Digital Democracy Project	Cyber security	Harvard's Belfer Center holds the Defending Digital Democracy Project, which aims to develop strategies, tools, and recommendations to protect democratic processes and systems from cyber and information attacks	Academia	https://www.belfercenter.org/project/defending-digital-democracy
Digital Innovation and Democracy Initiative	Digital security, tecnology	The German Marshall Fund has created the Digital Innovation and Democracy Initiative to work against the misuse of new technologies by developing strategies that advance innovation and strengthen democratic values.	Academia	https://www.gmfus.org/digital-innovation-and-democracy-initiative
High Level Expert Group on Artificial Intelligence and European AI Alliance	AI governance	Initiatives of the European Commision and member states. The overall work of the AI HLEG has been central to the development of the Commission's approach to Artificial Intelligence and in providing inputs for drafting legislation.	Government	https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

[1] New York Times. One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
[2] Wakefield, Jane, AI emotion-detection software tested on Uyghurs (BBC, 2021), https://www.bbc.com/news/technology-57101248
[3] Feldstein, Steven, The Global Expansion of AI Surveillance (Carnegie Endowment for International Peace, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847
[4] A Surveillance Net Blankets China's Cities: Giving Police Vast Powers. (New York Times, 2019), https://www.nytimes.com/2019/12/17/technology/china-surveillance.html
[5] Policy Brief: Internet Shutdowns (Internet Society, 2019), Editor's note: Policy Brief: Internet Shutdowns was originally published in November 2017. This is an updated version, as of December 2019, https://www.internetsociety.org/policybriefs/internet-shutdowns/
[6] Cockerell Isobel, Authoritarian Tech: Xinjiang's TikTok wipes away evidence of Uyghur persecution — Coda Follows Up (Coda, 2020), https://www.codastory.com/authoritarian-tech/xinjiang-china-tiktok-uyghur/

[7] Mandavia, Megha, TikTok's spreading fake news, MPs say in house (The Economic Times, 2019), https://economictimes.indiatimes.com/tech/internet/tiktoks-spreading-fake-news-mps-say-in-house/article-show/70082227.cms?from=mdr
[8] Twitter Safety, Disclosing networks of state-linked information operations we've removed (Twitter, 2020), https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020
[9] Transparency International, Report: Information Operations (Transparency International, 2021), https://transparency.twitter.com/en/reports/information-operations.html
[10] Marczak Bill, Hulcoop Adam, Maynier Etienne, Razzak Bahr Abdul, Crete-Nishihata Masashi, Scott-Railton John, Deibert Ron, Hulcoop Adam, Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits (Toronto: Citizen Lab, 2019), https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/
[11] Schneier, Bruce, China Isn't the Only Problem With 5G (FP, 2020), https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/
[12] Karásková Ivana, Bachulska Alicja, Matura Tamás, Šimalčík Matej, Policy Paper: Careful or careless? Debating Chinese investment and 5G technology in Central Europe (Prague: Association for International Affairs, 2021), https://mapinfluence.eu/wp-content/uploads/2021/06/Mapinfluence_policy-paper_careful-or-careless_A4_web_09-1.pdf
[13] Creemers, Rogier, China's Approach to Cyber Sovereignty (Berlin: Konrad-Adenauer-Stiftung, 2020), https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537
[14] Haggard, Stephan, Freedom of Expression: The South Korean Case Continued (Washington: Peterson Institute for International Economics, 2013), https://www.piie.com/blogs/north-korea-witness-transformation/freedom-expression-south-korean-case-continued
[15] Brannon, Valerie C., Free Speech and the Regulation of Social Media Content (Congressional Research Service, 2019), https://crsreports.congress.gov/product/pdf/R/R45650/1
[16] Ray, Trisha, Digital Frontiers: The quest for cyber sovereignty is dark and full of terrors (Observer Research Foundation, 2020), https://www.orfonline.org/expert-speak/the-quest-for-cyber-sovereignty-is-dark-and-full-of-terrors-66676/
[17] Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, Pegasus Project (Amnesty International, 2021), https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/
[18] Going Digital Toolkit, (OECD, 2021), http://goingdigital.oecd.org/
[19] OECD, Principles on AI: What are the OECD Principles on AI? (OECD, 2021), https://www.oecd.org/going-digital/ai/principles/
[20] European Commission, Excellence and trust in artificial intelligence (European Commission, 2021), https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en
[21] United Nations. Report of the Secretary-General: Roadmap for Digital Cooperation (United Nations, 2020), https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf
[22] AI for good (ITU, 2021), https://aiforgood.itu.int/
[23] Digital Nations (Canada: Digital Nations, 2020), https://www.leadingdigitalgovs.org/
[24] The White House. Quad Leaders' Joint Statement: "The Spirit of the Quad" (The White House, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/quad-leaders-joint-statement-the-spirit-of-the-quad/
[25] Ministry of Foreign Affairs of Denmark. Tech for Democracy 2021. (Ministry of Foreign Affairs of Denmark, 2021), https://um.dk/en/foreign-policy/tech-for-democracy-2021/
[26] Rosenbach, Eric, Defending Digital Democracy Project (D3P), (Harvard Kennedy School: Belfer Center for Science and International Affairs, 2021), https://www.belfercenter.org/project/defending-digital-democracy
[27] The German Marshall Fund of the United States. Digital Innovation and Democracy Initiative (United States, 2021), https://www.gmfus.org/digital-innovation-and-democracy-initiative
[28] Donahoe, Eileen, The Digital Technology Agenda at the Summit for Democracy (Just Security, 2021), https://www.justsecurity.org/75462/the-digital-technology-agenda-at-the-summit-for-democracy/
29 Cohen Jared, Fontaine Richard, Uniting the Techno-Democracies: How to Build Digital Cooperation (Foreign Affairs, 2020), https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies
[30] European Commission, Policy and investment recommendations for trustworthy Artificial Intelligence (European Commission, 2019), https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence
[31] European Union. Ethics guidelines for trustworthy AI (Office of the European Union, 2020), https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1
[32] Cohen Jared, Fontaine Richard, Uniting the Techno-Democracies: How to Build Digital Cooperation (Foreign Affairs, 2020), https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies

[33] Princeton University, Socialization in International Relations Theory, (Princeton University Press), http://assets.press.princeton.edu/chapters/s8559.pdf
[34] United Nations, Group of Governmental Experts (United Nations, 2021), https://www.un.org/disarmament/group-of-governmental-experts/
[35] United Nations, Open-ended Working Group (United Nations, 2021), https://www.un.org/disarmament/open-ended-working-group/
[36] The Global Commission on the Stability of Cyberspace (GCSC), Report: Global Commission on the Stability of Cyberspace promoting stability in cyberspace to build peace and prosperity (GCSC, 2019), https://cyberstability.org/
[37] The Global Partnership on Artificial Intelligence (GPAI), https://gpai.ai/
[38] UNESCO, Information for All Programme (IFAP), (UNESCO, 2021), https://en.unesco.org/programme/ifap
[39] United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide (UNCTAD, 2021), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[40] Ray, Trisha, Trust but verify: A narrative analysis of "trusted" tech supply chains (Observer Research Foundation, 2021), https://www.orfonline.org/expert-speak/trust-verify-narrative-analysis-trusted-tech-supply-chains/
[41] National Security Council Secretariat. Launch of the 'Trusted Telecom Portal' for implementation of the National Security Directive on Telecommunication Sector (National Security Council Secretariat, 2021), https://dot.gov.in/sites/default/files/Brief%20on%20launch%20of%20Trusted%20Telecom%20Portal-1.pdf?download=1
[42] European Commission, Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures (European Commission, 2021), https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[43] Dastin, Jeffrey, Amazon scraps secret AI recruiting tool that showed bias against women (San Francisco: Reuters, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G
[44] Heaven, Will Douglas, Artificial Intelligence: Predictive policing algorithms are racist, They need to be dismantled (MIT Technology Review, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/
[45] Hosanagar, Kartik and Jair, Vivian, Technology: We Need Transparency in Algorithms, But Too Much Can Backfire (Harvard Business Review, 2018), https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire
[46] Tsygankov, Andrei P. Nobody loves Russia: how western media have perpetuated the myth of Putin's 'neo-Soviet autocracy', (LSE, 2015), https://blogs.lse.ac.uk/europpblog/2015/08/17/nobody-loves-russia-how-western-media-have-perpetuated-the-myth-of-putins-neo-soviet-autocracy/
[47] Meernik, James, United States Military Intervention and the Promotion of Democracy (Journal of Peace Research, Vol. 33, No. 4, Nov., 1996), https://www.jstor.org/stable/424565
[48] Ray, Trisha, Trust but verify: A narrative analysis of "trusted" tech supply chains (Observer Research Foundation, 2021), https://www.orfonline.org/expert-speak/trust-verify-narrative-analysis-trusted-tech-supply-chains/
[49] Kanth, D. Ravi, India boycotts 'Osaka Track' at G20 summit (MINT, 2019), https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html
[50] Joint Communication to the European Parliament, The European Council and the Council, A new EU-US agenda for global change (Brussels, 2020), https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf
[51] Gonzalez Hernando, Marcos, Williams, Kate, Examining the Link Between Funding and Intellectual Interventions Across Universities and Think Tanks: a Theoretical Framework (International Journal of Politics, Culture, and Society volume 31, pages193–206, 2018), https://link.springer.com/article/10.1007/s10767-018-9281-2
[52] Clarke Laurie, Williams Oscar, Swindells, How Google quietly funds Europe's leading tech policy institutes (NewStatesman, 2021), https://www.newstatesman.com/business/sectors/2021/07/how-google-quietly-funds-europe-s-leading-tech-policy-institutes

Authors

Jan Hornát is the Head of the Department of North American Studies at Charles University and fellow at the Peace Research Center Prague. He currently focuses on transatlantic relations, the role of status in international relations, and the state of global democracy. Jan is the author of a number of academic articles and books, of which the most recent is The Visegrád Group and Democracy Promotion: Transition Experience and Beyond (Palgrave Macmillan, 2021). He has been a member of the "VirusImpact" team of the Ministry of Foreign Affairs of the Czech Republic, which examined the geopolitical impacts of the COVID-19 pandemic. Before joining the academia, he was Head of Unit at the Department of European Programs of the Ministry of Justice of the Czech Republic.

Trisha Ray is an Associate Fellow at the Center for Security, Strategy and Technology at the Observer Research Foundation in India. Her research focuses on geopolitical and security trends in relation to emerging technologies, including AI, 5G and critical minerals. Trisha is a member of UNESCO's Information Accessibility Working Group, as well as a Pacific Forum Young Leader. Trisha completed her MA in Security Studies from the Walsh School of Foreign Service at Georgetown University.

Forum 2000 Foundation
Pohořelec 6
118 00 Prague 1
Czech Republic
T +420 224 310 991
secretariat@forum2000.cz
www.forum2000.cz

This paper is a publication of the Forum 2000 Foundation and its creation was financially supported by the National Endowment for Democracy (NED). The views expressed in the paper are the responsibility of its authors.