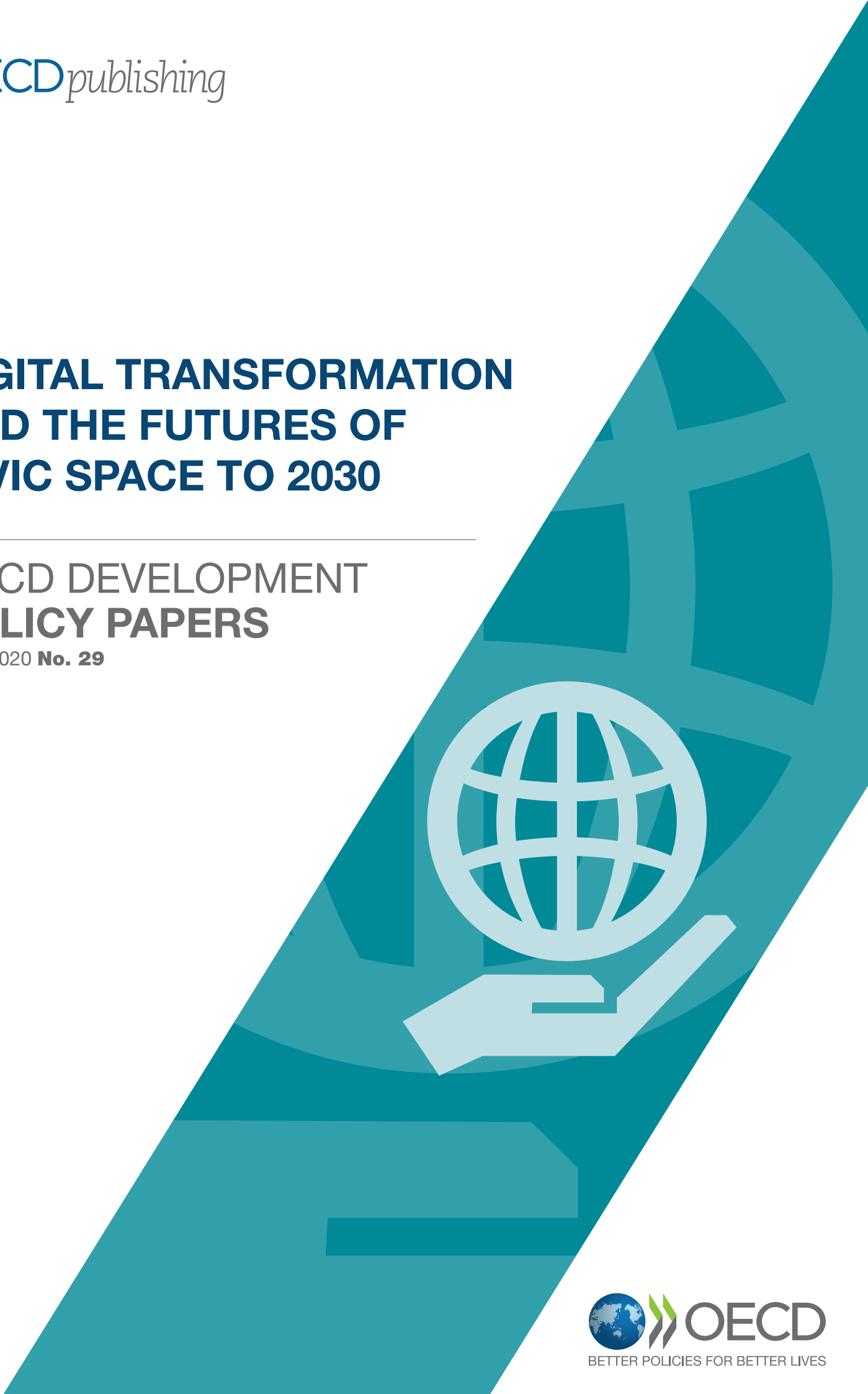
OECD publishing

DIGITAL TRANSFORMATION AND THE FUTURES OF CIVIC SPACE TO 2030

OECD DEVELOPMENT
POLICY PAPERS
June 2020 **No. 29**



OECD
BETTER POLICIES FOR BETTER LIVES

OECD Policy Papers

Disclaimer

This paper is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed do not necessarily represent the official views of the OECD member countries.

This document, as well as any data and any map include herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. The document was authorised for publication by Jorge Moreira da Silva, Director of the Development Cooperation Directorate.

Please cite this paper as OECD 2020, Digital Transformation and the Futures of Civic Space to 2030, *OECD Development Policy Paper 29*.

Abstract

Digital transformation is rapidly altering civic space, challenging the ways in which members of the OECD Development Assistance Committee (DAC) and other providers of development co-operation strive to promote an enabling environment for civil society to contribute to sustainable development. This paper aims to support DAC members and other providers of development co-operation to integrate the implications of a range of plausible futures of civic space into positive policy action today. To this end, it provides an overview of the variables (i.e. current trends, drivers of change and uncertainties) that may determine the trajectory of civic space in the context of digital transformation; identifies four plausible futures that emerge from four different logical interactions of these variables - that could materialise over a ten-year horizon and be fully realised by 2030; and draws policy implications to support DAC members and other providers in designing development co-operation policies that best leverage the opportunities that digital transformation offers while mitigating its risks.

Foreword

This paper complements work on civil society by the OECD and its Development Assistance Committee (DAC), including the Development Assistance Committee and Civil Society study (OECD, 2020[1]). The objective of this work is to create guidance for DAC members to best promote enabling environments for civil society in partner countries through (1) support to and engagement with civil society; (2) promotion and protection of civic spaces; and (3) promotion of CSO effectiveness and accountability; (4) grounded in principles of inclusive dialogue and participation. This paper also complements the DAC Network on Governance's (GovNet) efforts to promote inclusive governance and address the growing challenge of autocratisation.

This paper integrates a foresight approach to policy making and is part of the foresight analysis that is being developed by the OECD Development Co-operation Directorate (DCD), Foresight, Outreach and Policy Reform (FOR) Unit. This foresight analysis supports policy makers in thinking about alternative plausible futures as a prerequisite for successful anticipatory governance. It aims to equip providers of development co-operation with an overview of civic space trajectories as well as the potential outcomes and trade-offs from different scenarios. Development co-operation policy choices made today will shape what civic space looks like tomorrow.

Acknowledgements

This paper was prepared by the OECD Development Co-operation Directorate (DCD), under the guidance of Director Jorge Moreira da Silva.

The DCD team was led by Ana Fernandes, Head of the Foresight, Outreach and Policy Reform Unit and Jacqueline Wood, Team Leader – Senior Civil Society Specialist. Lead authors are: Marilyn Cham, Civil Society Policy Analyst, and Krystel Montpetit, Foresight Team Lead.

Contributions were provided by a broader team of OECD specialists, in particular, Karin Fällman, Sidney Leclercq, Takashi Yukizawa, Nadine Piefer-Soyler, Piero Fontolan, John Egan, Catherine Anderson, Marc De Tollenaere (all from DCD), Duncan Cass-Beggs, Joshua Polchar, Julia Staudt (Office of the Secretary General), Alessandro Bellantoni, João Vasconcelos, Claire McEvoy, Piret Tonurist, Carlotta Alfonsi (Public Governance Directorate).

The project team is grateful for the insights of external contributors: Douglas Rutzen and Ona Flores (International Center for Not-for-Profit Law), Wolfgang Jamann (International Civil Society Centre), David Saldivar (Oxfam), Cat Tully (School of International Futures), Poonam Joshi (Funders Initiative for Civil Society), Anupam Saraph (Symbiosis Institute of Computer Studies and Research) and Betty Sue Flowers (University of Texas).

The paper also benefitted from consultations and comments from members of the Development Assistance Committee (DAC), the DAC-Civil Society Organisation (CSO) Reference Group, Forus International, the Task Team on CSO Development Effectiveness and Enabling Environment (Task Team), and the European Commission (EC) Directorate General for International Cooperation and Development.

The paper was prepared for publication under the direction of Henri-Bernard Solignac-Lecomte and Stacey Bradbury. Our appreciation also goes out to Stephanie Coic for graphic design.

Thanks and appreciation is extended to all those who made contributions at various stages of the paper, including colleagues who participated in the two foresight workshops (see Annex B for the full list).

Abbreviations and acronyms

AI	Artificial intelligence
CCTV	Closed-circuit television
Civic tech	Civic technology
CSO	Civil society organisation
DAC	Development Assistance Committee
DCD	Development Co-operation Directorate
DDP	Digital Defenders Partnership
EC	European Commission
EU	European Union
FOR	Foresight, Outreach and Policy Reform
GovNet	DAC Network on Governance
GPEDC	Global Partnership for Effective Development Co-operation
Iot	Internet of things
NGO	Non-government organisation
ODA	Official development assistance
OECD	Organisation for Economic Co-operation and Development
OGP	Open Government Partnership
SDGs	Sustainable Development Goals
Sida	Swedish International Development Co-operation Agency
STI	Science, technology and innovation
Task Team	Task Team on CSO Development Effectiveness and Enabling Environment
Tech	Technology
USAID	United States Agency for International Development
VPN	Virtual Private Network

Executive summary

Digital transformation refers to the economic and societal effects of digitisation (the technical process of converting analogue information into digital form) and digitalisation (the organisational or business process of the technologically-induced change within industries, organisations, markets and branches). It is altering civic space, that is, the physical, virtual, and legal place where people associate, express themselves, and assemble. Digital technologies are providing new ways to exercise the freedoms of association, peaceful assembly and expression, as well as new ways to restrict those rights, raising questions about how technological advances will affect civic space in the future. The implications of digital transformation for fundamental freedoms and civic space are particularly relevant in the context of the Covid-19 pandemic marked by a widespread deployment of digital technologies to respond to the global health crisis. These trends are challenging the way members of the OECD Development Assistance Committee (DAC) and other providers of development co-operation promote an enabling environment for civil society to contribute to sustainable development. Effective development co-operation requires an enabling environment for civil society to contribute to the Sustainable Development Goals' (SDGs) achievement; an open and dynamic civic space is an essential component of this.

The objective of this paper is to shed light on how civic space is evolving in the face of digital transformation including in the context of the Covid-19 pandemic, and support DAC members and other providers of development co-operation to integrate the implications of a range of plausible futures into positive policy action today. Development co-operation policies can be designed to leverage the opportunities that digital transformation offers to civic space and also mitigate potential adverse impacts. This paper uses foresight analysis to explore the different possibilities of what the future might look like; the paths to those possible futures i.e. the range of plausible trajectories that civic space could take; and their respective implications for policy making today. In so doing, it will assist development co-operation policy makers to prepare for and shape the future of civic space in a dynamic way.

In certain cases, the opportunities brought about by digital transformation are creating the conditions for civic space and civil society to thrive. Digital transformation has opened new spaces on line. It is connecting civic spaces at a global level, supporting mass mobilisation of social movements offline, and creating more dynamic and inclusive civic spaces, marked by greater activism and engagement. In the context of Covid-19, countries have turned to digital technologies in their emergency response to control the outbreak of the pandemic. Surveillance technology is being used to locate people with symptoms and monitor the spread of the disease. At the same time, mass surveillance systems deployed in the Covid-19 response have triggered concerns related to personal privacy and civil liberties on a global scale. Other risks and threats that undermine civic space and freedoms are emerging from the perverse use of digital technologies. Adverse practices are being carried out by a range of actors (i.e. states, companies or consultancy firms, media outlets, and civil society actors). In addition to surveillance abuse, digital technologies are being exploited to silence and manipulate civil society, as well as to express extremist views. The current business models of technology companies present risks to data protection, algorithmic bias, discrimination and infringement of privacy, undermining the safety and security of online civic spaces. The control of online spaces by technology companies are challenging CSOs' independence. In contexts where individuals do not have equal access to digital technologies, new forms of exclusion are proliferating.

An inductive scenario-building exercise was conducted to analyse the different logical interactions of current trends, drivers of change and uncertainties that could determine the future trajectory of civic space. Four plausible, differentiated, disruptive and memorable futures of civic space have emerged, and could be fully realised by 2030. Civic space could either:

Collapse: Actors have free rein to leverage digital technologies in adverse ways that restrict civil society actors' activities and lead to the gradual collapse of civic space.

Flourish: An enabling legal framework exists for civic space to flourish both on line and offline. A democratic model of digital governance has been established through which fundamental rights are respected across the digital sphere.

Transform itself: Social movements permeate online and offline civic spaces and engage primarily in political activism. The evolving interactions and dynamics between civil society actors as well as between civil society and governance structures and institutions transform the nature and purpose of civic space. Online space has become a modern *agora* where people practice direct democracy.

Break apart: Civic space has broken into micro spaces that vary in levels of openness and inclusiveness. Civic space as a whole is not cohesive nor integrated but has become dysfunctional and is considerably weakened and limited. The fragmentation of civic space is amplified and exacerbated along the following lines: geography, age, level of education, gender, and level of income.

DAC members can consider a number of policy implications and action points to leverage the opportunities that digital transformation offers in each plausible future, as well mitigate the risks. They can:

- Have a civil society or CSO-specific strategic policy document recognising the need to protect civic space and address the challenges associated with digital transformation; support policies and programming that address the interconnection between civic space and digital transformation.
- Conduct risk assessments and refrain from providing digital support to countries where such support could inadvertently do harm; support activities that promote digital inclusion and reach the most vulnerable civil society actors e.g. digital literacy and capacity building of local CSOs.
- Address risks for civic space in aid for trade policies that involve surveillance technology; co-operation with other providers of development co-operation that export digital technologies; engagement with the private sector (tech companies).
- Engage with partner countries in developing rights-respecting governmental measures during a national emergency or crisis, and establishing safeguards to minimise risks for digital surveillance and other laws from being used to intentionally or inadvertently shrink civic space.
- Strengthen compliance with article 20(2) of the International Covenant on Civil and Political Rights - ensuring hate speech provisions do not violate the freedom of expression.
- Work with civil society (including non-traditional, digitally-empowered forms of civil society actors such as social movements), partner country governments, and private sector partners such as non-profit tech companies; engage them in policy dialogues related to digital transformation and civic space.
- Strengthen digital rights and laws which comply with international human rights laws, civic rights and international digital governance frameworks; as well as the press, public service media, media and social media-related laws which tackle disinformation; support programmes that build (i) local capacities of legal, judicial and security officials and institutions to address violations of digital rights; and (ii) national and community level media capacities for quality, investigative journalism.

As a Committee, the DAC can consider supporting the development of policy guidance or a recommendation on enabling environments for civil society, which addresses among other issues, effective donor support for the promotion and protection of civic space – including in the digital age.

Table of contents

Tables

Figures

Boxes

Introduction to the futures of civic space and foresight methodology

We live in a time of great digital upheaval and disruptions.[1] From the Internet of things (Iot)[2] and open data[3] to artificial intelligence (AI)[4] and robotics[5], digital technologies are providing new ways to exercise the freedoms of association, peaceful assembly and expression, as well as new ways to restrict those rights[6]. Digital transformation, and the rapid pace at which it is evolving, raises questions about how technological advances will affect civic space in the future. These questions are relevant for DAC members and other providers of development co-operation as effective development co-operation requires an enabling environment for civil society to contribute to the achievement of the Sustainable Development Goals (SDGs).[7] An open, plural and dynamic civic space is a central feature of a civil society enabling environment.[8]

[1] See Annex A for the full list of definitions.

[2] The Internet of things refers to the connection of devices (other than typical fare such as computers and smartphones) to the Internet. Cars, kitchen appliances, and even heart monitors can all be connected through the Iot. It is the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

[3] Open data is the data that anyone can access, use and share freely without restrictions from copyright, patents or other mechanisms of control.

[4] Computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision making, and translation between languages.

[5] The branch of technology that deals with the design, construction, operation, and application of robots.

[6] The International Center for Not-for-Profit Law (ICNL) is conducting similar research in this field: https://www.icnl.org/our-work/technology-civic-space.

[7] The 2018 OECD Development Co-operation Report dedicated a chapter to the role of CSOs in achieving the SDGs and leaving no one behind (OECD, 2018[4]).

[8] Act Alliance published a report in 2019 on the implications of civic space for the sustainable development goals: https://actalliance.org/wp-content/uploads/2019/05/ACT_SynthesisReport_CivicSpace_2019_Final_WEB-Copy.pdf.

DAC members are being called upon to address challenges facing civic space,[9] especially in the context of digital transformation,[10] as well as prioritise civil society enabling environments in development co-operation policy agendas.[11] In order to do so, it will be important to be aware of a range of plausible future evolutions of civic space and the implications of each. This is precisely the objective of this paper: to shed light on the rapidly evolving landscape of civic space in the face of digital transformation, and support DAC members to integrate the implications of a range of plausible futures into positive policy action today. Action can be taken today by designing development co-operation policies that leverage the opportunities that digital transformation offers to civic space while mitigating its risks.

The outbreak of the Covid-19 pandemic[12] at the time of this paper's publication, marked by the widespread deployment of digital technologies to respond to the global health crisis, with important implications for fundamental freedoms and civic space, accentuates the timeliness and relevance of this subject matter (International Center for Not-for-Profit Law, 2020[2]).

Whilst a wealth of material on digital transformation is available and some studies have emerged on the fringes of how it relates to civic space, as of today, no research has been conducted from the vantage point of development co-operation, and even less so when it comes to applying a foresight methodological approach. The foresight analysis used in this paper was done with the objective to scan the horizon for emerging changes related to civic space, analyse megatrends at a global scale and develop multiple scenarios, to reveal and discuss useful policy considerations for the future. As such the analysis – while highlighting country examples from across the world, does not attempt to draw possible lines between what is happening or will happen in the developed world versus the developing world, nor does it attempt to single out civic space challenges in partner countries. As for the policy implications, they primarily address DAC members; the role they can play, actions they can undertake, and responses they can bring – globally – through their strategies and national policies, within the framework of development co-operation. They could also be considered relevant by other providers of development co-operation.

The main focus of the paper is on civic space. However, digital transformation's profound effect on the operating environment of civil society inextricably affects civil society organisations (CSOs). Inversely, the effects on CSOs also have impacts on civic space. In recognition of this, the analysis of the paper incorporates the nuances that derive from these inter-relations.

---

[9] 2019 GPEDC Senior Level Meeting Co-Chair Statement: "We remain concerned about the shrinking civic space ... We therefore call for joint actions to analyse the different constraints on our shared support to civil society to play its full role as development actors in their own right, and to work towards relevant recommendations" (p. 3): https://effectivecooperation.org/wp-content/uploads/2019/07/2019-Senior-Level-Meeting-Co-Chair-Statement.pdf.

[10] 'Defending Civic Space: Is the International Community Stuck?': "Develop a strategic framework that links closing civic space to other key foreign policy challenges, articulates a positive vision of civic space globally, and offers tailored tactical guidance" (p. 21); "Bring experts on board who understand the rapidly evolving digital landscape and can make the connection to civic space issues, including to future threats" (Carnegie Endowment for International Peace, 2019[95]).

[11] The 2019 Belgrade Call to Action: Positive Measures for Enabling Civic Space towards Maximising Civil Society Contributions to the SDGs. "The Call is addressed to Governments and Member States of the United Nations to take urgent action to reverse deteriorating conditions for civil society in the context of the 2030 Agenda" (p. 1): https://gcap.global/wp-content/uploads/2019/05/Revised-April-Action-Agenda.pdf.

[12] The Coronavirus disease 2019 (Covid-19) is an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). The disease was first identified in 2019 in Wuhan, the capital of the People's Republic of China (hereafter 'China') Hubei province, and has since spread globally. On 11 March 2020, the World Health Organisation declared the Covid-19 outbreak a pandemic.

How to use the chapters of this paper

The preamble presents the nature and advantages of scenario-based foresight in policy making. It also outlines the steps of the scenario-based foresight process chosen for this paper.

Chapter 1 provides a comprehensive, evidence-based overview of the current trends of civic space in the context of digital transformation.

Chapter 2 analyses the drivers of change[13] and uncertainties that could determine the future trajectory of civic space in the face of digital transformation.

Chapter 3 describes the four possible futures of civic space that could plausibly materialise within a 10-year horizon, by 2030, including compelling storylines and tables of comparative descriptions, i.e. key drivers of change and the sequence of events to 2030.

Chapter 4 outlines the policy implications of each scenario, as well as puts forward suggested action points to leverage the opportunities or mitigate the risks of each scenario.

What is scenario-based foresight and how can it help us navigate the future of civic space?

Foresight is the systematic, participatory and multi-disciplinary approach to explore mid- to long-term futures and drivers of change (Forward Thinking Platform, 2014[3]). It is a structured approach for looking beyond the expected future by:

1. Examining the strategic context. Analysing trends and drivers of possible future contexts and their inter-dependencies.
2. Engaging a wide set of views. A diversity of perspectives helps to understand and separate the "signal from the noise", and to develop common knowledge and ownership.
3. Exploring plausible futures (scenarios) and critical uncertainties.
4. Identifying policy implications to help build resilience in alternative futures including new policy opportunities and challenges (OECD, 2018[4]).

Foresight is not the same as *forecasting*. Forecasting is the science that predicts the future in a static and pre-deterministic way. Foresight is the science that explores different possible trajectories of the future and their respective pathways, to be able to shape the future in a dynamic way. Foresight is not a discipline that is about one future and determinism. Rather, it is a discipline that is about several plausible futures and action as the only determining factor of the future.

What are scenarios?

Scenarios are a set of alternative descriptions of how the future may unfold according to an explicit, coherent and internally consistent set of assumptions about the combination and interplay of drivers of change. Scenarios are not forecasts; they do not attempt to correctly predict what the future will look like. Rather, scenarios describe what might happen in the future and what we can learn from this process, to inform and guide our actions today.

[13] See the definition of a driver of change in Annex A.

A scenario has two main features: (i) a description of the end-state i.e. what does the world look like at the end of the time horizon for which the scenario has been developed; (ii) a causal logic explaining how this future came about, describing a sequence of events.

The scenarios of this paper were designed in a way to give equal weight to the following criteria:

- **Plausibility factor:** The combination and sequences of the drivers of change can logically be connected to the final outcome of each scenario.
- **Differentiation factor:** Each scenario provides insights that the others cannot.
- **Disruptive power:** Each scenario adds value beyond the 'business as usual' trajectory.
- **Policy-making utility:** Each scenario can support policy makers to identify policy implications for action today.
- **Memorability factor:** Each scenario is easily memorable to increase their use and impact in policy discussions and processes.

The scenarios were constructed using the inductive or bottom-up scenario-building method:[14]

1. Identification and analysis of variables [e.g. current trends, drivers of change (mega-trends, emerging patterns and early signals) and uncertainties about the future] that could influence the future trajectory of civic space in the face of digital transformation.
2. Study of the possible interactions of these variables.
3. Selection of the most logical interactions of variables in terms of (i) inter-connectedness between variables and (ii) causality to the final outcome.
4. Step-by-step build-up of the future scenario, following a logical sequence and timeline of events to 2030.

The inductive scenario-building method was selected for this paper as it allows the emergence of a scenario structure unconstrained in the number of drivers of change, uncertainties and current trends that can be used to form the scenarios.

How was the plausibility of this paper's scenarios ensured?

Plausibility was used as one of the main scenario validation criteria. Plausibility does not imply that a future situation will happen. Rather, it means that the combination and sequence of variables grounding a scenario can logically be connected to the final outcome of this scenario (Forward Thinking Platform, 2014[3]). This paper acknowledges that the plausibility of a scenario is a subjective characterisation: a scenario may be viewed to be plausible by one stakeholder and implausible by another. This is the reason why this paper engaged a diverse group of participants in its scenario-based foresight process. This modality ensures that the set of scenarios judged plausible by a diverse group of participants is also likely to be judged plausible by others outside the group. The scenarios of this paper were judged plausible by the diverse group of participants because of (i) their underlying assumptions; (ii) internal consistency; and (iii) logical connection.

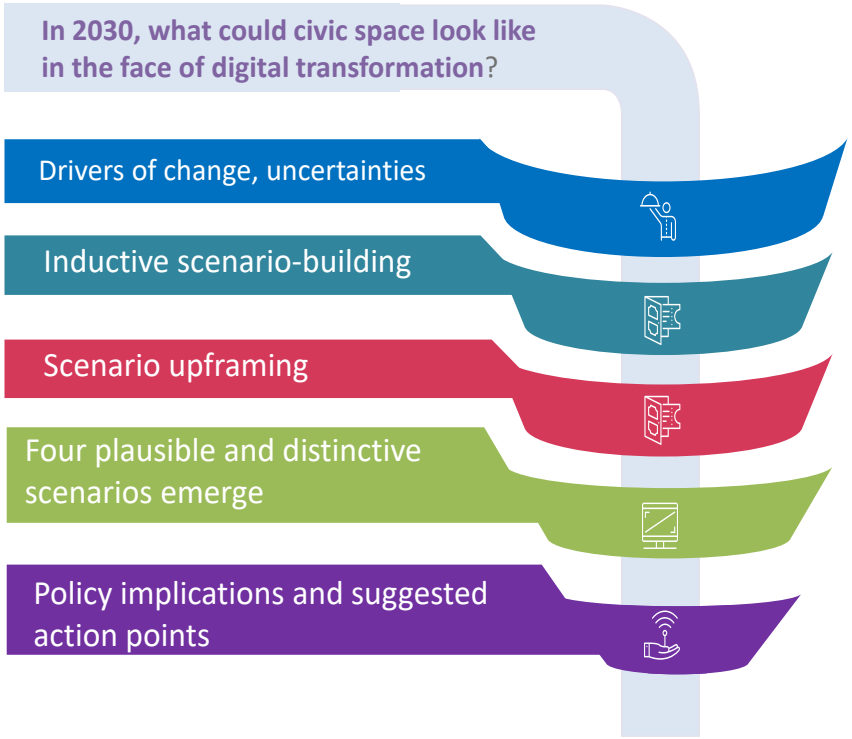
[14] The inductive method (or bottom-up method) is an approach which builds step-by-step on the data available. It allows the structure of the scenarios to emerge by itself. The overall framework is not imposed so that the storyline can grow out of the step-by-step combination of drivers of change.

What are the advantages of using scenario-based foresight in policy making?

There are several advantages of using scenario-based foresight in policy making. In the context of this paper, it serves as a means to:

- Reveal and test assumptions about the future of a policy issue, that is – civic space.[15]
- Reveal and examine not just one but several plausible trajectories of civic space in the face of digital transformation.
- Reveal and examine the opportunities and risks associated with each plausible trajectory.
- Equip policy makers to prepare for several plausible trajectories for the future of civic space rather than preparing for just one.
- Equip policy makers to choose their normative[16] trajectory[17] for the future of civic space; support them to begin working towards it by considering its policy implications today, to increase its probability of materialising in the future.
- Equip policy makers to better prepare for the least favourable plausible trajectories of civic space by mitigating their risks today, or preparing to adapt to these risks if mitigation fails.

Figure 1.1. Scenario-based foresight process



[15] The future of a policy issue or the future of an interaction of policy issues.

[16] A normative scenario is a preferred scenario or future (see Annex A for the full list of definitions).

[17] Trajectory or trajectories.

What were the steps of this paper's foresight process?

Step 1: In light of the analytical review of current trends related to the impacts of digital transformation on civic space, the paper proceeded to ask: In 2030, what could civic space look like in the face of digital transformation?

Step 2: The paper identified and analysed the key drivers of change, i.e. mega-trends, emerging patterns and early signals, which are likely to influence the future of civic space in the face of digital transformation. It also identified the main uncertainties about the future. The identification of these drivers of change and key uncertainties was achieved through a collaborative process, more specifically through: (1) a first foresight workshop including the participation of a diverse range of in-house experts; (2) consultations[18] with external experts, CSOs and other stakeholders.

Step 3: The paper leveraged insights from the first in-house workshop, as well as from the first round of consultations, to undertake a scenario-building exercise using the inductive method.[19]

Step 4: A second foresight workshop was held to up-frame the initial future scenarios identified. A final set of four inductive scenarios emerged from this workshop. Inputs for the policy implications of these plausible scenarios were drawn from the workshop discussion, a second round of external consultations, and an analysis of existing relevant policy guidance.[20] These policy implications have informed the suggested action points put forward in this paper.

[18] For more information about the consultation process, please see Annex B.

[19] The inductive method (or bottom-up method) is an approach which builds step-by-step on the data available. It allows the structure of the scenarios to emerge by itself. The overall framework is not imposed so that the storyline can grow out of the step-by-step combination of drivers of change.

[20] For more information about the consultation process, please see Annex B.

1. Current trends in civic space in the context of digital transformation

Digital transformation refers to the economic and societal effects of digitisation and digitalisation (OECD, 2019[5]). Digitisation (the technical process of converting analogue information into digital form), digitalisation (the organisational or business process of the technologically-induced change within industries, organisations, markets and branches) and digital transformation (the effect) are said to ''accelerate the already existing and ongoing horizontal and global processes of change in society''.[21] These processes of change are affecting civic space, i.e. the physical, virtual, and legal place where people exercise their rights to freedom of association, expression, and peaceful assembly (CIVICUS, n.d.[6]). In certain cases, the opportunities brought about by digital transformation are creating the conditions for civic space and civil society to thrive. At the same time, digital transformation has also brought a range of new risks and threats that undermine civic space and freedoms.

1.1. Positive trends

Civic space and civil society organisations (CSOs) have benefitted in many ways from digital transformation. The benefits include: the opening of new online spaces; the strengthening of offline civic spaces in certain contexts; the emergence of a global connected civic space capable of mobilising civil society and advancing causes across borders; and more dynamic and inclusive civic spaces marked by greater civic activism and engagement.

1.1.1. The opening of new online civic spaces

The digital age has opened new online spaces for association, assembly and free expression. At a time when civic space is shrinking globally,[22] digital technologies offer an alternative space, on line, including in countries where the offline exercise of the rights to freedom of expression, of peaceful assembly and of association is heavily curtailed or suspended (UN-OHCHR, 2019[7]). Following the confinement measures put in place across the world during the Covid-19 pandemic, Greta Thunberg took her climate protest online with the hashtag #climatestrikeonline. She and her followers joined action on Friday through this hashtag and assembled online (European Center for Not-for-Profit Law, 2020[8]).

[21] Khan, Shahyan, ''Leadership in the Digital Age - a study on the effects of digitalization on top management leadership'', Stockholm Business School, 2017 (Shahyan Khan, 2017[96]).

[22] More than a hundred countries are characterised by closed, repressed or obstructed civic space. More than 80% of the world's population – 6 billion people – face a situation where either the conditions are closed for civil society (24 countries), or where civil society is highly repressed (38 countries), or where civil society faces substantial legal and political obstacles (49 countries) (CIVICUS Monitor, 2019[88]).

1.1.2. The strengthening of certain civic spaces offline

In certain contexts, the power of digital technology to fuel and sustain activism and mass mobilisation is contributing to strengthening civic spaces offline[23]. Civic freedoms are being exercised along a continuum between online and offline spaces (Association for Progressive Communications, 2019[9]). Activists use social media as a space for advocacy and organising, to mobilise a large group of people in a prompt and effective manner and at little cost, as well as to co-ordinate public protest in real time (OECD, 2019[10]). These new opportunities for civic action and freely organised mobilisation brought about by digital transformation are creating the conditions for civil society to thrive. As stated by the Special Rapporteur on the rights to freedom of peaceful assembly and of association: "By serving both as tools through which civic rights can be exercised offline and as spaces where individuals can exercise free expression and actively form online assemblies and associations, digital technologies have vastly expanded the capacities of individuals and civil society groups to organise and mobilise, to advance human rights and to innovate for social change" (UN-OHCHR, 2019[7]).

Labour action (e.g. strikes) is another form of civic activism that is commonly mobilised on line, in at least 77 countries (Varieties of Democracy (V-DEM) Institute, 2019[11]). Digital platforms and apps have become increasingly important for labour unions to organise protests, keep in touch with members and provide spaces for online discussions and decision making.

> *Digital "technology serves both as a means to facilitate the exercise of the rights of assembly and association offline, and as virtual spaces where the rights themselves can be actively exercised on line" (UN-OHCHR, 2019[7]).*

1.1.3. The emergence of a global connected civic space

Digital transformation is enabling civil society actors to connect and mobilise at a global level. Digital technologies provide tools such as social media platforms and applications that allow CSOs to reach new audiences, attract members, and build coalitions and networks across the world. By connecting people and civil society from different regions and backgrounds, digital technologies have allowed CSO networks to speak on behalf of national development platforms all over the world. They have strengthened and consolidated CSO networks as a voice of international civil society and allowed them to speak to a global audience on issues of common concern that go beyond borders. For example, the #MeToo movement used social media platforms to mobilise women all around the world against sexual violence.

Civic actors are now communicating, spreading and accessing information and organising on a whole new scale, in ways that were previously impossible or extremely costly (Heinrich Böll Foundation, 2016[12]). Global connectedness has led to greater access for citizens and organised civil society to international information and support, and has facilitated better co-ordination, and exchange of good practices between civil society in different parts of the world. For example, in less than three weeks, the hashtag #BringBackOurGirls that emerged in Nigeria in response to the kidnapping of 276 girls, spread around the world and had been used more than a million times world wide, bringing global attention to the Boko Haram

[23] The Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association lists many examples. According to the Report: In Armenia, the social media platforms, live-streaming tools and communication apps played a key role in the velvet revolution of 2018 that led to the resignation of the Prime Minister. The hashtags #MyStep and #MerzhirSerzhin were used to share information, and mobilise citizens and gather their support. Many other movements across the world are supported by social media, as demonstrated by the #BlackLivesMatter movement in the US, the #RoadSafetyMovement in Bangladesh, the #FeesMustFall campaign in South Africa, and the #FridaysForFuture and the #ClimateStrikes global movement (UN-OHCHR, 2019[7]).

conflict. This online social campaign was able to gain international support and inspired the creation of the #BringBackOurStudents movement in Ethiopia (Global Citizen, 2017[13]).

Moreover, digital transformation has enhanced opportunities for regional and international institutions to consult citizens and organised civil society globally. Individuals and CSOs can now provide virtual inputs into or advocate for community-driven alternatives not only in national but also regional and international policy and decision-making processes (OECD, 2019[14]). The UN global survey on the post-2015 development agenda for example constitutes an unprecedented process of consultation which involved more than 1 million people from all over the world, including civil society, who were empowered to share their ideas about the shape and content of the new sustainable development agenda.[24]

1.1.4. More dynamic civic spaces marked by greater civic activism

In certain places, digital transformation is creating more dynamic civic spaces marked by greater civic activism. As stated in a report published by St George's House, the Corsham Institute and RAND Europe, in contexts where individuals have equal access to digital technologies, these offer "newly enhanced and expanded opportunities for citizens to directly participate in civil society action and in democratic processes more broadly" (RAND Europe, 2017[15]). The OECD has also recognised that ''by increasing accessibility, facilitating freedom of expression, and making it easier to communicate with one's elected representatives, Internet openness can lead to greater civic engagement, more government transparency, and a more informed and vocal public" (OECD, 2016[16]).

Civic activism is being strengthened through the proliferation of digital technologies that enable citizens to hold governments to account, known as civic technologies (or civic tech).[25] Civic tech is facilitating online state-to-public communication and more convenient and improved mechanisms for public participation in democratic processes e.g. electronic voting, e-petitions, participatory budgeting, etc. It is contributing to invigorating citizen activism, increasing transparency, broadening public debate, and revitalising the relationships citizens have with their cities, their communities, their representatives, and governments.[26] For example, '*Better Reykjavík'* is an online consultation forum where citizens are given the chance to present their ideas on issues regarding services and operations of the City of Reykjavik.[27] The 'Plebiscito Digital por Colombia'[28] was a digital referendum made for the Colombians living abroad to cast symbolic

[24] My world 2015: http://vote.myworld2015.org/.

[25] 'Civic tech' is often mentioned along with sister buzzwords like 'smart cities', 'e-gov', 'govtech', 'ICT4D' and 'Tech For Good'. Civic tech embraces all digital tools that enable citizens to easily and effectively engage with civic life, whether that is reporting an issue to a local authority, engaging with elected representatives or monitoring the use of community assets. Civic tech is often — but not exclusively — built by non-profit organisations working for a better, more representative, democratic or functional society. The result is often open source 'tech for good' software that is free or cheap to implement. See: https://tictec.mysociety.org/static/guide-2019.00220a58f9fd.pdf.

[26] The OECD Director of Public Affairs and Communications, Anthony Gooch, refers to the potential of these technologies at the TICTeC (The Impacts of Civic Technology) Conference hosted by the OECD in 2019. TICTeC is an annual conference dedicated to exploring how civic technologies are impacting citizens, institutions and the development of digital participation around the world. See: https://tictec.mysociety.org/static/guide-2019.00220a58f9fd.pdf. The remarks of Anthony Gooch, are accessible here: https://tictec.mysociety.org/2019/presentation/oecd-welcome. See also: https://m.villeintelligente-mag.fr/Civic-Tech%C2%A0-la-technologie-au-secours-de-la-democratie_a426.html.

[27] Visit the 'Better Reykjavík' website here: https://betrireykjavik.is/domain/1.

[28] The digital referendum tested for the first time what's commonly referred as liquid democracy i.e. Instead of giving a voter the binary option of electing a choice, each voter had 100 votes allocated to be placed as they desire on each of the 7 open decisions of the referendum http://plebiscitodigital.co.

votes as part of the official Peace Agreement referendum.[29] Beyond improved communication and public consultation, digital technologies also have the potential to enhance effective government-civil society collaboration.[30] In particular, crowdsourcing and co-design approaches can support new forms of collaboration and engagement, from policy-making to service delivery. As an example, new approaches to government as a platform - through open government data or open source software - can also lead to joint value creation.

1.1.5. More inclusive civic spaces marked by greater civic engagement

The opportunities of digital transformation with the emergence of civic tech are starting to reach previously unserved or underserved areas and populations, resulting in more inclusive civic spaces. In such cases, digital technologies and civic tech are providing online spaces for groups of people that are marginalised or disadvantaged to engage. Depending on the specific local context, these groups can include e.g. women, unemployed youth, ethnic minorities, remote populations, elderly persons, low-income citizens, and people with low levels of education. For example, mobile applications such as GovChat in South Africa, allow for alternative ways of participating in public decision making, and when made accessible to all, are helping to increase civic engagement and participation among all groups of people.[31]

1.2. Negative trends

While digital transformation has brought remarkable opportunities for the enjoyment of the rights to freedom of expression, of peaceful assembly and of association, it has also brought a range of new risks to these very same rights, acting as a double-edged sword. For example: the enhanced flow of information between citizens is counterbalanced by the spread of misinformation and extreme views; the growth of strengthened online communities and particular narratives may fragment and polarise public discourse; the development of digital tools for civic activism and political participation may risk marginalising certain demographic groups who are unable or disinclined to engage to the same degree as others who are better represented (RAND Europe, 2017[15]). As recognised in the OECD Council Recommendation on Artificial Intelligence, “these transformations may have disparate effects ... notably regarding … inequalities, and implications for democracy and human rights, privacy and data protection, and digital security” (OECD, 2019[17]). Across the world, adverse practices are being carried out by a range of actors (i.e. states, companies, consultancy firms, media outlets, even civil society actors themselves) who use - or rather misuse - digital technologies to silence, surveil, manipulate and harass civil society, as well as to express extremist views. Such practices are interfering with civic activism, intimidating and supressing voices of dissent or destroying their credibility and legitimacy, creating incentives for self-censorship and inspiring acts of violence against certain groups. Moreover, digital tech companies control online civic spaces and their current policies and practices fail to meet the necessary safeguards for civic space in terms of transparency and accountability. Finally, in contexts where individuals do not have equal access to digital

[29] More examples can be found in the Open Government Partnership Toolbox, a collaborative platform that gathers digital tools developed and used throughout the world by organisations to improve democracy and promote transparency, participation and collaboration. Read about the toolbox here: https://oecd-opsi.org/toolkits/ogp-toolbox/; access the list of examples here: https://ogptoolbox.org/en/.

[30] Despite growing interest in the potential of digital technologies to enhance coproduction and co-creation in public services, there is a lack of hard evidence on their actual impact. Participation in many of these platforms can be passive (Lember, Brandsen and Tõnurist, 2019[92]).

[31] GovChat is South Africa’s largest civic engagement platform accessible on line, on any mobile handset and feature phones: https://www.govchat.org/.

technologies, new forms of exclusion are proliferating with marginalised groups cut off from the digital space and under-represented in online forums.

1.2.1. Adverse practices carried out by state actors

Across the world, legal restrictions and adverse practices related to the use of digital technologies are being carried out by state actors (in both authoritarian countries and liberal democracies). Internet shutdowns are routinely used to restrict public activism and control the media narrative. Free speech is censored by blocking and controlling the sharing of information digitally. Increased criminalisation of online activity and speech is intimidating and supressing voices of dissent (OECD, 2019[10]). Women journalists and women human rights defenders are particularly targeted. Self-censorship is on the rise among civic activists who are fearful of speaking out. According to a report from Front Line Defenders for example, a new Information Technology Bill considered in Nepal could threaten the freedom of expression on social media (Front Line Defenders, 2019[18]).

Findings from the Digital Society Project dataset[32] indicate that the primary threat to digital civic space comes from the dissemination of false information. This practice is more common in autocratic countries However, both autocracies and democracies are targets of false information spread by foreign governments (Varieties of Democracy (V-DEM) Institute, 2019[11]). Online manipulation and disinformation are used as a tactic to distort electoral processes and public debate, and sometimes as an incitement to violence. As reported by the World Economic Forum, from increased "curated social media experiences to online bots misrepresenting public voices in an online government comment system, the digital information ecosystem is rife with disinformation, distraction, and misrepresentation" (World Economic Forum, 2017[19]). The emergence of so-called "fake news" has highlighted a lack of transparency and accountability mechanisms as digital technologies become more widely used (OECD, 2019[10]). These realities are undermining civic spaces.

The United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association draws a similar conclusion:

> *States are using digital technology to silence, surveil and harass dissidents, political opposition, human rights defenders, journalists, whistle-blowers, activists and protesters; and to* manipulate public opinion, including through misinformation campaigns, cyberattacks and government-sponsored trolling.[33] These tactics aim to intimidate civil society actors, create incentives for self-censorship, destroy their credibility and legitimacy and deny them the attention necessary for mobilisation in the digital space. Governments are ordering Internet and telecommunication services shutdowns and network disruptions more frequently, as well as arbitrarily blocking websites and platforms (including of human rights organisations and political opposition parties) ahead of critical democratic moments such as elections and protests *(UN-OHCHR, 2019[7]).*

The broad and vague language that is often used in national security, public safety and antiterrorism legislation gives leeway for abuses in surveillance. For example, The New York Times reports that Egypt blocked over 500 websites and introduced laws that criminalise criticism of the government on social media. According to The New York Times, the Government invoked national security and public order concerns to restrict online expressions of dissent and arrest online critics (The New York Times, 2019[20]). The outbreak of Covid-19 ("coronavirus") in 2020 and associated global public health emergency have

[32] The dataset is available here: http://digitalsocietyproject.org/.

[33] Government-sponsored trolling and cyberattacks involve: "hacking phones and computers, issuing death and rape threats, disseminating doctored images, hijacking hashtags, spreading conspiracy theories, accusations of treason and promoting virulently discriminatory sentiments. (...) Trolls are instructed to disseminate propaganda, isolate or drown out critical views, and inhibit anti-government movements, while amplifying the messages of government officials and boosting follower numbers" (UN-OHCHR, 2019[7]).

prompted governments to put in place digital surveillance measures to contain the pandemic. While these surveillance tools and measures may be considered necessary during a health crisis, mass surveillance systems used to track infected individuals along with health data disclosure requirements have triggered concerns over the need to balance public safety and personal privacy and civil liberties on a global scale (Carnegie Endowment for International Peace, 2020[21]); (International Center for Not-for-Profit Law, 2020[2]).[34] In its report on Covid-19 and Human Rights, the United Nations pointed out that: "the use of technologies, including artificial intelligence and big data, to enforce emergency and security restrictions or for surveillance and tracking of impacted populations raise concerns (United Nations, 2020[22])." The UN's report further noted that "the potential for abuse is high: what is justified during an emergency now may become normalised once the crisis has passed. Without adequate safeguards, these powerful technologies may cause discrimination, be intrusive and infringe on privacy, or may be deployed against people or groups for purposes going far beyond the pandemic response" (United Nations, 2020[22]). In particular, the UN report highlighted that sometimes under the pretext of fake news, journalists, activists or political opposition were being arrested. Online surveillance and aggressive cyber policy are on the increase. "Sweeping efforts to eliminate misinformation or disinformation can result in purposeful or unintentional censorship that underpins trust" (United Nations, 2020[22]).

Violations of civic freedoms are exacerbated by the availability and use of new forms of digital surveillance technology, including artificial intelligence (AI), closed-circuit television (CCTV)[35], and facial recognition programmes. For example, predictive policing[36] allows police to disrupt peaceful protests before they begin.[37] When demonstrations do occur, facial recognition enables police to identify protesters so that they can be detained and questioned (Open Global Relations, 2018[23]). The social media platform WhatsApp, popular for organising and communications, is sometimes weaponised against civic activists. According to Front Line Defenders, for example, Tibetan activists were sent WhatsApp messages purporting to be from non-government organisations (NGOs) and journalists which contained links designed to allow for the installation of spyware on their phones if clicked.[38]

Mass surveillance and data collection also take place through mandatory sim card registration and data intensive collection of biodata information (for example, by national registries and electoral commissions) (ICNL, CSRG, CIPESA, 2019[24]). An article from Foreign Policy reports about the Chinese Social Credit System which uses digital technologies to monitor the behaviour of the country's population, ranking people based on their social credit. According to the article, people with low scores are facing travel bans and restricted access to schools and jobs among other things (Foreign Policy, 2018[25]). With the growth of smart cities and networked devices, data can be collected from smartphones, Iot components in common spaces, sensors spread in garbage cans, street lights, or retail screens (Tactical Tech, n.d.[26]).

[34] Read Lawfare's article 'Government surveillance in an age of pandemics' (March 2020): https://www.lawfareblog.com/government-surveillance-age-pandemics.

[35] CCTV: a system that sends television signals to a limited number of screens, and is often used in shops and public places to prevent crime.

[36] Monitoring of social media to predict when protects and civil unrest will take place.

[37] Spyware digital technology is used to infiltrate social media groups and hack into civil society actors' online communications and activities, and in some cases arrest them before peaceful protests take place.

[38] Front Line Defenders 2019 global analysis report is available here: https://www.frontlinedefenders.org/sites/default/files/global_analysis_2019_web.pdf.

Table 1.1. Rising digital authoritarianism, by the numbers

8 Consecutive years of global Internet freedom declines.
In the past year, at least 17 countries approved or proposed laws that would restrict online media in the name of fighting "fake news" and online manipulation.
18 out of 65 countries have passed new laws or directives to increase state surveillance since June 2017, often eschewing independent oversight and exposing individuals to persecution or other dangers to gain unfettered access to data.
Of the 65 countries assessed, 26 have been on an overall decline since June 2017, compared with 19 that registered net improvements. The biggest score declines took place in Egypt and Sri Lanka, followed by Cambodia, Kenya, Nigeria, the Philippines, and the Bolivarian Republic of Venezuela.

Source: (Freedom House, 2018[27]) Freedom on the Net 2018: The Rise of Digital Authoritarianism, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Table 1.2. Global Internet user statistics

Nearly 3.8 billion people have access to the Internet.

71% live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.
56% live in countries where political, social, or religious content was blocked on line.
65% live in countries where individuals have been attacked or killed for their online activities since June 2018.
59% live in countries where authorities deployed pro-government commentators to manipulate online discussions.
46% live in countries where access to social media platforms was temporarily or permanently restricted.
46% live in countries where authorities disconnected Internet or mobile networks, often for political reasons.

Source: (Freedom House, 2019[28]), Freedom on the Net 2019: the crisis of social media, https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf.

1.2.2. Adverse practices carried out by other actors

Adverse practices are being carried out by other actors who use technologies in ways that curtail civic freedoms, manipulate public opinion and spread misinformation or hate speech. Examples include:

- **Infringement of privacy by media outlets.** For example, in 2011, employees of the Rupert Murdoch News Corporation newspaper engaged in phone-hacking activities in the pursuit of stories.[39]
- **Data abuse by consultancy firms**. For example, in 2018, Cambridge Analytica had harvested the personal data of millions of peoples' Facebook profiles without their consent and used it for political advertising purposes in the United States.[40] It is also accused of having used digital tools and data to influence the 2017 elections in Kenya.[41]

[39] Read more about the phone-hacking scandal here: https://en.wikipedia.org/wiki/News_International_phone_hacking_scandal.

[40] Read more about the Facebook–Cambridge Analytica data scandal here: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.

[41] Read about how Cambridge Analytica interfered in the Kenyan elections here: https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/.

- **Online astroturfing[42] or "cyberturfing"[43] by corporations** (as well as other actors). For example, Wal-Mart was suspected of cyberturfing when its public relations firm created a blog called "Working Families for Wal-Mart" in order to counter the negative press Wal-Mart had received on line (European Journal of Law and Technology, 2016[29]).
- **Adverse forms of civic activism carried out by individuals, extremist and hate groups.** Digital technologies are sometimes negatively affecting the quality of discourse and civic engagement. Through online digital tools, individuals inclined towards xenophobia, racism, intolerance, misogyny, or homophobia have found niches that can reinforce their views and inspire acts of violence. Social media and other digital forms of communication are being exploited as platforms for bigotry to spread hateful and incendiary rhetoric, inciting violence against women, the lesbian, gay, bisexual, transgender, queer, questioning and intersex (LGBTQI) community, and ethnic and religious minorities, among other groups. For example, according to an article from the Council on Foreign Relations, a correlation was found between anti-refugee Facebook posts by the German far-right party and attacks on refugees in Germany (Council on Foreign Relations, 2019[30]). Social media platforms also offer violent actors the opportunity to publicise their acts. For example, the white nationalist/supremacist gunman who opened fire in a mosque in Christchurch, New Zealand in March 2019, filmed the entire crime and live-streamed it directly to Facebook (BBC News, 2019[31]). Societies are now struggling to reconcile the values of free expression with prevention of hate speech and dissemination of terrorist content on line. In the context of the Covid-19 pandemic, the virus has had a disproportionate impact on certain communities through the rise of hate speech and the targeting of vulnerable groups (such as migrants, refugees and internally displaced persons), facilitated by social media and other digital tools. The use of phrases such as "foreigner's disease" to describe the virus, the UN has warned, is leading to discrimination, xenophobia, racism and attacks (United Nations, 2020[22]).

1.2.3. Harmful behaviour of digital technology companies

The behaviour of digital tech companies is also harming civic space. The fact that online civic space is controlled by digital tech companies is challenging CSO's independence and legitimacy, increasingly putting their work, their resources and their activists under threat (CONCORD Europe, FOND Romania, 2018[32]). According to the report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, civic freedoms on line are dependent on "business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms affect these freedoms" (UN-OHCHR, 2019[7]). Dominant online platforms and social media companies such as Facebook, Twitter, WhatsApp and YouTube – and the Chinese equivalents such as Weibo, WeChat, Youku - have become important gatekeepers to people's ability to enjoy the rights to freedom of peaceful assembly and of association, wielding enormous power over whether and how individuals and civil society actors can access and participate in this online democratic space (UN-OHCHR, 2019[7]).

---

[42] Definition of astroturfing: organised activity that is intended to create a false impression of a widespread, spontaneously arising, grassroots movement in support of or in opposition to something (such as a political policy) but that is in reality initiated and controlled by a concealed group or organisation https://www.merriam-webster.com/dictionary/astroturfing.

[43] Cyberturfing is the un-attributable and undetectable manipulation of online content which aims to amplify or suppress information or certain narratives and misleadingly present them as grassroots. With cyberturfing, digital tools are used to manufacture false consensus and give the illusion of popularity or disapproval. By falsely representing popular sentiment, usually for political or marketing purposes to influence voter or consumer behaviour, a bandwagon effect is created, whereby civic engagement is weaponised (Maplight, 2019[34]; Quartz, 2018[78]).

By and large, tech companies and Internet service providers are left unchecked (Open Government Partnership, 2019[33]), leveraging digital technologies to control information to pursue their own corporate and commercial interests, sometimes in collusion with repressive governments, for the sake of profit.[44] The goals of commercial operators and tech companies do not always coincide with the goals of activists using social networks for expression, assembly and association.

A handful of platforms are building the codes and algorithms that ultimately define which opinions or ideas are shared, how online content is managed, and what values are protected or banned, without any sort of accountability. Content is controlled by internet intermediaries, who apply their own, internally drafted rules on what civil society may or may not say and how civil society can appeal blocking or takedown of information (European Center for Not-for-Profit Law, 2020[8]). The digital tools and platforms they govern present risks related to data protection, algorithmic bias[45], increased discrimination[46] and infringement of privacy[47], undermining the security of civil society.[48]

In the same vein, companies providing digital communications services are also dominating the online environment for freedom of expression. The control of private companies, and particularly social media, search platforms and other intermediaries, over digital communications combined with the abuse of market dominance of online advertising companies, represent a threat to free expression. The power over content creation and distribution channels is in the hands of very few, and so is the ability of platforms to influence public debate. There are many reports of companies abusing transparency by sharing personal data information for targeted paid digital advertising that seek to manipulate public opinion (Maplight, 2019[34]). The fact that digital tech companies are dependent on advertising companies creates an environment which can also be used for viral dissemination of disinformation and hateful expression (OSCE, 2019[35]). According to Jim Balsillie, former co-CEO of Research In Motion and co-founder of the Council for Canadian Innovators: “the online advertisement-driven business model subverts choice and represents a foundational threat to markets, election integrity, and democracy itself”.[49]

---

[44] Companies around the world often fail to adequately disclose information about data collection and governments’ requests for access to users’ data for surveillance purposes. See Ranking Digital Rights 2018 Corporate Accountability Index: https://rankingdigitalrights.org/index2018/.

[45] Algorithmic organisation of online content (sometimes termed the ‘filter bubble’ or ‘echo-chamber’ effects) is an automated process, which flags content for takedown and influences the findability, visibility and accessibility of material. Algorithms learn from data sets that contain historical bias for factors like race and gender, they start to exhibit those biases and even strengthen them. Algorithms have a disproportionate effect on already marginalised or at-risk groups, including women. Marginalised groups and communities find themselves discriminated against by algorithmic decision processes (UN-OHCHR, 2019[7]).

[46] Content policies of social media companies may not be compliant with international human rights standards and norms. This gives rise to risks of arbitrary and discriminatory content removal and account suspension or deactivation (UN-OHCHR, 2019[7]).

[47] User privacy and security of communications also affect online expression and the rights to freedom of peaceful assembly and association. Only a few digital technology companies allow the use of pseudonyms or other ways to mask an individual’s identity, or provide for encrypted communications. Interferences with the use of encryption and anonymity technologies are increasing (UN-OHCHR, 2019[7]).

[48] Cybersecurity threats loom over the civil society sector, as hackers have increasingly targeted charities and other non-profits who collect personal, financial, and genetic data. Data theft by corporate bodies becomes more frequent, putting at risk the privacy and security of civilians (OECD, 2019[10]).

[49] See the full testimony of Jim Balsillie at the hearings of the International Grand Committee on Big Data, Privacy and Democracy held in Ottawa: https://nationalpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium/wcm/8b03e6c0-a8a3-40f6-885e-f367bfb866f1.

Table 1.3. Ranking digital rights

Companies fall short in four key areas

Privacy	Security	Expression	Governance
Companies fail to disclose enough about what user information is collected and shared, with whom, and under what circumstances.	Companies provide insufficient evidence of measures to protect users' information.	Companies keep the public in the dark about how content and information flows are policed and shaped through their platforms and services.	Too few companies make users' expression and privacy rights a central priority for corporate oversight, governance, and risk assessment.

Note: The index evaluates 22 of the world's most powerful Internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting freedom of expression and privacy.
Source: (Ranking digital rights, 2018[36]) , Corporate Accountability Index, https://rankingdigitalrights.org/index2018/ .

Overall, the majority of companies including tech giants such as Google, Amazon and Apple fall short in complying with the Global Data Protection Regulation (TechRadar, 2019[37]). Many fail to ensure the respect of users' freedoms in their policies and practices. For example, Global Voices Advocacy (Advox)[50] reported that Google took down videos promoting a protest rally against an unpopular pension reform law in order to comply with a demand from the Russian Federation's (hereafter 'Russia') government authorities.[51]

1.2.4. New forms of exclusion

Unequal access to and usage of digital technologies are creating new forms of exclusion and inequality and amplifying existing ones. While digitalisation offers the opportunity to overcome many forms of economic inequality and social exclusion in contexts where individuals have equal access to digital technologies (see point 1.1.5), in places where this is not the case, new divisions are proliferating. Tim Unwin[52] wrote an article for the OECD's Development Matters blog in which he argues that the digital age has given further rise to tendencies of concentration of power and that "instead of improving the lives of the poorest and most marginalised, such technologies have actually dramatically increased inequality at all scales, from the global to the local" (Unwin, 2019[38]).

The so-called "digital divide" exists *between* nations that have the infrastructure, funds, talent pool, and policy environment to adapt quickly to digital transformation and those that do not, with developing nations being hit harder (Charities Aid Foundation, 2018[39]). According to the International Telecommunication Union (ITU), only 24% of the population in Africa has access to the Internet versus 80% in Europe (ITU, 2018[40]).

The digital gap exists *within* nations also, between connected, urban groups and low-income urban and rural groups (OECD, 2019[14]). Divisions are related to income and education levels, as well as generational and gender gaps. In the African context, fewer women and marginalised communities are active in online spaces, and they are specially and disproportionately affected by such barriers (ICNL, CSRG, CIPESA, 2019[24]). An article from the World Economic Forum reports that women who face cultural barriers are up to 50% less likely to be connected; people with low levels of education lack the skills to use digital

[50] Advox is a global network of bloggers and online activists dedicated to protecting freedom of expression and free access to information on line.

[51] Read the full article of Advox here: https://advox.globalvoices.org/2018/09/10/google-caves-in-to-russian-demands-censors-videos-promoting-a-protest-rally/.

[52] Chairholder, UNESCO Chair in ICT4D, Royal Holloway, University of London, and Co-Founder of TEQtogether.

technologies, and people who live below the international poverty line are not able to afford them (World Economic Forum, 2016[41]). An example highlighted in an article from The Good Things Foundation concords with these findings, stating that a social media tax in Uganda has negatively impacted the ability of users, particularly low-income citizens, to gain affordable access to the Internet (Lawley, 2019[42]). Availability and access to digital information at an affordable cost and quality have long been a concern for many disadvantaged groups. Barriers brought by the digital divide are linked to the increasing costs and commercialisation of online spaces. Global broadband-internet user penetration is at 51% (Broadband Commission for Sustainable Development, ITU, UNESCO, 2019[43]). This means that almost half of Internet users do not have access to high-speed wireline or wireless services. These gaps persist across all kinds of places from small towns to urban neighbourhoods, and among demographic groups of all races, educational attainments, and income levels.

In a digital age where civic freedoms are increasingly exercised online, individuals who don't have Internet access are automatically cut off from the digital space. Almost 4.5 billion people were active Internet users as of June 2019, encompassing 58% of the global population.[53] This means that 42% - a little less than half of the world's population - are still not using the Internet. This puts them at a serious structural disadvantage as they are prevented from exercising their digital rights on the same footing as those who are connected (OECD, 2019[10]). Moreover, discrepancies in the use of digital technologies by distinct demographic groups lead to certain groups being disproportionately represented (over or under-represented) in civic spaces and online governance forums. This undermines the democratic principle of inclusive representation of all of the people in such forums (OECD, 2019[14]).

[53] Internet world stats: https://www.internetworldstats.com/stats.htm.

2. Drivers of change and uncertainties

Building on the findings from the analysis of civic space trends related to digital transformation (Chapter 1), Chapter 2 proceeds with identifying and outlining key drivers of change and uncertainties that could determine the future trajectory of civic space in the face of digital transformation. A driver of change is a factor causing change, affecting or shaping the future. Drivers can be characterised as direct or indirect (i.e. underlying). A direct driver influences an outcome in the system in an unambiguous way. An indirect driver – also called a moderating or mediating variable - acts more diffusely, changing one or more direct drivers (Forward Thinking Platform, 2014[3]). In this paper, drivers of change include both mega-trends, emerging patterns and early signals.[54] As for the uncertainties, these are questions that arise resulting from a state of having limited knowledge about the future. The analysis of the current trends covered in Chapter 1, combined with the analysis of drivers of change and uncertainties covered in this Chapter, and the study of the logical interactions between these variables are at the heart of the scenario-building process which is addressed in the following chapter.

2.1. What is expected for the future of civic space: Mega-trends[55]

The following mega-trends (i.e. major trends that occur at a large or global scale) can be observed in relation to digital transformation, as well as in relation to civic space in the context of digital transformation:

2.1.1. Mega-trends related to digital transformation, with implications for civic space

- A more highly educated citizenship could become increasingly interested and engaged in the debates around the direction of science, technology and innovation (STI) developments, particularly with regards to associated benefits, risks and values (OECD, 2016[44]).
- Innovation will increase inequality as benefits predominantly accrue to innovators and possibly their customers.[56] For all actors in society to benefit, innovations must diffuse (OECD, 2016[44]).
- Furthermore, most new technologies require new sets of skills to use. This will possibly contribute to unemployment and inequality, and highlights the need for skills training (OECD, 2016[44]).
- On the other hand, technologies can directly promote social inclusion and economic growth, e.g. digital technologies have opened up access to education, financial services and other knowledge-based services (OECD, 2016[44]).
- Globalisation will continue to facilitate the wide diffusion of knowledge, technologies and new business practices and will itself be deepened by this diffusion (OECD, 2016[44]).
- Governments will continue to collect and increasingly make open large amounts of data that are useful for research and innovation (OECD, 2016[44]).

[54] See Annex A for more definitions.

[55] See Annex A for the definition of mega-trends.

[56] This is not only an "innovators" game; new barriers to entry and rents are also emerging.

- Governments are themselves innovating, conducting experiments and relying increasingly on digital technologies for policy formulation, delivery and evaluation (OECD, 2016[44]).
- With the emergency adoption of machine learning in several sectors of the economy, society and even government, auditing and holding institutions accountable may prove challenging due to the nature and complexity of these technologies (European Parliamentary Research Service - Scientific Foresight Unit, 2019[45]).
- The growing maturity and convergence of digital technologies are likely to have far-reaching impacts on productivity and income distribution (OECD, 2016[44]).
- New mega-trend: In emergencies like a global pandemic such as Covid-19, digital technologies have become critical to helping societies effectively deal with the outbreak. Their use is weighed against other considerations, including risks presented by digital surveillance measures enacted by countries, in order to strike a balance between public health needs and people's privacy and fundamental freedoms (Forbes, 2020[46]).

Box 2.1. The use of digital technologies in the emergency response to control the outbreak of Covid-19

Countries all around the world have turned to digital technologies in the battle against Covid-19. Their use spans a wide spectrum of applications: from assisting in locating people with symptoms, monitoring and tracking the spread of the disease (e.g. through the use of mobile phones for contact tracing), to enforcing quarantines and stopping the spread of fake news or misinformation.[57]

In **Korea**, government agencies have harnessed surveillance-camera footage, smartphone location data and credit card purchase records to help trace movements of coronavirus patients and establish virus transmission chains. Detailed location histories on each person who tested positive for the coronavirus were posted on line.[58]

In **Singapore**, the government maintains an online dashboard that provides detailed information about each positive Covid-19 case. The Ministry of Health posts information on line about each coronavirus patient. The idea is to warn individuals who may have crossed paths with them, as well as alert the public to potentially infected locations. Singapore also introduced a smartphone application for citizens to help the authorities locate people who may have been exposed to the virus. The application, called TraceTogether, uses Bluetooth signals to detect mobile phones that are nearby. If an application user later tests positive for the virus, the health authorities may examine the data logs from the application to find people who crossed their paths. The application preserves privacy by not revealing users' identities to one another. [59]

In **China**, citizens are required to use software on their phones that automatically classifies each person with a colour code — red, yellow or green — indicating contagion risk, based on their travel history and self-reported health condition. The software determines which people should be quarantined or permitted to enter public places like subways.[60] Disinfecting robots (deployed to complete tasks such as cleaning and sterilising and delivering food and medicine to reduce the amount of human-to-human contact i.e. contactless delivery), smart helmets (that can measure the temperature of anyone within a 5 metre radius), thermal camera-equipped drones and advanced facial recognition software are all being deployed in the fight against Covid-19 to scan crowds for fever/detect temperatures and identify individuals not wearing masks.[61] Drones have been deployed to transport medical samples and conduct thermal imaging.[62]

In **Lombardy, Italy**, the authorities are analysing location data transmitted by citizens' mobile phones to determine how many people are obeying the government lockdown order and the typical distances they move every day.[63]

Israel approved emergency measures for its security agencies to deploy surveillance technology normally reserved for battling terrorists to track the mobile-phone data of people with suspected coronavirus. Location data collected through telecommunication companies by the domestic security agency, is shared with health officials. Once an individual is highlighted as a possible coronavirus case, the health ministry will then be able to track whether or not they are adhering to quarantine rules.[64]

The **United Kingdom** is developing a smartphone application that would notify individuals who may have come into contact with those infected with the coronavirus.[65] People would sign up for the programme and would agree to share their location data on a voluntary basis and out of a sense of civic duty.[66]

In the **United States**, discussions between technology companies and the White House have focused on using large amounts of anonymous, aggregated location data captured from Americans' mobile phones to conduct general public health surveillance, including by tracking whether people are keeping

one another at safe distances to stem the outbreak; and to anticipate where more serious outbreaks are likely to occur.[67]

The Government of **Brazil** has created an application to offer health information to citizens. [68]

Sweden has quickly developed a new education platform that will offer resources for children who can no longer attend school.[69]

Canadians have created a platform that allows people to post #ISO posts ('in search of' help requests), or #offer posts, enabling people to acquire important medical or household goods that they may not have been able to find for health or mobility reasons.[70]

[57] Read Lawfare's article 'Government surveillance in an age of pandemics' (March 2020): https://www.lawfareblog.com/government-surveillance-age-pandemics.

[58] Read more about this in The New York Times article 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' (March 2020): https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

[59] Read more about this in The New York Times article 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' (March 2020): https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

[60] Read more about this in The New York Times article 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' (March 2020): https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

[61] Read more about this in Forbes' article 'Coronavirus: How Artificial Intelligence, Data Science And Technology Is Used To Fight The Pandemic'(March 2020): https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/#74f82b365f5f.

[62] The BBC reports about this in the article 'Coronavirus: China's tech fights back' (March 2020): https://www.bbc.com/news/technology-51717164.

[63] Read more about this in The New York Times article 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' (March 2020): https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

[64] Read the BBC article (March 2020) 'Coronavirus: Israel enables emergency spy powers' for more information about this: https://www.bbc.com/news/technology-51930681.

[65] Read Lawfare's article 'Government surveillance in an age of pandemics'(March 2020): https://www.lawfareblog.com/government-surveillance-age-pandemics.

[66] Read more about this in The New York Times article 'Translating a Surveillance Tool into a Virus Tracker for Democracies' (March 2020): https://www.nytimes.com/2020/03/19/us/coronavirus-location-tracking.html.

[67] Read more about this in The Washington Post's article 'U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus' (March 2020): https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/.

[68] The application is available here: https://play.google.com/store/apps/details?id=br.gov.datasus.guardioes&hl=en_US.

[69] Read more about this in OECD's Observatory of Public Innovation blog 'Innovation in the Time of Coronavirus' (March 2020): https://oecd-opsi.org/innovation-in-the-time-of-coronavirus/.

[70] Read more about this in OECD's Observatory of Public Innovation blog 'Innovation in the Time of Coronavirus' (March 2020): https://oecd-opsi.org/innovation-in-the-time-of-coronavirus/.

Liberia is preparing for Covid-19 with mHero, a two-way communication platform that connects the Ministry of Health with frontline health workers in even the remotest regions, allowing for real-time information exchange and a more effective outbreak response. Alerts starting at the facility level can be sent to District Surveillance Officers and up through the health system to the Central Ministry. The Central Ministry of Health can also send out information to frontline health workers – all disaggregated by cadre or by county for targeted information or educational messages.[71]

Nigeria is deploying CommCare, a mobile data collection platform, for patient risk assessments and contract tracing to contain the potential spread of Covid-19.[72]

Globally, the World Health Organization (WHO), UNICEF and UNDP partnered with WhatsApp to launch a messaging service for real time health updates with the potential to reach billions of people. The aim is also to curb the spread of fake or misinformation about the coronavirus pandemic.[73]

2.1.2. Mega-trends related to civic space in the context of digital transformation

- The opportunities or threats that digital transformation presents to civic space will increase as emerging technologies develop and become more common. Digital technologies "are proliferating so quickly, in such a multitude of directions all over the globe, that it is hard to keep track of the changes afoot let alone their implications. (...) Much will depend on which technologies take precedence and who will control them and to what ends" (CONCORD Europe, FOND Romania, 2018[32]).
- Diverse forms of hybrid civic activism will take root across the world. New and older forms of civic activism will coexist and intertwine in a variety of ways across the different online and offline civic spaces; they will interact and influence each other. New forms of digital activism will supplement traditional forms; they will either harness or be harnessed by the more traditional forms of activism (Carnegie, 2017[47]).
- If a technology is sufficiently powerful and widespread, then people's ability to make use of it will become a fundamental dividing line. The likelihood is that people will continue to become increasingly dependent on digital technologies so there could be a stark inequality between those who are able to access digital technologies and those who are not able to (Charities Aid Foundation, 2018[39]).
- Digital transformation is impacting the future of employment and work; the way CSOs work is no exception to this rule. CSOs are just starting to leverage the opportunities of digital transformation for their work and have yet to explore its full potential; from using drones and satellite technology to detect violations of human rights to mobile phone data informing humanitarian responses, CSOs are finding ways to harness digital technologies to achieve their goals and act for the public good. Many CSOs use virtual reality as a medium for communication and advocacy (i.e. Amnesty

[71] Read more about this in the article of ICT Works 'Three Early Digital Health Covid-19 Response Success Stories' (March 2020): https://www.ictworks.org/digital-health-covid-response-success-stories/#.XoDeFfZuI2z.

[72] Read more about this in the article of ICT Works 'Three Early Digital Health Covid-19 Response Success Stories' (March 2020): https://www.ictworks.org/digital-health-covid-response-success-stories/#.XoDeFfZuI2z.

[73] Read more about this on UNDP's webpage: https://www.undp.org/content/undp/en/home/news-centre/news/2020/COVID-19_WHO_UNICEF_UNDP_Partner_with_WhatsApp_to_Get_Real_Time_Health_Information_to_Billions_around_the_World.html.

International's Syrian Arab Republic ("Syria") 360 project[74]); camera apps (eyeWitness) to capture verifiable footage related to human rights violations with images that can be used in investigations or trials[75]; and blockchain technology[76] for better documentation of land titles to strengthen marginalised groups, such as women's right to hold land and property in countries with a lot of corruption (DanChurchAid & DareDisrupt, 2019[48]).[77]

2.2. What is new about the future of civic space: Emerging patterns and early signals[78]

New patterns (i.e. new trends or novel situations created by the same repeating signals of change) and early signals related to civic space are emerging in connection with digital transformation:

- The fabric of civil society is changing through digital tools and platforms which allow more organic and fluid mobilisations (OECD, 2019[14])**.** More fluid and informal civic actors, including large-scale, global social movements, engaging on an ad-hoc basis, are proliferating all over the world, alongside more institutionalised forms of civic engagement (European Economic and Social Committee, 2017[49]). The socio-political arena in which social movements operate is a combination of local, national and supranational elements - product of a globalised society - characterised by greater inclusion, interdependence and mobility. With globalisation, there are very few people's lives in the world today that remain hermetic to international forces; this interdependence favours the dissemination and mutual reinforcement of collective expressions, and mobility ensures the fluidity of ties between societies.[79]
- It is likely that future advances in technologies particularly around AI (machine learning and big data) will continue to come from authoritarian countries where human rights frameworks and rule-of-law protection are not as prevalent as they are in other parts of the world. Today China has become one of the major drivers of AI surveillance worldwide.[80] Technology linked to Chinese companies, particularly Huawei, Hikvision, Dahua, and ZTE, supply AI surveillance technology in 63 countries (Carnegie Endowment for International Peace, 2019[50]).
- The growing role that authoritarian countries play in digital transformation multiplies the risks of data-driven digital systems being increasingly built to govern citizens in a way that restricts

[74] Find out more about Amnesty International's Syria 360 project here: http://www.360syria.com/intro.

[75] The rise of mobile phones and social media provides a new stream of data for documenting human rights violations.

[76] The term blockchain technology refers to the transparent, publicly accessible ledger that allows to securely transfer the ownership of units of value using public key encryption and proof of work methods. The technology uses decentralised consensus to maintain the network, which means it is not centrally controlled by a bank, corporation, or government. In fact, the larger the network grows and becomes increasingly decentralised, the more secure it becomes. See: https://support.blockchain.com/hc/en-us/articles/211160223-What-is-blockchain-technology-. It is simply defined as a decentralised, distributed ledger that records the provenance of a digital asset. See: https://builtin.com/blockchain.

[77] Blockchain may enable to make paperwork and physical contracting digital, and smoother systems without increasing the risk of someone tampering with the data.

[78] See Annex A for the definition of emerging patterns and early signals.

[79] This point is drawn from Bertrand Badie's theses on globalisation available here: https://www.lemonde.fr/idees/article/2019/11/08/bertrand-badie-l-acte-ii-de-la-mondialisation-a-commence_6018418_3232.html

[80] China has articulated its ambitions to lead the world in AI by 2030 (Lawfare, 2017[53]).

freedoms and contributes to civic spaces that are less free, less open and less safe (Digital Civil Society Lab - Stanford PACS, 2017[51]).[81] The Journal of Democracy reports that China's efforts to build sophisticated AI capabilities for social control, along with the proliferation of such technology to other authoritarian regimes, present serious long-term risks to civic space (Journal of Democracy, 2019[52]); (Lawfare, 2017[53]). As documented by Freedom House, China is now exporting its model of comprehensive Internet surveillance around the world, offering training, seminars, and study trips as well as advanced equipment that takes advantage of artificial intelligence and facial recognition technologies (Freedom House, 2018[27]).

- The confirmation of China as the global digital power could mean that markets and policies framing emerging technologies would drift away from democratic countries' influence and control and with this, so would the means of exerting influence and authority in terms of impacting decision and policy making to protect civic space.[82] In sum, the continuing trend of rising digital authoritarianism witnessed in countries like China and Russia will likely weaken democratic models of digital governance. A cohort of countries is already moving toward digital authoritarianism by embracing the Chinese model of automated surveillance systems (Journal of Democracy, 2019[52]).
- While governments in autocratic and semi-autocratic countries are more prone to abuse AI surveillance for repressive purposes than governments in liberal or advanced democracies, all political contexts present and will continue to present cases of unlawful exploitation of AI surveillance technology (Carnegie Endowment for International Peace, 2019[50]). An article from The Guardian states that the use of AI surveillance technology is becoming the global norm, even in advanced democracies, and that it is actually most widespread in democracies (The Guardian, 2019[54]). [83]
- In fact, the misuse of digital technologies that threaten civic space are not only coming from authoritarian countries but also from the so-called "liberal democracies"[84]. According to Carnegie, AI surveillance technology supplied by US firms is present in 32 countries. The most significant US companies are IBM, Palantir, and Cisco. Other companies based in liberal democracies such as France, Germany, Israel, and Japan, are also playing important roles in proliferating this technology. The next largest non-Chinese supplier of AI surveillance technology is Japan's NEC

[81] China's global digital governance agenda and vision is laid out in its AI plan and already calls for the use of AI to enhance "social management" such as automating surveillance. The AI Plan (English translation) can be accessed here: https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/.

[82] If China successfully expands the set of countries following its approach to the Internet, there will be a growing base of support for China's "cyber sovereignty" principles in global governance forums (Center for American Progress, 2019[74]).

[83] Liberal democracies are major users of AI surveillance. The index shows that 51% of advanced democracies deploy AI surveillance systems. In contrast, 37% of closed autocratic states, 41% of electoral autocratic/competitive autocratic states, and 41% of electoral democracies/illiberal democracies deploy AI surveillance technology (Carnegie Endowment for International Peace, 2019[50]).

[84] McGill University definition: "Liberal democracy is a form of government. It is a representative democracy in which the ability of the elected representatives to exercise decision-making power is subject to the rule of law, and usually moderated by a constitution that emphasizes the protection of the rights and freedoms of individuals, and which places constraints on the leaders and on the extent to which the will of the majority can be exercised against the rights of minorities. The rights and freedoms protected by the constitutions of liberal democracies are varied, but they usually include most of the following: rights to due process, privacy, property and equality before the law, and freedoms of speech, assembly and religion. (...) The states of the European Union, Japan, the United States, Canada, India, South Africa, Australia, and New Zealand are considered liberal democracies." See: https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/l/Liberal_democracy.htm.

Corporation (Carnegie Endowment for International Peace, 2019[50]). Google and Amazon are building cloud computing servers for government surveillance and the UK arms firm BAE is providing mass monitoring systems (The Guardian, 2019[54]). In her recent book, *The Age of Surveillance Capitalism*, Shoshana Zuboff describes how global tech companies such as Google and Facebook gather personal information/data to predict, influence, and modify peoples' behaviour, with disastrous consequences for democracy, human rights and civic freedoms.[85]

- The current economic and political forces that govern and regulate the digital space - through government restrictions, the frameworks of the dominant digital platforms, and other digital threats and vulnerabilities - do not make it inviting nor safe for civil society. A growing "chilling effect"[86] among civil society actors is deterring them from exercising their rights online. For example, The Guardian reports that Facebook's usage has plummeted over the last year, and that this decline coincided with a series of data, privacy and hate speech scandals.[87] An article from the European Digital Rights Association reported that the surveillance of Grindr, the biggest social networking digital application for the LGBTQI community in Egypt, led to individuals being imprisoned for illegal sexual behaviour, consequently the community became reluctant to use the app (EDRi, 2019[55]). The lack of transparency in how technology is used, who can access it, and how data collection/storage is undertaken are increasing the exposure and vulnerability of CSOs, media, and activists, who are becoming more and more aware of these shortfalls. In many jurisdictions, there are inadequate or no data protection laws to address risks, and little to no independent oversight of these processes. The legal framework is inadequate to deal with the proliferation of surveillance technology and data collection; and regulators, lawyers and judiciaries are not equipped to address the human rights violations. These challenges are deterring civil society actors particularly in repressive contexts from using digital technology to exercise and assert their rights and freedoms on line (ICNL, CSRG, CIPESA, 2019[24]).
- The majority of national institutions, rules, and regulatory frameworks are currently not designed to adequately deal with any of the emerging challenges related to digital technologies and civic space. Despite the existence of international frameworks and tools to guide digital governance and regulation including data privacy, protection and security (e.g. UN-OHCHR Guiding Principles on Business and Human Rights, the EU General Data Protection Regulation, and the OECD Recommendation of the Council on Artificial Intelligence; see the example of UNESCO's ROAM-X indicators in Box 2.1), adherence to these is limited. Rather, countries and regions are starting to develop their own response to the global discourse, and adopting disparate approaches toward oversight and regulation of digital technologies and tech giants, different digital security norms, and different Internet landscapes and infrastructure (see examples of national digital regulations and data governance approaches in Box 2.2). The different approaches to Internet and digital regulation and data governance are creating discrepancies in terms of access to, security, and usage of digital tools and online platforms by civil society.

[85] Information about The Age of Surveillance Capitalism is available here: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy.

[86] A discouraging or deterring effect, especially one resulting from a restrictive law or regulation: https://www.collinsdictionary.com/dictionary/english/chilling-effect.

[87] Read the full article from The Guardian here: https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows.

Box 2.2. UNESCO's ROAM-X indicators[88]

Example of an international tool developed to guide digital governance and regulation in a way that protects civic space.

UNESCO developed an indicator framework to measure the Internet's compliance with Human Rights (R), evaluating its Openness (O) and Accessibility (A), and assessing the involvement of multi-stakeholder actors (M) in its governance (ROAM-X Indicators). The ROAM-X indicators framework allows countries, to gain a holistic diagnosis of its Internet policies, digital environment and to what extent they are curbing civic space related rights.

Examples of indicators related to the freedom of association:

Can non-governmental organisations organise freely online?

Indicator: Evidence of online organisation, and absence of undue interference with such organisation.

Examples of indicators related to the freedom of expression:

To what extent is ex ante or ex post censorship of online content undertaken, on what grounds and with what transparency?

Indicator: Quantitative and qualitative evidence of ex ante and ex post censorship of online content.

Are individuals, journalists or other media/online actors subject to arbitrary detention, prosecution or intimidation for disseminating information online?

Indicator: Evidence concerning the extent and nature of arbitrary detentions and prosecutions for online expression.

Do individuals, journalists or other media/online actors practice self-censorship in order to avoid harassment by government or other online actors?

Indicators: Evidence of self-censorship by journalists, bloggers and other media/online actors. Evidence of self-censorship as a result of online abuse, particularly by women and children.

Source: UNESCO (2019), UNESCO'S Internet Universality Indicators: A Framework for Assessing Internet Development, https://unesdoc.unesco.org/ark:/48223/pf0000367617 (UNESCO, 2019[56])

[88] More information about UNESCO's ROAM-X Indicators is available here: https://en.unesco.org/themes/internet-universality-indicators.

Box 2.3. Examples of national digital regulations and data governance approaches

China has the 'Great Firewall', which is used to regulate the Internet within the country by blocking access to certain domestic and foreign websites and slowing down cross-border Internet traffic. The government has invested heavily in monitoring content online by-passing laws on acceptable content. The Personal Information Security Specification ("the Standard") establishes the principle of "data sovereignty" that specifies that all information of citizens must be stored in-country and can be accessed on-demand by the Chinese government (Center for Strategic and International Studies, 2019[57]).

Russian Federation's (hereafter 'Russia') 'sovereign Internet' law tightens Moscow's control over the country's Internet infrastructure and aims to provide a way for Russia to disconnect its networks from the rest of the world. It has been called an online Iron Curtain. In theory, the measure would allow Russia to operate its own internal networks that could run independently from the rest of the world wide web. Russia is seeking to route the country's web traffic and data through state-controlled infrastructure and creating a national system of domain names, reducing reliance on foreign servers.[89]

Other countries are regulating the use of data on social platforms prioritising rights to privacy. The most prominent example of this is the **European Union** General Data Protection Regulation (GDPR) that came into force in 2018. The underpinning precautionary principle of the regulation puts citizen protection, ethics and responsible management before tech innovation.[90]

The **United States** has taken another approach toward regulating its technology giants, prioritising innovation (Center for Strategic and International Studies, 2019[57]). In 2019, a new bill, the Online Privacy Act, was introduced. It creates user rights, places obligations on companies to protect users' data, establishes a new federal agency to enforce privacy protections, and strengthens enforcement of privacy law violations.[91]

Kenya is another country that is stepping up its citizens' digital security with a new EU-inspired data protection law introduced in 2019. The new law outlines restrictions on data handling and sharing by government and corporations. Any infringements of the new law will be investigated by an independent office, with violators facing two-year prison sentences or fines of up to USD 29 000.[92]

The Personal Information Protection and Electronic Documents Act (PIPEDA)[93] in **Canada** governs how private sector organisations collect, use and disclose personal information in the course of commercial business.

Singapore released the Model Artificial Intelligence Governance Framework in January 2019. It acts as a guide for organisations to address key ethical and governance issues when deploying AI technologies, and ensure that decisions made by or with the assistance of AI are explainable, transparent and fair to consumers, and that their AI solutions are human-centric.[94]

[89] Read more about Russia's "sovereign Internet" law here: https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html.

[90] Read more about the European Union General Data Protection Regulation here: https://gdpr-info.eu/.

[91] Read more about the Online Privacy Act here: https://eshoo.house.gov/news-stories/press-releases/eshoo-lofgren-introduce-the-online-privacy-act/.

- Local CSOs operating in repressive physical environments are using online platforms, but they are either unaware of the dangers of online communication, association and assembly, or lack the digital knowledge or skills to use available digital-security tools to protect themselves, e.g. Virtual Private Networks (VPNs), open source[95] tools like Tor for anonymous browsing or Thunderbird for email encryption (DW Akademie, 2018[58]).
- The control of the digital realm by governments and companies is reshaping the foundation and boundaries of civic spaces, and creating new digital dependencies and vulnerabilities for non-profits, foundations, activists, journalists, and others agents of civil society (Digital Civil Society Lab - Stanford PACS, 2017[51]). Civil society is increasingly facing challenges in remaining effective and independent as privately controlled digital platforms and technologies are developed and controlled outside the context of democratic norms (OECD, 2019[10]). The Philanthropy and Digital Civil Society 2019 Blueprint has illustrated this trend with concrete examples:

> *"When algorithms decide the content of a web page, a video feed, and the prominence of certain voices in people's news feed, they are also shaping the bounds of people's associational lives. When companies hold people's identities and networks, and make it difficult if not impossible for them to 'move' to another network, they are defining their associational options. When companies or governments shut down Internet access during a protest, slow down WiFi speeds for certain communities, or refuse to bring broadband access to rural areas, they are locking whole populations out of the digital economic and public square"* (Bernholz, 2018[59]).

- At the same time, despite repression or difficult contexts in which civil society actors operate, civic space continues to subsist, with civil society actors continuing to remain at the forefront of generating positive social and political change.[96] In 2019, civic activists were on the front lines defending and advancing causes in many cities and towns around the world. In many places around the world, civil society groups are expanding their power and influence through the use of digital technology. Digital transformation and the emergence of civic tech are not only impacting civic space but also improving the operating environment of civil society, disrupting the governance and business models of CSOs.[97] With broad and quicker outreach, new potentials for advocacy,

[92] Read about Kenya's data protection law here: https://qz.com/africa/1746202/kenya-has-passed-new-data-protection-laws-in-compliance-with-gdpr/.

[93] Read about the Personal Information Protection and Electronic Documents Act here: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[94] Read about the Model Artificial Intelligence Governance Framework here: https://www.nytimes.com/paidpost/imda/singapores-governing-framework-for-artificial-intelligence.html.

[95] Open source software is software with source code that anyone can inspect, modify, and enhance. Unlike proprietary software, its authors make its source code available to others who would like to view that code, copy it, learn from it, alter it, or share it. Open source software gives its users more control. They can examine the code to make sure it is not doing anything they do not want it to do, and they can change parts of it they do not like. Users who are not programmers also benefit from open source software, because they can use this software for any purpose they wish - not merely the way someone else thinks they should: https://opensource.com/resources/what-open-source.

[96] Front Line Defenders shares examples in its 2019 Global Analysis Report: Autocrats in Sudan and Algeria were deposed, while in Chile, Ecuador and Lebanon, authorities relented to demands to reduce inequality by introducing reforms or backtracking on bills which had initiated demonstrations. The report is available here: https://www.frontlinedefenders.org/sites/default/files/global_analysis_2019_web.pdf.

[97] For more information on how digital technologies are transforming CSOs, see: (Dalberg, 2018[76])

fundraising (such as crowdfunding),[98] and recruiting members and volunteers, are emerging. A report from CONCORD Europe and FOND Romania explains how digital technologies have improved CSO's "effectiveness and efficiency, minimising wasted resources, reaching the right people directly without the unnecessary intervention of costly middlemen, and, with the right software, significantly improving the monitoring and evaluation of projects" (CONCORD Europe, FOND Romania, 2018[32]). This same report argues that better programme and project management through digital technologies have also increased the effectiveness of CSOs:

> *"Thanks to the use of digital platforms and their services, routine tasks can be automated, more responsibilities can be moved to a lower level, and best practice can spread more easily. (...) Thanks to big data powered analytics , CSOs have better options for tracking the effectiveness of initiatives and projects; data is able to clearly demonstrate what works and resources can be allocated to projects with the greatest impact. At the same time, failures can be detected immediately"* (CONCORD Europe, FOND Romania, 2018[32]).

Not only are digital technologies used at the operational level to streamline internal processes, they are also used to provide better, faster services to constituents. For example, according to an article from Global Voices, a Russian CSO developed a bot that provides real-time legal assistance to protestors (Global Voices, 2019[60]).

- Moreover, governments are starting to play a more active role to safeguard civic freedoms in the digital space. For example, in 2019, the Parliament in Jordan withdrew a Cybercrime Bill restricting freedom of speech and the right to privacy, after pressure from human rights activists and CSOs.[99] Tech companies too, are starting to adapt their business practises. For example, during the protest movement in Hong Kong, China according to the BBC, Twitter announced it would no longer allow advertisements from broadcasters who were financially and editorially controlled by governments, after facing criticism for allowing anti-Hong Kong, China advertisements to spread on the platform (BBC News, 2019[61]). In Sudan, The New York Times reported that Facebook and Twitter announced the shutdown of hundreds of accounts associated with disinformation campaigns after pro-democracy demonstrators were killed in Khartoum in June 2019 (The New York Times, 2019[20]). Following the massacre in Christchurch, New Zealand, in March 2019, all of the social media firms acted quickly to remove violent footage that was circulating on Facebook, and other social networks including YouTube, Twitter, and Reddit (BBC News, 2019[31]). Governments and online service providers were quick to respond by issuing the Christchurch Call to Action,[100] a global pledge to eliminate terrorist and violent extremist content online. Another example reported by the New York Times relates to the decision of Uber and Careem to deny requests by the Egyptian government to access the data of their Egyptian customer database for surveillance purposes (The New York Times, 2017[62]). Also noteworthy, tech companies are launching programmes and funding research to better align digital technologies with human rights principles. WhatsApp established the Research Awards for Social Science and Misinformation program[101] to fund independent research to inform its understanding of the safety problems people encounter on WhatsApp and what more it can do in partnership with civil society to address these problems. In July 2019, it funded a report to investigate the impact of WhatsApp on the Nigerian elections and

[98] Crowdfunding is the practice of funding a project or venture by raising money from a large number of people who each contribute a relatively small amount, typically via the Internet.

[99] More information about the Jordanian bill is available in Front Line Defenders 2019 Global Analysis Report: https://www.frontlinedefenders.org/en/resource-publication/global-analysis-2019.

[100] Read about the Christchurch Call to Action here: https://www.christchurchcall.com/call.html.

[101] Read more about the Research Awards for Social Science and Misinformation programme here: https://www.whatsapp.com/research/awards/.

whether it had facilitated the spread of misinformation and disinformation. Moreover, in 2018, Microsoft launched The Defending Democracy Program.[102] The programme seeks to: protect campaigns from hacking; increase political advertising transparency online; explore technological solutions to preserve and protect electoral processes; and defend against disinformation campaigns and cyberattacks. The company is working with governments, CSOs, academics and industries globally. Microsoft is now rolling out a new voting technology called ElectionGuard, a free open-source software development kit (SDK) that will make voting secure and more accessible.

- The emerging 'free-network movement'[103] which is pushing to bring unfettered network access to as many people as possible and rewire online networks to make it harder for a government or corporation to exert undue control or surveillance, will likely gain more ground in the coming years. Computer programmers and tech savvy civil society actors will succeed in building alternate Internets to counter digital repression.[104] Open source software will become widespread,[105] and contribute to protecting civic space by allowing civil society to control and run online spaces that are currently controlled by tech companies. With open source software, digital activism/online civic activism is expected to grow. For example, LiquidFeedback[106] is an open source implementation of liquid democracy[107] created for policy development by political parties and led by the non-profit Public Software Group; Adhocracy[108] is an open source implementation of liquid democracy for decision-making processes, primarily for civil participation projects, but also by political parties and the German Federal Parliament.

2.3. What we do not know about the future of civic space: key uncertainties[109]

The future of civic space in the context of digital transformation holds many uncertainties, that is, questions that arise resulting from a state of having limited knowledge about the future. These questions have also been taken into account in the scenario-building process as they can influence the future trajectory of civic space in one way or another, depending on how they play out.

- Who will control, govern and operate digital technology and online space? Will it continue to be tech companies? Will the efforts of technologists to decentralise the infrastructure of the Internet

[102] Read more about Microsoft's Defending Democracy Programme here: https://news.microsoft.com/on-the-issues/topic/defending-democracy-program/.

[103] Read more about the free-network movement here: https://www.chronicle.com/article/Fear-of-Repression-Spurs/129049.

[104] There are examples of tests being conducted currently of homemade Internet that could go online if parts of the current global Internet becomes blocked by a repressive government.

[105] Business Insider reports about the future of open software here: https://www.businessinsider.fr/us/sc/open-source-technology-future-of-cloud-2019-1; Forbes magazine also supports this projection: https://www.forbes.com/sites/taylorarmerding/2019/01/09/the-future-of-open-source-software-more-of-everything/#3cd58b468fa4.

[106] Liquid Feedback: https://liquidfeedback.org/

[107] Liquid democracy is a democratic system in which most issues are decided (or strongly suggested to representatives) by direct referendum.

[108] Adhocracy: https://adhocracy.de/

[109] See Annex A for the definition of uncertainties.

gain traction (International Center for Not-for-Profit Law, 2020[63])? Who will have control over data ownership?

- Will tech companies continue to be left unchecked and free to determine their business models (e.g. how online content is managed, what algorithms are used, what values are protected or banned, etc.) with clear implications for civic freedoms? Will the current practices and business models of technology companies be reformed? Will there be greater regulation and oversight of tech companies by governments and multilateral organisations in partnership with civil society?
- What will be the degree to which "states instrumentalise technology for their own geopolitical and domestic goals" (International Center for Not-for-Profit Law, 2020[63])?
- Will digital technologies reduce both cross-country and intra-country inequality, reduce one and increase the other, or increase both?
- How will CSOs adapt to new roles and work alongside automated systems? Will they have the capacity to integrate digital technology into every aspect of their work (International Center for Not-for-Profit Law, 2020[63])? Will civil society become digital tech savvy and empowered to counter digital attacks or will heavily digitally-resourced actors continue to level digital technologies against civil society actors with less digital capacity to defend themselves (Digital Civil Society Lab - Stanford PACS, 2017[51])?
- Will the proliferation of large scale social movements powered by digital technologies strengthen civic space as a cornerstone of democracy or will these movements continue to present democratic shortfalls?[110]
- Will advanced democracies work collectively to reinforce the standards and implementation of a democratic model of governance of digital technologies through which fundamental rights are respected across the digital sphere?
- Will physical civic space altogether disappear and be fully replaced by online civic space?
- What effect will digital transformation have on the nature and purpose of civic space? Will there be an emergence of a new sense of purpose for civic space and civil society actors (Charities Aid Foundation, 2018[39])?
- Could digital surveillance measures enacted in response to a national emergency such a public health crisis or terrorist security threat - that infringe upon people's privacy and civil rights - lead to a weakening or a change in the perception of democracy and civic space around the world?

[110] Richard Youngs argues that new forms of civic activism unleashed by digital technologies – including large-scale social protest movements – present democratic shortfalls. In his report, 'Rethinking civil society and support to democracy', he indicates that civic movements mobilised through digital tools seek direct action that circumvent the channels of representative democracy. They tend to reflect individual demands rather than represent group interests. Movements become popular through individuals with followers on social media rather than by group-based political engagement. They oppose government power and policies but do not necessarily have governing manifestos of their own, nor solutions or alternatives to propose. The voices of these movements that are primarily urban protests eclipse the voices of people living in rural areas. In short, these "movements may not be optimal from the point of view of developing the kind of deeply rooted social capital that can make the difference between successful and dysfunctional democracy" (Youngs, 2015[79]).

3. Plausible futures to 2030

The future of civic space is subject to uncertainties and drivers of change that may have an impact (positive or negative) on how civic space evolves. How these will combine, and the consequences for civic space is unknown. Based on a study of different logical interactions of current trends, drivers of change, and uncertainties, four distinctive futures of civic space have emerged through to 2030. They represent the four most plausible, differentiated, disruptive and memorable futures that have come out from the scenario-building exercise. The findings of this paper do not exclude the possibility of other scenarios playing out; of the future being a hybrid of these four scenarios, or of different scenarios unfolding or playing out in different parts of the world.

Figure 3.1. Digital transformation and the futures of civic space to 2030: futures overview

Future #1: Civic space collapses

In this future, governments, as well as other non-state actors (companies, media outlets, certain civil society actors such as extremist groups) have free rein to leverage emerging digital technologies in adverse ways that restrict civil society actors' activities and lead to the gradual collapse of civic space.

From 2020 to 2030, civic space has very quickly, considerably shrunk, with **two main drivers influencing this evolution:** 1) State crackdown, partly enabled by the export of surveillance tech to developing countries; 2) In reaction to this, the voluntary desertion of hostile online spaces by digitally disadvantaged civil society actors who fear exposure and reprisals.

Future #2: Civic space flourishes

In this future, an enabling legal framework exists for civic space to flourish both on line and offline. A democratic model of digital governance has been established through which fundamental rights are respected across the digital sphere. Space is defended and expands through the action and interactions of responsible states, companies and other actors. Civil society actors, digitally empowered in part by development co-operation providers, have found ways to adapt to and circumvent restrictions to civic space.

From 2020 to 2030, civic space has very quickly, considerably expanded, with **two main drivers influencing this evolution**: 1) The emergence of a human-centric and human-driven global digital governance regime; 2) The agency of responsive stakeholders, including civil society actors.

Future #3: Civic space transforms itself

In this future, social movements form the bulk of civic activism; they permeate online and offline civic spaces and engage primarily in political activism. Institutionalised CSOs are no longer as prominent; they operate primarily in physical civic spaces and their activities are limited to apolitical service provision.

From 2020 to 2030, the evolving interactions and dynamics between civil society actors as well as between civil society and governance structures and institutions transform the nature and purpose of civic space. Civic space is not only a space to assemble, express oneself and associate; online space has also become a modern *agora* where people practice direct democracy - at national, regional and global levels - ushering in a new age of democratic renewal.

Two main drivers influence this evolution: 1) The behavior of civil society actors who gradually use civic technologies on a wide scale; 2) The deconstruction of state-citizen relations and of current political institutions, which are primarily based on models of representative democracy.

Future #4: Civic space breaks apart

In this future, civic space has broken into micro spaces that vary in levels of openness and inclusiveness. Some spaces are nearing collapse or have collapsed; others are thriving because stakeholders have adopted human-centric and human rights based tech principles as well as other measures necessary to protect and expand civic space; while other spaces are somewhere in between, facing heavy restrictions but still managing to ward off a complete closure, through the use in part of civic technologies. As a result, civic space as a whole is not cohesive nor integrated but has become dysfunctional and is considerably weakened and limited.

From 2020 to 2030, the fragmentation of civic space – across and within countries - is amplified and exacerbated along the following lines: geography, age, level of education, gender, and level of income.

Two main drivers influence this evolution: 1) The proliferation of self-contained digital regimes, which have disrupted international civic space and made it difficult for civic actors bound by different regulations to connect, co-ordinate and mobilise; 2) Increased inequalities, which have disrupted national and local civic spaces by making it difficult for different communities to engage equally.

Table 3.1. Plausible future to 2030 #1: Civic space collapses

What does civic space look like in 2030	Current trends and drivers of change supporting this future	How this future happened: The years 2020-2030
1) In authoritarian and semi-authoritarian developing countries, online civic space has been fully or 80 to 90% shut down. The remaining space is under constant digital harassment and surveillance. 2) Malevolent actors have saturated online space with fake news and disinformation campaigns, driving many CSOs away from the digital space in reaction to these restrictions. 3) Authoritarian governments are fully subsidising the purchase of repressive AI technology in developing countries. Countries in Africa, Southeast Asia and South Asia are the main buyers. Online civic space in many developing countries is compromised and operates at only 10-20% of 2020's capacity. 4) In more liberal democracies in developing countries, the surveillance and analysis of citizens' data by governments and the private sector have become normalised. Data is being collected from social media activity, smart city, Iot technology and CCTV cameras. This is also a world in which migration and terrorism have steadily increased, boosting the use of surveillance in the name of national security. Furthermore, populism has also steadily increased and with this, the rise of populist parties' and movements attacks on local and international CSOs. The normalised digital surveillance and cyberattacks has reinforced a chilling effect among civil	1) In many authoritarian and semi-authoritarian countries, digital technologies are being used to crack down on civic space including through Internet shutdowns, network disruptions, criminalisation of online activity, disinformation campaigns, fake news, as well as digital harassment and surveillance. Following demonstrations in the Islamic Republic of Iran (hereafter 'Iran') in Nov. 2019, Freedom House reports that the worst Internet disruption in the country's history took place, affecting up to 95% of users. [111] 2) Freedom House declared 2019 the 13th consecutive year of decline in global freedoms in terms of curbs on civil liberties. [112] 3) In its 2019 State of Civil Society Report, CIVICUS states that over 100 countries are characterised by closed, repressed or obstructed civic space. [113] 4) The recent rise in populism has had negative effects on CSOs in liberal democracies: (i) denials of funding and government-sponsored spread of stigmatising misinformation as seen in the case of e.g. reproductive rights groups like Planned Parenthood in the United States, (ii) restrictive laws and police incursions, e.g. raids of NGOs in Hungary, (iii) the criminalisation and confiscation of resources, e.g. the Italian government's impounding of a migrant-rescue boat belonging to a Spanish NGO. These examples have been reported by	1) Stakeholders, including international institutions, governments and tech companies did not address the issue of an optimal balance between AI technology, government surveillance and citizens' privacy rights. Technologies became increasingly embedded in governance and politics. 2) Stakeholders did not address the issue of shrinking civic space induced by the negative use of digital technologies because they underestimated the risks associated with this trend or were not able to effectively co-operate and reach consensus on the course of action. 3) International and national companies caused, contributed or were complicit in the closing of civic space either by obligation because they were dependent on authoritarian governments' authorisations to operate, or because they sought to only serve their commercially-focused interests with indifference towards the challenges facing civil society on line. Companies failed to develop ethical and responsible business charters in part because they were not prodded by governments to do so. 4) A revision of corporate governance of digital technologies did not happen. The digital/tech industry did not develop a model of digital governance that protects the digital space as an open and constructive forum for democratic and civic life. 5) Civil society has gradually chosen to disengage from the online space because of a rise in public consciousness of the shortfalls of

[111] Freedom House's article is available here: https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

[112] See Freedom's House 2019 report here: https://freedomhouse.org/report/freedom-world/freedom-world-2019/democracy-in-retreat.

[113] The 2019 State of Civil Society Report is available here: https://www.civicus.org/index.php/state-of-civil-society-report-2019.

society actors. Many fear for their safety and privacy and become less active digitally and partially desert online civic spaces. 5) The online space is a crucial catalyst for wider civic engagement in the physical space (digital tools and social media in particular can be used to raise awareness and mobilise people offline). As such, cyberattacks and restrictions to the online space have had direct or indirect negative repercussions on the physical space. In contexts where physical civic space is already extremely limited, further repressions in the online space result in an almost complete shutdown of civic space.	the NGO Tactical Tech.[114] 5) Recent research from the Asia Foundation reveals that civic space in Southeast Asia is shrinking in at least seven countries in the region, largely due to rising populist intolerance and backsliding of democratic ideals. Shrinking space is characterised by growing restrictions on free speech and funding for civil society organisations, dwindling engagement with government, and fewer opportunities for these organisations to participate in regional or international forums.[115] 6) In recent years, activists and CSOs have also experienced covert attacks using malware, phishing and spyware.[116] For instance, Tactical Tech reports that in Egypt, CSOs were the targets of an organised phishing attack. Amnesty International was the target of Operation Kingphish in which a fake social media persona was created by an unknown actor who used phishing attacks to gain access to dozens of journalists, human rights defenders, trade unions and labour rights activists, many of whom were seemingly involved in the issue of migrants' rights in Qatar and Nepal.[117] 7) In The Global Expansion of AI Surveillance (2019), Carnegie Endowment for International Peace reports that 37 per cent of closed autocratic states, 41 per cent of electoral autocratic/competitive autocratic states, 41 per cent of electoral democracies/illiberal democracies and 51% of advanced democracies deploy AI	digital technologies, general online security concerns and the risks and threats that exist on line, as well as a lack of digital knowledge which prevents CSOs from being able to counter digitally-induced restrictions or repression. The public lost trust in digitised procedures.

[114] See Tactical Tech's report on 'shrinking civic space: a digital perspective' here: https://ourdataourselves.tacticaltech.org/posts/shrinking-civil-space-a-digital-perspective/.

[115] Based on research presented by the Asia Foundation at the 2020 Australasian AID Conference (Asia Foundation panel "Rethinking Civic Space in Southeast Asia"). More information available here: https://devpolicy.org/insights-from-the-australasian-aid-conference-2020-20200310/.

[116] Malware is an umbrella term for a whole range of malicious software including viruses, trojans, adware, ransomware and all other kinds of malicious programs. Spyware is a type of malware that, once installed on a computer, collects information without you knowing. Phishing is a method of acquiring information. It refers to the actual process of attempting to get information from someone. This can involve using malware.

[117] See Tactical Tech's report on 'shrinking civic space: a digital perspective' here: https://ourdataourselves.tacticaltech.org/posts/shrinking-civil-space-a-digital-perspective/.

	surveillance systems from safe city platforms to facial recognition cameras (for lawful and unlawful policy objectives).[118] 8) Governments in authoritarian and semi-authoritarian states are more likely to abuse/misuse AI surveillance systems than governments in liberal democracies. For instance, according to Carnegie, China, Russia and Saudi Arabia are exploiting AI technology for mass surveillance purposes. Governments with poor human rights records are also abusing AI surveillance to reinforce repression.[119] 9) According to Carnegie, China is the main supplier of AI surveillance world wide. Chinese companies (Huawei, Hikvision, Dahua and ZTE) export AI surveillance technology to 63 countries, 36 of which have signed onto China's Belt and Road Initiative.[120] Chinese selling pitches are often accompanied by soft loans to encourage developing countries to purchase equipment. This was the case with Kenya, the Lao People's Democratic Republic, Mongolia, Uganda and Uzbekistan.[121] According to an article from the South China Morning Post, Chinese export of AI surveillance tech is also happening in advanced liberal democracies, as showcased by the hundreds of Huawei surveillance cameras installed in Serbia.[122] 10) There is a lack of transparency, accountability and security mechanisms in the cyber space. The majority of companies including	

[118] Carnegie's report can be found here: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

[119] Ibid.

[120] The Belt and Road Initiative is a massive trade and infrastructure project that aims to link China to dozens of economies across Asia, Europe, Africa, and Oceania.

[121] Carnegie's report on The Global Expansion of AI Surveillance (2019) is available here: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

[122] Access the full article of the South China Morning Post here: https://www.scmp.com/comment/letters/article/3034087/huawei-cameras-serbia-only-add-fears-about-chinese-mass.

	tech giants are breaching existing data protection rules.[123] Companies around the world fail to adequately disclose information about data collection and governments' requests for access to users' data for surveillance. Instead of regulation, governments have allowed digital tech companies – many of which are showing a lack of ethical standards across the industry - to draft their own codes of conduct.[124] According to Reuters, Google, which quit China's search engine market in 2010, has been criticised by Human Rights activists for actively seeking ways to re-enter the Chinese market, despite the implications in terms of surveillance demands.[125] There are also reports of companies abusing transparency by sharing personal data information for targeted paid digital advertising that seek to manipulate public opinion.[126] 11) Border and terrorism issues are on the rise in many countries and are gaining pre-eminence amongst voters' concerns.[127] 12) Facebook's usage rate has plummeted over the last year following a series of data, privacy and hate speech scandals.[128] According to the Edelman Trust Barometer, trust in all technology-based sectors declined in 2020, with concerns over data privacy and security being a key factor.[129]	

[123] TechRadar (the largest UK-based consumer technology news and reviews site) reports about this here: https://www.techradar.com/news/majority-of-companies-still-arent-gdpr-compliant.

[124] The BBC reports about this here: https://www.bbc.com/news/technology-49719946.

[125] Find Reuters' article here: https://www.reuters.com/article/us-china-google/google-plans-return-to-china-search-market-with-censored-app-sources-idUSKBN1KN09C.

[126] Maplight reports about this here: https://maplight.org/story/digital-deception-and-our-democracy/.

[127] Read more about these trends here: https://www.voanews.com/usa/report-ethnic-racial-terrorism-rise-around-world.

[128] The Guardian reports about this here: https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows.

[129] Edelman Trust Barometer (page 15): 61% of individuals surveyed consider that governments do not understand emerging technologies enough to regulate them: https://cdn2.hubspot.net/hubfs/440941/Trust%20Barometer%202020/2020%20Edelman%20Trust%20Barometer%20Global%20Report.pdf?utm_campaign=Global:%20Trust%20Barometer%202020&utm_source=Website.

Table 3.2. Plausible future to 2030 #2: Civic space flourishes

What does civic space look like in 2030	Current trends and drivers of change supporting this future	How this future happened: The years 2020-2030
1) An enabling legal framework exists for civic space to flourish both on line and offline. A democratic model of digital governance has been established through which fundamental rights are respected, protected and fulfilled across the digital sphere. The existing international human rights norms and principles safeguarding civic space, including the rights to freedom of expression, of peaceful assembly and of association have become the framework that guides digital tech companies' design, control and governance of digital technologies. 2) Space is defended and expands through the action and interactions of responsive states and companies. Civic freedoms are reinforced by open, inclusive, participative and transparent online spaces and platforms that are owned and run by civil society, bringing with it greater accountability, more civic engagement and accelerated positive political change. Access and usage of digital technologies are guaranteed to all citizens irrespective of their geographical location, income, education, gender and social status. 3) Digital tech companies have created digital tools and platforms that embody and protect the values of human rights and open societies; such tools and platforms are used by tech savvy civil society and have contributed to increasing online	1) A number of frameworks are emerging at the international, regional and national levels to protect civic space as well as to ensure compliance of digital technologies with human rights e.g. the UN Guiding Principles on Business and Human Rights; the OECD Recommendation of the Council on Artificial Intelligence; the EU General Data Protection Regulation; Singapore's AI Governance Framework, etc.[130] 2) In response to the growing concentration of power and new forms of digital exclusion, international frameworks are also emerging to ensure the equal access to and inclusive usage of digital technologies so that people around the world benefit from the same rights on line e.g. UNESCO has developed guidelines for inclusive digital solutions for people with low skills and low literacy.[131] Moreover, the 2030 Agenda for Sustainable Development contains a commitment to: 1. Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2030 (target 9.C); and 2. Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women (target 5.B).[132] The UN Broadband Commission for Sustainable Development, in a report published in September 2018, lists half a dozen recommendations for governments, including support for local digital businesses and reducing taxes on telecoms equipment. The Alliance For Affordable Internet (A4AI), an advocacy group, focuses on how the cost of access can be reduced, for instance by fostering competition and clever allocation of	1) Civil society and human rights activists, as well as international organisations put pressure on governments and companies to develop and comply with legal frameworks that protect civic space on line and offline. 2) More liberal democracies led the way (i) in adopting and putting pressure on authoritarian and semi-authoritarian governments to adopt norms that help prevent or mitigate human rights risks of digital technologies; and (ii) applying sanctions in the lack thereof. 3) Governments and multilateral organisations in partnership with civil society were able to better regulate how tech companies operate, establishing independent bodies that: (i) oversee e.g. how online content is managed, what algorithms are used, etc.; and (ii) make sure practices of tech companies do not put civic space at risk. 4) Digital tech companies took action to reform their business models in order to keep the trust of their users, aware of the risks their business faced in terms of fines/sanctions from governments, reputational damage and loss of users. Companies invested in the development of new technologies and business models that strengthened human rights, creating a digital space that was safer and more conductive to civic engagement. Incentivised by governments and CSOs alike, they realised that unless they were able to offer safe and trustworthy digital tools and platforms, civil society would no longer use their products and

[130] UN Guiding Principles on Business and Human Rights: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf; OECD Recommendation of the Council on Artificial Intelligence : https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449; EU General Data Protection Regulation: https://gdpr-info.eu/; Singapore's AI Governance Framework: https://www.pdpc.gov.sg/Resources/Model-AI-Gov

[131] UNESCO's guidelines are available here: https://en.unesco.org/news/unesco-launches-guidelines-inclusive-digital-solutions-people-low-skills-and-low-literacy.

[132] The SDG indicator framework is available here: https://unstats.un.org/sdgs/indicators/indicators-list/.

activism.	wireless spectrum.[133] 3) At the national level, there are examples of measures taken by governments to protect civic space and rights both on line and offline, adopt policies to limit disinformation and abusive surveillance and safeguard against arbitrary shutdowns. For example: Italy adopted a Charter of Internet Rights which links on- and offline rights, including protecting basic civil liberties such as the freedom to assemble.[134] The UK 2019 parliamentary report on disinformation and 'fake news' calls for policy measures such as mandating social media companies to take down known sources of harmful content, including proven sources of disinformation.[135] There are also efforts to strike a balance between freedom of expression on line and the prohibition of incitement to hatred, such as the free speech law adopted in Germany in 2017 which aims to combat illegal and harmful content on social media platforms.[136] In Jordan, the Parliament withdrew a Cybercrime Bill in February 2019 that would have restricted freedom of speech and the right to privacy.[137] There are efforts to strike a balance between the protection of public safety / national security (e.g. against terrorism and hate speech) and the principles of a free, open and secure Internet. The UN in particular has identified guidelines for the regulation of digital space including via surveillance and online content removal, without compromising human rights and fundamental freedoms, including the freedoms of expression, association and assembly.[138]	services. 5) Civil society actors in developing countries adapted to digital transformation and strengthened their digital skills and knowledge, in part, thanks to the support of development co-operation providers. They found original solutions to resist and circumvent barriers to civic activism and activities. 6) The control of online spaces and data shifted from tech companies to civil society.

[133] These examples are highlighted in an article from The Economist on 'closing the digital divide in 2019' available here: https://worldin2019.economist.com/digitaldivide.

[134] The Charter of Internet Rights is available here: http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf.

[135] UK 2019 parliamentary report on disinformation and 'fake news' is available here: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/.

[136] Read more about German's free speech law here: https://medium.com/@_cberger_/will-germanys-approach-to-content-and-platform-regulation-prevail-in-2018-d7e6e2db5cb.

[137] Front Line Defenders reports about this bill here: https://www.frontlinedefenders.org/en/resource-publication/global-analysis-2019.

[138] The use of digital technologies for surveillance to combat terrorism, protect national security and public safety should occur only on the basis that such activities "are adopted openly; are time-limited; operate in accordance with established international standards of legal prescription, legitimate aim, necessity and proportionality; and

	4) People are increasingly participating in local, national and global activism through social media platforms; this phenomenon is known as 'digital activism'. 5) Digitisation of many areas and aspects of society are gaining ground in many countries. 6) Governments, businesses, and civil society are joining coalitions to promote guidelines on digital technologies that uphold human rights and civic freedoms (i.e. Christchurch Call to Action). [139] 7) In February 2020, the Privacy Commissioner of Canada asked a federal court to: (i) declare that Facebook violated Canadian privacy laws; (ii) issue and order demanding that Facebook put in place effective, precise and easily accessible measures to obtain the valid consent of all users and to ensure that it is kept; (iii) ban the social network from continuing to collect, use and disclose users' personal information. [140] 8) Individuals facing increased efforts to limit their access to the global Internet and monitor their online activities, are slowly developing their digital skills and knowledge and turning to virtual private networks (VPNs) as a secure means of reaching uncensored information on line. This is	

are subjected to continued independent supervision that includes robust mechanisms for prior authorisation, operational oversight and review" (UN-OHCHR, 2019[7]) (Report of the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/141/02/PDF/G1914102.pdf?OpenElement). Any restrictions to online content should be "pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy" (UN Human Rights Council (2018) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (HRC/38/35), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement).

[139] The Christchurch Call to Action is a global pledge to eliminate terrorist and violent extremist content on line developed and endorsed jointly by governments and online service providers: https://www.christchurchcall.com/call.html.

[140] CTV News reports about this example here: https://www.ctvnews.ca/politics/privacy-commissioner-wants-federal-court-to-declare-facebook-broke-federal-privacy-law-1.4800320?cache=yes%3FclipId%3D104059.

	the case in Iran according to Freedom House.[141] 9) Big tech companies are starting to take action to respond to the adverse impacts of digital technologies including on civic space i.e. The Ranking Digital Rights - Corporate Accountability Index reports that more than half of the companies evaluated in 2018 improved disclosure in multiple areas affecting users' freedom of expression and privacy. Transparency reporting continues to improve and expand. More companies disclosed more information and data related to their policies and processes for responding to government or other third party requests to restrict content, as well as to share user information with authorities.[142] Microsoft launched the Defending Democracy Program in 2018 to safeguard civic freedoms on line and protect democratic processes.[143] WhatsApp established the Research Awards for Social Science and Misinformation program to fund independent research to inform its understanding of the safety problems people encounter on WhatsApp and what more it can do in partnership with civil society to address these problems..[144] 10) Big tech companies are also making efforts to close the digital divide and bring more people on line. Facebook's Free Basics programme, for instance, is now available in 65 countries. It gives smartphone owners access to a limited selection of data-light websites and services, including Facebook and Whats-App, the mobile messaging app it owns. These are "zero rated", meaning they can be browsed for nothing..[145] 11) Digital platforms that are run and owned by people (instead of tech companies) are starting to emerge with the expansion of open source	

[141] Freedom House's article is available here: https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

[142] The Ranking Digital Rights website is available here: https://rankingdigitalrights.org/index2018/report/executive-summary/.

[143] More information about Microsoft's Defending Democracy Program is available here: https://news.microsoft.com/on-the-issues/topic/defending-democracy-program/.

[144] More information about WhatsApp's Research Awards for Social Science and Misinformation program is available here: https://www.whatsapp.com/research/awards/.

[145] Find out more about Facebook's Free Basics programme here: https://worldin2019.economist.com/digitaldivide.

	software. These digital platforms are set up as citizen, consumer or worker-run co-operatives. For example, Goteo is a non-profit organisation designed to raise money for community projects. Like other crowdfunding platforms, it generates funding by encouraging people to make small investments. But the rights to the projects have been made available to the community through open-source and Creative Commons licensing..[146]	

Table 3.3. Plausible future to 2030 #3: Civic space transforms itself

What does civic space look like in 2030	Current trends and drivers of change supporting this future	How this future happened: The years 2020-2030
1) Social movements form the bulk of civic activism and permeate online and offline civic spaces. They are fast-moving, nomadic, footloose, versatile and transient, forging and un-forging alliances as their individual and/or group interests evolve. Civic space is used primarily by these actors for political activism; as a place to advocate for a cause; raise issues of public concern and contribute to public debate; report human rights violations; and hold governments accountable. 2) Membership-based institutionalised CSOs are no longer as prominent; they operate primarily in physical civic spaces and their activities are limited to apolitical service delivery and humanitarian relief. 3) Digital technologies have given a new centrality to citizens and enabled the global convergence of individual and societal needs to supersede state structures and inter-state relations.	1) Digital technologies have given rise to networked social movements that provide new means for the articulation of citizen voice, mostly outside the frameworks of organised civil society. 2019 was characterised by waves of social uprisings of remarkable magnitude from Iraq, Algeria and Lebanon in the Middle East; France and Spain in Europe; Zimbabwe, Guinea and Sudan in Africa; to Hong Kong, China and India in Asia; and Chile and Ecuador in the Americas.[151] These protests, ranging from global political movements to neighbourhood campaigns, revolve around outright rejection of deep economic inequality, rampant corruption and calls for greater civil and political rights. 2) Processes of globalisation and digitalisation have precipitated the development of a global civil society. People are increasingly using social media and technologies for global debate and activism (World Economic Forum, 2017[19]). 3) Solidarity amongst movements is growing. Protesters in the 2019 Hong Kong, China Anti-Extradition Law Amendment Bill movement shared	1) Civil society became less dependent on permanent membership structures and less exclusively channelled through traditional, institutionalised and professionalised CSOs. 2) Traditional institutionalised and professionalised CSOs operating in the physical space continued to provide service delivery and humanitarian relief. However, when it comes to political advocacy work, they lost ground to other types of digital activism and were seen as failing to achieve progressive political and social change that addresses global challenges. 3) Traditional mechanisms and policies for co-operation with civil society were revised, allowing governments, international organisations, donors and other actors to engage with social movements and other digital actors (despite the challenges of shifting organisation, membership and capacity) including through the widespread use of civic tech and gov.

[146] Read more about Goteo here: http://theconversation.com/beyond-hashtags-how-a-new-wave-of-digital-activists-is-changing-society-57502.

[151] The Guardian reports about these social uprisings here: https://www.theguardian.com/law/2020/jan/14/300-human-rights-activists-killed-2019-report.

Solidarity, co-operation and support between civil society movements across national borders have led to the deconstruction of state-citizen relations and of political institutions which were primarily rooted in representative democracy.[147] 4) As a result of the evolving interactions and dynamics between civil society actors as well as between civil society and governance structures and institutions, the nature and purpose of civic space are transformed. Civic space is not only a space to assemble, express oneself and associate; thanks to civic technologies, it has also become a space to practice direct democracy (either deliberative[148] or participatory[149]) at national, regional and global levels. Online civic space has become a modern *agora*[150] where people gather, deliberate political issues, and participate directly in political matters, ushering in a new age of democratic renewal.	protest techniques with individuals involved in the 2019 protest movements in Chile, Spain and France. *Gilets Jaunes* in the small city of Commercy, France received support messages from protesters in Hong Kong, China; protesters in Hong Kong, China received thank you messages from Chilean protesters. When Catalan protesters blocked the Airport of Barcelona in 2019, they drew their inspiration from Hong Kong, China protesters' methods. In October 2019, protesters in Hong Kong, China waved Catalan flags to show their solidarity with protesters in Barcelona.[152] Women's rights activists across the world are wearing black bands in front of their eyes as an expression of solidarity. 4) With digital transformation, civic activism is becoming more sporadic, footloose, tactically innovative, daring. These dynamic forms of civic activism, ranging from protest movements to community-level forums and online campaigns by individual activists, are displacing the influence wielded and the role played by traditional, professional CSOs (Carnegie, 2017[47]). 5) Social movements are yielding results. In Chile, Ecuador and Lebanon,	tech.[155] 4) Social movements managed to overcome the challenges relating to the fact that their activities and membership can shift unexpectedly. They were able to develop sustainable models of functioning as well as organisational capacity, allowing them to incrementally leverage the momentum of protests for tangible political change.

[147] This point draws its inspiration from political scientist Bertrand Badie's forward-looking 'New Perspectives on the International Order' (Badie, 2019[89]).

[148] Deliberative democracy empowers people to deliberate issues as equals and reach consensus or majority vote on the laws that govern them. It is rooted in discussion, reasoning and the public debate that precedes decision making.

[149] Participatory democracy empowers people to take decisions, weigh in on policies, elect government officials, etc. It is rooted in the direct actions of citizens who receive certain levels of decision-making power.

[150] The *agora* was a central public space in ancient Greek city-states. It was the physical place where every Athenian citizen gathered to conduct their business, participate in their city's governance, decide judicial matters, express their opinion, and elect their city officials. Agora is the place where the direct Athenian Democracy took root and flourished.

[152] Read more about these movements in Le Monde's article: https://www.lemonde.fr/international/article/2019/11/08/de-hongkong-a-santiago-une-contestation-mondialisee_6018419_3210.html.

[155] Gov. Tech aim is to increase efficiency in government administration by digitalising work processes or bringing in new tools. Civic tech enables engagement, participation or enhances the relationship between the people and government. The definitions of gov. tech and civic tech are available here: https://www.citizenlab.co/blog/civic-tech/whats-difference-civic-tech-govtech/.

	authorities relented to demands to reduce inequality by introducing reforms or backtracking on bills. [153] 6) Digital civic technologies are enhancing opportunities for national and international institutions to consult citizens and organised civil society. Individuals and CSOs can now provide inputs electronically or advocate for community-driven alternatives in national, regional and international governance processes e.g. through electronic voting, e-petitions, participatory budgeting etc. (OECD, 2019[14]). 7) Recent research by The Asia Foundation argues for moving beyond the somewhat narrow and value-laden notion of "civil society" – often associated with advocacy NGOs working on democracy at one end of the spectrum, or with faith-based charity organisations at the other – to a reconceptualisation of the terminology, "civic space", which is more inclusive and captures a broader range of civic engagement. [154]	

[153] Front Line Defenders shares examples of these changes in its 2019 global analysis report: The report is available here: https://www.frontlinedefenders.org/sites/default/files/global_analysis_2019_web.pdf.

[154] Findings from the 2020 Australasian AID Conference (Asia Foundation panel "Rethinking Civic Space in Southeast Asia"). More information available here: https://devpolicy.org/insights-from-the-australasian-aid-conference-2020-20200310/.

Table 3.4. Plausible future to 2030 #4: Civic space breaks apart

What does civic space look like in 2030	Current trends and drivers of change supporting this future	How this future happened: The years 2020-2030
1) Civic space has broken up into micro spaces that vary in levels of openness and inclusiveness. Some spaces are nearing collapse or have collapsed; others are thriving because stakeholders have adopted human-centric and human rights based tech principles as well as other measures necessary to protect and expand civic space; while other spaces are somewhere in between, facing heavy restrictions but still managing to ward off a complete closure, through the use, in part, of civic technologies. As a result, civic space as a whole has become dysfunctional and is considerably weakened and limited. 2) The first type of fragmentation of civic space amplified by digital transformation is a geographic fragmentation: Disparate digital regulations have sprang up like mushrooms all over the world. China, the United States, the European Union, Russia, and other big nations have their respective digital governance regime. Smaller countries have followed suit, copying existing models or adopting hybrid regimes that incorporate a mix of elements. Instead of one cohesive, integrated, global civic space enabled by digital technologies,	1) Income inequalities are increasing.[156] 2) Extreme poverty continues to decline. However, the pace is slowing down[157] and many people who are already vulnerable risk being left behind even further, especially with climate change-induced extreme events which could reverse gains in poverty reduction.[158] 3) Almost 4.5 billion people were active Internet users as of June 2019, encompassing 58% of the global population.[159] This means that a little less than half of the world population is still not using the Internet – the majority of these people live in developing countries. Moreover, Internet access is not equally distributed within developing countries. Many individuals in poor urban, and rural areas have no or unreliable access due to a lack of basic or a lack of quality infrastructure. Women living in low-income countries are less active on line. Countries that have the highest mobile Internet prices have the lowest percentages of women on line.[160] Up to 50% of women are less likely to be using the Internet than men. A key barrier for some is education – 15% of adults globally are	1) The digital divide between developed and developing countries widened. Digital divides within developing countries also widened, especially the rural-urban digital gap, the gender digital gap, the generational digital gap, and the socioeconomic digital gap. 2) Digital systems that ensure Internet access is inclusive and addresses barriers to affordability and accessibility for underrepresented/marginalised communities and geographically isolated regions, were not established. 3) Hate speech targeting, stigmatising and discriminating against specific groups on line, spiralled out of control. 4) Stakeholders did not address the lack of compliance of national digital legal regulations with international digital governance frameworks. International co-ordination and co-operation around a set of globally recognised principles regulating digital technologies, that all countries can adhere to – did not take place.

[156] The IMF reports about rising income inequalities here: https://blogs.imf.org/2019/05/15/tackling-income-inequality-requires-new-policies/. Research from UN DESA (https://www.un.org/en/development/desa/policy/wess/wess_bg_papers/bp_wess2013_svieira1.pdf) and the (OECD, 2011[90]) confirm these trends.

[157] Read more about these trends reported by The World Bank here: https://www.worldbank.org/en/news/press-release/2018/09/19/decline-of-global-extreme-poverty-continues-but-has-slowed-world-bank.

[158] According to Science Daily, climate change would reverse development gains: https://www.sciencedaily.com/releases/2017/07/170714140300.htm; According to the World Bank, climate change affects the poorest in developing countries: https://www.worldbank.org/en/news/feature/2014/03/03/climate-change-affects-poorest-developing-countries.

[159] According to the Internet World Stats website: https://www.internetworldstats.com/stats2.htm.

[160] Tactical Tech reports about this here: https://ourdataourselves.tacticaltech.org/posts/shrinking-civil-space-a-digital-perspective/.

the proliferation of self-contained digital regimes has disrupted international civic space and made it difficult for civic actors engaging in these fragmented geographic spaces bound by different regulations, to connect, co-ordinate and mobilise. 3) Within countries, increased inequalities induced by the unequal access to and usage of digital technologies, have further amplified the fragmentation of civic space along other existing lines of fracture related to age, level of education, gender, and level of income. 4) Hate and extremist groups contribute to exacerbating the fragmentation of civic space by leveraging digital technologies to attack certain groups that are already digitally disadvantaged i.e. women; indigenous communities, ethnic minorities, etc., discouraging them to engage in online spaces.	considered illiterate.[161] 4) Increasing costs and commercialisation of online spaces (e.g. high cost of broadband access, cost of mobile devices) are contributing to the digital divide along income levels.[162] The cost of devices and connectivity is preventing many people from accessing the Internet, especially the 13% of the world population living below the poverty line.[163] Global broadband-internet user penetration is at 51%.[164] 5) The social media tax in Uganda has negatively impacted the ability of users, particularly low-income citizens, to gain affordable access to the Internet.[165] 6) Digital technological developments are contributing to steep declines or closures of local newspapers. The collapse of the press is exacerbating polarization and the rise of non-cohesive spaces with different levels of access to reliable information.[166] 7) Female journalists are subject to more digital abuse and threats than their male counterparts. They are disproportionally experiencing gender-related threats, harassment and intimidation on the Internet which	

[161] The World Economic Forum reports about this here: https://www.weforum.org/agenda/2016/05/4-billion-people-still-don-t-have-internet-access-here-s-how-to-connect-them/.

[162] Read more about these trends here: https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2019/03/Henry-Bridging-the-Digital-Divide-2019.pdf.

[163] The World Economic Forum reports about this here: https://www.weforum.org/agenda/2016/05/4-billion-people-still-don-t-have-internet-access-here-s-how-to-connect-them/.

[164] See 2019 State of Broadband Report available here: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

[165] An article from the Good Things Foundation covers this issue: https://medium.com/goodthingsfoundation/how-the-social-media-tax-is-worsening-ugandas-digital-divides-7663adeec245.

[166] Read more about these trends here: https://www.governing.com/topics/politics/gov-newspapers-government-studies.html.

	has a direct impact on their safety and online activities.[167] 8) Red Salud de las Mujeres Latinoamericanas y del Caribe (RSMLAC) (Health Network of Latin American and Caribbean Women) and Planned Parenthood in the United States had their websites hacked during a public outreach campaign, and were forced to suspend their websites.[168] 9) The 2018 van attack in Toronto, Canada which took the lives of 10 people was perpetrated by a member of the INCEL Revolution, a misogynistic movement fomented on digital platforms such as Reddit and 4chan.[169] 10) Countries and regions are starting to develop their own digital governance regulations. → The U.S. digital governance model prioritises innovation and lawmakers intervene only when things go wrong. A new bill (the Online Privacy Act) was introduced in Nov. 2019 and if adopted, would create user rights, place obligations on companies to protect users' data, establish a new federal agency to enforce privacy protections, and strengthen enforcement of privacy law violations.[170] →In the European Union, the precautionary principle which puts citizen protection, ethics and responsible management before tech innovation underpins the 2018 General Data Protection Regulation (GDPR). The GDPR provides EU citizens with tough privacy protections and gives fines to tech companies that do not comply with these regulations. Some EU countries have taken further steps to protect their citizens' data. For	

[167] The OSCE issued a report on this topic in 2016 titled 'New challenges to freedom of expression: countering online abuse of female journalists' available here: https://www.osce.org/fom/220411?download=true.

[168] Tactical Tech reports about this here: https://ourdataourselves.tacticaltech.org/posts/shrinking-civil-space-a-digital-perspective/.

[169] An article from The Guardian covers this story here: https://www.theguardian.com/world/2018/apr/25/raw-hatred-why-incel-movement-targets-terrorises-women.

[170] Read more about the Online Privacy Act here: https://eshoo.house.gov/news-stories/press-releases/eshoo-lofgren-introduce-the-online-privacy-act/.

	instance, Germany recently blocked Facebook from pooling cross-platform data without user consent.[171] → The Chinese Personal Information Security Specification establishes the principle of data sovereignty that specifies that all information of citizens must be stored in-country and can be accessed on-demand by the Chinese government. With its 'Great firewall' built on a tight concentration of state-run network operators, China also uses data obtained from its tech giants to inform domestic surveillance, using a combination of facial recognition technology, catalogued biometric data, and artificial intelligence.[172] → Russia's sovereign Internet law gives the government the possibility to switch off connections within Russia and to disconnect its networks from the rest of the world. What has been called an 'online Iron Curtain' by some enables the Russian Government to decide what constitutes a threat (such as a foreign cyberattack) and what actions should be taken. The country is currently routing the country's web traffic and data through state-controlled points, reducing reliance on foreign servers over which it has less control. By 2021, it aims to have finished developing its own net address books so that it can operate almost autonomously.[173]	

[171] Read more about the EU's General Data Protection Regulation here: https://gdpr-info.eu/.

[172] The Centre for Strategic and International Studies reports about this here: https://www.csis.org/growing-need-us-leadership-technology-regulation ; The Brookings Institution also issued a policy brief on this: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

[173] See CNBC coverage of this here : https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html; refer to the policy brief of the Brookings Institution for more information here: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

4. Policy implications and suggested action points

Policy making requires preparing for a range of plausible futures and their respective as well as compounded implications. The four plausible futures of civic space presented in the previous chapter raise important questions which DAC members could consider when addressing the issue of civic space in the context of digital transformation. This chapter puts forward relevant policy considerations for each of the four futures, including suggested action points, to support DAC members in designing development co-operation policies related to civic space in forward-looking ways.[174] The policy implications primarily address DAC members; however some may also be considered relevant by other providers of development co-operation.

These policy considerations are regrouped by scenario to support DAC members to easily identify *what action for what situation*. However, they do not seek to be exhaustive, nor are they static. Rather, they aim to highlight a limited number of relevant actions DAC members can take to leverage the opportunities and mitigate the challenges specific to each of the four future scenarios put forward in this paper, focusing specifically on what can be achieved within the framework of development co-operation. Some policy implications and action points can be relevant to more than one future; moreover, one or more action points of one future can be selected and applied in combination with one or more action points of other futures – as relevant – depending on how the actual trajectory of civic space evolves.

Collectively – and in response to all four scenarios – the DAC can also consider supporting the development of policy guidance or a recommendation on enabling environments for civil society, which addresses – among other issues – effective donor support for the promotion and protection of civic space, including in the digital age.[175]

[174] The policy considerations are informed by several sources, including: (i) the Open Government Partnership's 'Strengthening Democracy and Protecting Civic Rights in the Digital Era': https://www.opengovpartnership.org/strengthening-democracy-and-protecting-civic-rights-in-the-digital-era/; (ii) Oxfam's blog 'From Poverty to Power: Here's what we know about closing civic space': https://oxfamblogs.org/fp2p/heres-what-we-know-about-closing-civic-space-what-other-research-would-you-suggest; (iii) the European Parliament's 'A governance framework for algorithmic accountability and transparency' report: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf; (iv) the European Commission's 'Tackling Online disinformation' https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation; (v) OECD's 'Artificial Intelligence in Society' report: https://ec.europa.eu/jrc/communities/sites/jrccties/files/eedfee77-en.pdf.

[175] This action point aligns with the action points of the study on *Development Assistance Committee Members and Civil Society* (OECD, 2020[1]).The guidance or recommendation can include pillars related to effective donor: (1) support to and engagement with civil society; (2) promotion and protection of civic spaces – including in the digital age; and (3) promotion of CSO effectiveness and accountability.

4.1. Policy considerations to address a future in which civic space collapses

How can DAC members address a future where actors (governments, companies, CSOs, etc.) have free rein to leverage digital technologies in adverse ways that considerably restrict the activities of digitally disadvantaged civil society, and accelerate the closing trend of civic space?

Currently, the majority of development co-operation policies tackle civic space and digital transformation as stand-alone issues. Preventing a future where civic space collapses in the face of digital transformation would require policies that recognise and address the inter-connections between both issues. In line with this, DAC members should consider developing digital policies that recognise digital implications for civic space and are consistent with the freedoms of association, peaceful assembly, expression and access to information. The United States Agency for International Development (USAID) sets a good example with its first-ever Digital Strategy (2020-2024).[176] The Strategy outlines USAID's vision for the responsible use of digital technology in development and humanitarian work. It seeks to advance the growth of self-reliant countries through "efficient, effective, and responsible digital initiatives that enhance security and economic prosperity, consistent with the values of respect for individual rights, freedom of expression, and the promotion of democratic norms and practices" (USAID, 2020[64]). In a similar vein, democracy assistance and CSO-related policies need to better incorporate the digital transformation dimension, including the need to promote democratic models of digital governance.

More fundamentally, it is important for DAC members to have a strategic policy document(s) that covers their work with civil society and CSOs. The strategic policy document(s) can articulate, among other things, a clear vision and objectives for promoting and protecting civic space, recognising concretely the following points: 1) the wide range of preconditions that are necessary to protect civic space e.g. freedoms of assembly, association, expression, access to information, strike and trade union rights, privacy, internet and media freedoms, rule of law, non-discrimination, etc.; 2) that civic space is not a means to an end but rather a precondition for meaningful civic participation in matters that affect the public (e.g. development of laws and policies, the delivery of services, spending of public money, etc.); 3) that a strategic and medium- to long-term approach to protecting civic space is required, as part of which digital issues should be front and centre; 4) that a sense of urgency is required as meaningful civic participation is central to democracies.

Suggested action points:

- Have a civil society or CSO-specific strategic policy document(s) recognising - among other points - the need to promote and protect civic space and address the challenges associated with digital transformation.
- Support policies and programming that address the inter-connection between civic space and digital transformation; integrate civic space considerations in digital policies/programming, and digital transformation considerations in democracy assistance or CSO-related policies/programming.

How can DAC members respond to partner country policies which abuse digital technologies to crack down on civic space e.g. restricting communications, accessing personal/user data for surveillance, or blocking/removing online content? Regulation alone at the international level is sometimes not enough; its efficiency only goes as far as the political will of each partner country to abide by it. International diplomacy in protecting civic space and countering negative narratives on civic space, can help make a difference.

[176] Find more information about USAID's digital strategy here: https://www.usaid.gov/usaid-digital-strategy.

How can DAC members work with partner countries to protect civic space within development co-operation?

Suggested action points:

- Halt activities in partner countries that could inadvertently support restrictive measures against civic space while supporting others that directly support partner countries to protect and expand civic space and reach the most vulnerable civil society actors.
- Work with partner countries – in co-operation with other providers of development co-operation – to promote civic space and counter negative narratives by highlighting the benefits of an open and enabled space for civil society (e.g. for the economy, to deliver on the SDGs, to tackle difficult social issues and corruption, etc.).

At the international level, efforts to strengthen cyber security and digital governance regulation are underway. However, the digital challenges of civic space will not be addressed without also adopting a bottom-up approach. In line with this, how can DAC members support CSOs to counter digital power asymmetries at the local level by increasing civil society knowledge of digital technologies (e.g. issues such as digital security, encryption, access to information and data privacy)? Good practices are starting to emerge among DAC members. For example, Denmark is supporting CSO digital resilience programmes in partner countries to counter shrinking space. Finland is supporting digital human rights defenders through the Digital Defenders Partnership (DDP).[177] In addition to providing financial support and expert assistance, DDP also produces guides and other tools for human rights defenders to raise awareness of potential threats related to security and human rights. Moreover, USAID promotes digital safety in repressive environments by supporting: (i) Training for at-risk journalists and activists; (ii) Training locally based digital security trainers; (iii) Broad campaigns to reach individuals who may not recognise the threats they face as Internet users; (iv) Civil society-led policy and advocacy projects that promote Internet freedom as part of a broader human rights agenda.[178]

Suggested action point:

- Support capacity building programmes that strengthen digital activism, skills and awareness raising of local CSOs, to reduce their vulnerability to repressions and support them to counter digital power asymmetries.

How should DAC members respond to partner countries which request digital development support (such as digital ID programmes)[179] and which do not have a safe and secure digital governance system in place, let alone a good record in protecting civic space? Should DAC members refrain from providing support in this area and proceed in steps, first ensuring that a solid digital governance system is established and legal measures are taken to promote enabling environments for civil society? If they decide not to engage in this area ("do no harm"), could this approach actually end up doing more harm, by leaving room for private companies or donors from authoritarian countries to support these programmes, with the risk that they do so with less consideration for human rights and open space principles?

[177] More information about this Partnership is available here: https://www.digitaldefenders.org/.

[178] Inputs from the October 2019 DAC meeting.

[179] From financial inclusion and migrant identification, to border security and state surveillance, digital identity constitutes a new, and potentially dangerous, tool to systematise and track individuals and groups.

Suggested action points:

- Conduct a risk assessment by weighing the pros and cons – as well as looking at implications - of providing digital support versus not providing such support.
- Make sure aid for digital development in partner countries (such as digital identity systems or base registers) does not inadvertently empower actors to use digital technologies against civic space. Ensure such support takes place only once basic digital rights are secured and other minimum standards/requirements are met (e.g. data protection, cyber security, etc.).
- Refrain from supporting digital development programmes in partner countries that have poor records in protecting civic space or loopholes in their existing digital governance systems.

What should DAC members' position be vis-à-vis tech companies that supply or support authoritarian regimes[180] and emerging donors and other providers of development co-operation that export digital technologies to countries that use them for repressive purposes? As per the recommendation of the 2019 Civil Society Belgrade Call to Action,181 should DAC members seek to regulate the sale, supply and export of dual-use items such as surveillance and cyber-surveillance technology and software, restricting trade in these goods to countries where their use may lead to civic space violations?[182]

Suggested action points:

- When considering private sector engagement policies – including with tech companies – take into account and address possible risks to civic space to ensure the respect of civic freedoms and fundamental digital rights of civil society.
- Ensure co-operation policies with other providers of development co-operation that export digital technologies do not entail risks for civic space.
- Review aid for trade policies – if needed – to address civic space risks in trade in surveillance technology.

How can DAC members recognise the legitimate interest of developing countries to protect national security and public health safety from a range of threats, not least espionage, hate speech, pandemics, terrorism and the like without compromising human rights and civic freedoms online, including the freedom of expression? How can DAC members help ensure that online content restrictions in developing countries meet international standards in the area of civic rights?

[180] E.g. by building tools that prevent citizens from exercising their rights to free expression; turning citizen data over to governments with poor human rights records; or providing surveillance that is likely to be used to violate user rights, etc.

[181] 2019 Civil Society Summit - Belgrade Call to Action – Action Agenda (point 11 page 13): https://gcap.global/wp-content/uploads/2019/05/Revised-April-Action-Agenda.pdf

[182] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, called for a moratorium on the transfer, sale, and use of surveillance technology until "rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways" (June 2019) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

Suggested action points:

- Engage with partner countries in developing rights-respecting governmental measures during a national emergency or crisis, and establishing safeguards to minimise risks for digital surveillance and other laws from being used to shrink civic space deliberately or inadvertently.
- Support partner country governments' work with civil society to undertake an impact assessment to ensure measures and actions such as digital surveillance and censorship do not inappropriately infringe upon digital rights and fundamental freedoms, including on line. Strengthen the capacities of legislative and judicial officials to conduct oversight of these measures and actions.
- Engage with partner countries in developing laws that strike a balance between countering hate speech while safeguarding freedom of expression, including by strengthening compliance with article 20(2) of the International Covenant on Civil and Political Rights (ICCPR).183
- Establish and strengthen partnerships with new and traditional media to address hate speech narratives and promote the values of tolerance, non-discrimination, pluralism, and freedom of opinion and expression.
- Support a new generation of digital citizens, empowered to recognize, reject and stand up to hate speech (e.g. media literacy programmes).

4.2. Policy considerations to address a future in which civic space flourishes

How can DAC members address a future where an enabling legal framework exists for civic space to flourish both on line and offline and where space is defended and expands through the responsive action of states, companies, CSOs and other actors?

Linking the DAC policy community to other relevant stakeholders will be key to enhance effective polices towards the protection of civic space in the digital age (Journal of Democracy, 2019[52]). Including CSOs when issues of digital technology ethics and development are being deliberated can play a vital role in forecasting, mitigating and preventing the potential misuses of digital technologies from a civil society and civic space perspective (Charities Aid Foundation, 2018[39]). As one of the key end-users of the benefits, but also the ones that face the impacts of digital transformation, DAC members should engage civil society in development co-operation policy-making processes involving the governance/regulation and responsible use of digital technology, including via the DAC-CSO Dialogue Framework.[184] DAC members should also seek to engage other relevant stakeholders i.e. other providers of development co-operation, the private sector and tech industry, investors, engineers, technologists and researchers. For example, USAID partners with the tech sector in North America to ensure that tech tools and products are designed

[183] Rather than prohibiting hate speech as such, international law prohibits the incitement to discrimination, hostility and violence. Article 20(2) of the International Covenant on Civil and Political Rights (ICCPR): Any measures undertaken to remove online content that is considered harmful must serve a legitimate aim and adhere to the principles of legality and proportionality. The removal or shutting down of online content and the criminalisation of online activity such as hate speech should happen only when there is a clear incitement to discrimination, hostility and violence to avoid any form of censorship, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[184] The DAC-CSO Dialogue Framework adopted in 2018 offers CSOs a space to engage with and influence the DAC as well as for the DAC to leverage CSO knowledge and capabilities in development co-operation: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DCD/DAC(2018)28/FINAL&docLanguage=En.

to consider the privacy and digital safety concerns of end-users in cyber-repressive environments. USAID assists these companies to deploy cutting-edge technologies to the field for testing and use.[185]

> *The issue of the governance of technologies and regulation in the cyber sphere must be addressed through multi-stakeholder and participatory governance models, rather than by private corporation alone. International, cross-sectoral and open multi-stakeholder initiatives are needed to promote the development of multi-stakeholder, consensus-driven global technical standards for trustworthy digital technologies (OECD, 2019[17]).*

Suggested action points:

- Engage civil society in development co-operation policy-making processes involving the governance/regulation and responsible use of digital technology.
- Engage other relevant stakeholders (other providers of development co-operation, the private sector/tech industry, investors, etc.) in policy-making processes involving digital technology.
- Support consultation mechanisms in partner countries for civil society and other relevant stakeholders' feedback into the design and implementation of national digital strategies.
- Include questions related to digital transformation and civic space in bilateral policy dialogues with partner country governments.

How can DAC members make sure legal and regulatory frameworks for civic space in developing countries are fit for the digital age? These legal frameworks can include for example data rights and privacy laws,[186] cyber surveillance laws,[187] regulations that apply to national digital tech companies[188] and also media laws.[189] What policies and programmes are needed to foster an enabling environment for civic space by

[185] Written inputs from the United States following the October 2019 DAC meeting.

[186] Data protection legal frameworks take into account specific conditions for disclosure of personal data and data processing. They also support regulations which give rights to individuals to decide what is accessed, stored and shared independently of public bodies and corporations.

[187] Cyber surveillance regulations can address the procedures for governmental actors to obtain permission from an independent judiciary body; or the creation of cyber surveillance institutions and bodies where CSOs and individuals can safely denounce surveillance abuses as well as seek legal assistance.

[188] These regulations can include making sure tech companies promote principles of corporate social responsibility and are held accountable and are more responsive to the adverse effects that their products, services, and business operations have on users' rights. More specifically, regulations can require digital tech companies to: 1. Exercise due diligence to identify, prevent, mitigate, and account for how they address the impacts of their business and products on human rights and civic freedoms (by conducting impact assessments of their products and services); 2. Ensure transparency of their policies and practices (by granting users control over their information and ensuring that it is not being misused/ensuring data protection; being transparent regarding what data they collect and how they are processed/stored/used; when government is granted access to data; when online speech is censored; or when access to a service is blocked or restricted) (Freedom House, 2018[27]); 3. Establish grievance and remedy mechanisms if users rights have been violated (UN-OHCHR, 2019[7]).

[189] Media laws can require e.g. the adoption of social media codes of conduct for political campaigns or social media companies to report the misuse or manipulation of their platforms: https://www.birmingham.ac.uk/news/latest/2019/07/whatsapp-both-strengthens-and-undermines-nigerian-democracy-says-uk-nigeria-research-team.aspx.

e.g. limiting abusive surveillance; safeguarding against arbitrary shutdowns; and preventing personal data from being misused and the spread of disinformation? This requires supporting the fulfilment of digital rights with due guaranteeing of civic freedoms. The same rights that civil society has offline, including the rights to freedom of expression, peaceful assembly and association, as well as access to information, need to be fully protected on line against state interference and the commercial interests of Internet service providers.

Suggested action points:

- Support programmes that strengthen digital-related laws and practices in developing countries which adhere to, comply with or complement international human rights law and meet international standards for civic rights.
- Support programmes that build local capacities of legal, judicial and security officials and institutions to address actions violating digital rights.
- Support programmes that strengthen media and social media-related laws and practices in developing countries which tackle disinformation.
- Support programmes that build local media capacities for quality, investigative journalism (including in local languages).
- Support programmes that tackle disinformation by strengthening e.g. public communication efforts (proactive, transparent and pre-emptive dissemination of information and deployment of counter-narratives); media literacy among civil society; and public service media.[190]

4.3. Policy considerations to address a future in which civic space transforms itself

How can DAC members support and adjust to the transformation of civic space; a space that is not only used by civil society to assemble, express itself and associate; but one that is characterised by the prevalence of digitally-empowered and digitally-operating civil society actors who use it to practice direct democracy?

So far, DAC members have been engaging primarily with professionalised and institutionalised CSOs. With digital transformation, the rise of different forms of digital activism and digital civil society actors requires new types of partnerships and donor support. For example, large-scale, global social movements face specific challenges related to translating short-term civic activism/mobilisation into actual political change with lasting impacts in the long-term; legitimising their work; and being more responsive to local constituencies.

Suggested action point:

- Review policies and strategies for engagement with civil society, and develop new modalities to work with and support non-traditional, digitally-empowered forms of civil society actors such as small-scale decentralised or large-scale global social movements.

[190] Public service media is a shared multi-platform media space that is relevant, credible and impartial. PSM is essential for an informed and effective democracy and should be accessible and accountable to all citizens.

Non-traditional tech companies are emerging and gaining ground outside the monopolisation of giant tech companies which concentrate digital market power today. These non-traditional tech companies foster civic space and E-Democracy[191] through civic technologies, as well as support open source software that are rights and value-based. To date, DAC members have not yet explored the potential of partnering with civic tech companies although these can help ensure business practices adhere to principles of corporate social responsibility, as well as the responsible stewardship of trustworthy, ethical, human-centric[192] and human-driven[193] digital technologies, with strengthened safeguards for civic space and mechanisms for transparency, oversight, and redress.

> *Technology companies and governments have a responsibility to more proactively shape the development and use of digital technologies, placing civic freedoms at the heart of this process, in order to make the online environment more closely reflect democratic norms and values (RAND Europe, 2017[15]).*

Suggested action point:

- Review policies and strategies for engagement with and support to non-traditional private sector partners such as non-profit tech companies which specialise in the development of civic technologies.

4.4. Policy considerations to address a future in which civic space breaks apart

How can DAC members address a future where civic space has broken into micro spaces that vary in levels of openness and inclusiveness, induced by the proliferation of self-contained digital regimes and widened digital divides that have further exacerbated the fragmentation of civic space?

How can DAC members better tackle the digital divide between and within countries that has resulted in inequalities in the way civil society across the world access information and exercise civic freedoms on line (BMZ, 2019[65])? How can DAC members ensure Internet access is inclusive and addresses barriers to affordability and accessibility, in particular for underrepresented and disadvantaged communities and geographically isolated regions? For example, the Belgian Ministry responsible for Development Co-operation produced a Strategic Policy Note called 'Digital for Development' (D4D) which focuses on the promotion of digital technologies for greater inclusion.[194] More specific considerations for DAC members include the following:

Should DAC members support legal frameworks that protect the rights of users to access, use and receive content over the Internet as well as specify conditions under which Internet service providers can control or price Internet content and protocol?

---

[191] For example: Votem (https://votem.com/) is a mobile voting system that supports both voter registration and voting using end-to-end blockchain-based encryption. Companies like Kialo (https://www.kialo.com/) support online debate-style communication through a deliberative discourse platform designed to present hundreds of supporting and opposing arguments in a dynamic argument tree.

[192] Anticipating the technological needs of citizens.

[193] Formulating tech approaches in partnership with citizens.

[194] The Strategic Policy Note 'Digital for Development' is available here: https://diplomatie.belgium.be/en/policy/development_cooperation/what_we_do/themes/digital_for_development_d4d

Online civic space requires a digital infrastructure that is robust, universal and regulated in a way that maintains it as accessible and open for all stakeholders. Should DAC members support digital infrastructure programmes including, for example, more sustainable and autonomous community networks and points for public access, such as libraries, schools and universities (ICNL, CSRG, CIPESA, 2019[24]); and establishing quality broadband Internet infrastructure in rural areas?

Should DAC members support digital education programmes for civil society groups with limited access to and lower usage rates of digital technologies (i.e. youth, women, low-income individuals, individuals living in rural areas, migrants, refugees, etc.) to help them learn how to effectively use digital technologies across the breadth of applications? Have DAC members considered supporting projects and initiatives by CSOs in DAC countries or international CSOs that have digital expertise and can support marginalised communities in becoming digitally literate, such as Front Line Defenders, for example?[195]

What response can DAC members bring to the collapse of the press and the adverse impacts this has on the cohesion of civic spaces?

Suggested action points:

- Promote a digital space that is free, open and inclusive; promote digital inclusion and leaving no one behind in the digital era, including by supporting:
  - Programmes that strengthen legal frameworks that protect Internet rights and digital freedoms of all people.
  - Digital infrastructure programmes.
  - Digital literacy policies and training programmes for marginalised civil society groups, including in partnership with DAC member-based CSOs or international CSOs.
- Support programmes that strengthen the press and community-level media in particular, as an agenda integrator locally, regionally and globally, and as a fundamental pillar of civic space cohesion.

Should DAC members be more engaged in strengthening the compliance of national legal regulations in partner countries with international digital governance frameworks and commitments such as the UN-OHCHR Guiding Principles on Business and Human Rights,[196] the Montreal Declaration for responsible AI development,[197] the Paris Call for trust and security in cyberspace,[198] the EU General Data Protection Regulation,[199] the OECD Recommendation of the Council on Artificial Intelligence;[200] the OECD

[195] Front Line Defenders provides trainings and resource materials on security and protection, including digital security. Read more about this organisation here: https://www.frontlinedefenders.org/.

[196] UN-OHCHR Guiding Principles on Business and Human Rights : https://www.ohchr.org/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf

[197] Montreal Declaration for responsible AI development: https://www.montrealdeclaration-responsibleai.com/the-declaration

[198] Paris Call for trust and security in cyberspace : https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf

[199] EU General Data Protection Regulation : https://gdpr-info.eu/

[200] OECD Recommendation of the Council on Artificial Intelligence : https://www.oecd.org/going-digital/ai/principles/

Recommendation of the Council on Digital Government Strategies,[201] and UNESCO's ROAM-X indicators?[202] Can these frameworks apply indiscriminately to all developing country contexts (i.e. "one size fits all") or will their systematic application have unintended negative consequences?

> *With the emergence of "digital authoritarianism", stronger responses are needed to develop a democratic model of digital governance that can outcompete authoritarian ones. This is an essential challenge of the next 10-15 years that will determine the dominant approach to policy making and global governance more broadly. Liberal democracies that share an interest in protecting global civic space will need to co-ordinate their action and co-operate to address digital challenges that are cross border. These range from surveillance and social media manipulation to cross-border data flows and common terms of use across platforms (Brookings, 2019[66]).*

Suggested action point:

- Support programmes that strengthen the compliance of national laws and regulations with international digital governance frameworks, while also paying attention to country context.

[201] OECD Recommendation of the Council on Digital Government Strategies: www.oecd.org/gov/digital-government/Recommendation-digital-governmentstrategies.pdf; The Recommendation aims to support the development and implementation of digital government strategies that bring governments closer to citizens and businesses.

[202] UNESCO's ROAM-X indicators : https://en.unesco.org/themes/internet-universality-indicators

Table 4.1. Summary of suggested action points to address each plausible future

Cross-cutting action point: Collectively, the DAC can consider supporting the development of policy guidance or a DAC Recommendation on enabling environments for civil society, which addresses among other issues, effective donor support for the promotion and protection of civic space – including in the digital age

Civic space collapses	Civic space flourishes	Civic space transforms itself	Civic space breaks apart
✓ Have a civil society or CSO-specific strategic policy document(s) recognising - among other points - the need to promote and protect civic space and address the challenges associated with digital transformation. Support policies and programming that address the inter-connection between civic space and digital transformation; integrate civic space considerations in digital policies/programming, and digital transformation considerations in democracy assistance or CSO-related policies/ programming. ✓ Halt activities in partner countries that could inadvertently support restrictive measures against civic space while supporting others that directly support partner countries to protect and expand civic space and reach the most vulnerable civil society actors. ✓ Work with partner countries – in co-operation with other providers of development co-operation – to promote civic space and counter negative narratives by highlighting the benefits of an open and enabled space for civil society (e.g. for the economy, to deliver on the SDGs, to tackle difficult social issues and corruption, etc.). ✓ Support capacity-building programmes that strengthen digital activism, skills and awareness raising of local CSOs, to reduce their vulnerability to repressions and support them to counter digital power asymmetries. ✓ Conduct risk assessments and refrain from providing digital support to countries where such support could inadvertently do harm (for example countries that have poor records in protecting civic space, loopholes in their existing digital governance systems or that do not respect the basic digital rights of civil society). ✓ Consider and address risks for civic space in: (i) aid for trade policies that involve surveillance technology; (ii) co-operation with other providers of development co-operation that export digital technologies; (iii) engagement with the private sector (tech companies). ✓ Engage with partner countries in developing rights-respecting governmental measures during a national emergency or crisis, and establishing safeguards to minimise risks for digital surveillance and	✓ Engage civil society in development co-operation policy-making processes involving the governance/regulation and responsible use of digital technology. ✓ Engage other relevant stakeholders (other providers of development co-operation, the private sector/tech industry, investors, etc.) in development co-operation policy-making processes on digital issues. ✓ Support consultation mechanisms in partner countries for civil society and other relevant stakeholders' feedback into the design and implementation of national digital strategies. ✓ Include questions related to digital transformation and civic space in bilateral policy dialogues with partner country governments. ✓ Support programmes that strengthen digital-related laws and practices in developing countries which adhere to, comply with or complement international human rights law and meet international standards for civic rights. ✓ Support programmes that build local capacities of legal, judicial and security officials and institutions to address actions violating digital rights. ✓ Support programmes that strengthen media and social media-related laws and practices in developing countries which tackle disinformation. ✓ Support programmes that build local media capacities for quality, investigative journalism (including in local languages). ✓ Support programmes that tackle disinformation by strengthening e.g. public communication efforts (proactive, transparent and pre-emptive dissemination of information and deployment of counter-narratives); media literacy among civil society; and public service media.	✓ Review policies and strategies for engagement with civil society, and develop new modalities to work with and support non-traditional, digitally-empowered forms of civil society actors such as small-scale decentralised or large-scale global social movements. ✓ Review policies and strategies for engagement with and support to non-traditional private sector partners such as non-profit tech companies which specialise in the development of civic technologies.	✓ Promote a digital space that is free, open and inclusive; promote digital inclusion and leaving no one behind in the digital era, including by supporting: -Programmes that strengthen legal frameworks that protect the Internet rights and digital freedoms of all individuals. - Digital infrastructure programmes. - Digital literacy policies and training programmes for marginalised civil society groups, including in partnership with DAC member-based CSOs or international CSOs. ✓ Support programmes that strengthen the press and community-level media in particular, as an agenda integrator locally, regionally and globally, and as a fundamental pillar of civic space cohesion. ✓ Support programmes that strengthen the compliance of national laws and regulations with international digital governance frameworks, while also paying attention to country context.

Civic space collapses	Civic space flourishes	Civic space transforms itself	Civic space breaks apart
other laws from being used to shrink civic space deliberately or inadvertently. Support partner country governments' work with civil society to undertake an impact assessment of such measures and strengthen the capacities of legislative and judicial officials to conduct oversight. ✓ Engage with partner countries in developing laws that strike a balance between countering hate speech while safeguarding freedom of expression, including by strengthening compliance with article 20(2) of the International Covenant on Civil and Political Rights (ICCPR); strengthen partnerships with new and traditional media to address hate speech narratives; and support a new generation of digital citizens, empowered to recognize and reject hate speech.			

Note: The policy considerations are regrouped by scenario to support DAC members to easily identify *what action for what situation*. They do not seek to be exhaustive, nor are they static. They aim to highlight a limited number of relevant actions DAC members can take to leverage the opportunities and mitigate the challenges specific to each of the four future scenarios put forward in this paper, focusing specifically on what can be achieved within the framework of development co-operation. Some policy implications and action points can be relevant to more than one future; moreover, one or more action points of one future can be selected and applied in combination with one or more action points of other futures – as relevant – depending on how the actual trajectory of civic space evolves. The policy implications primarily address DAC members; however, some could also be considered relevant by other providers of development co-operation.

Annex A. Definitions

Box 4.1. Definitions

Civic space

Civic space is the place, physical, virtual, and legal, where people exercise their rights to freedom of association, expression, and peaceful assembly. By forming associations, by speaking out on issues of public concern, by gathering in online and offline fora, and by participating in public decision making, individuals use civic space to solve problems and improve lives. A robust and protected civic space forms the cornerstone of accountable, responsive democratic governance and stable societies (CIVICUS, n.d.[6]).

Civil society organisations (CSOs)

Civil society is the multitude of associations around which society voluntarily organises itself and which represent a wide range of interests and ties. CSOs can be defined to include all non-market and non-state organisations outside of the family in which people organise themselves to pursue shared interests in the public domain. They cover a wide range of organisations that include membership-based CSOs, cause-based CSOs and service-oriented CSOs. Examples include community-based organisations and village associations, environmental groups, women's rights groups, farmers' associations, faith-based organisations, labour/trade unions, foundations, co-operatives, professional associations, chambers of commerce, independent research institutes, NGOs and the not-for-profit media (OECD, 2012[67]).

Digital transformation

Digitisation is the conversion of analogue data and processes into a machine-readable format.

Digitalisation is the use of digital technologies and data as well as inter-connection that results in new activities or changes to existing activities.

Digital transformation refers to the economic and societal effects of digitisation and digitalisation (OECD, 2019[5]). It is the profound transformation of business and organisational activities, processes, competencies and models to fully leverage the changes and opportunities of a mix of digital technologies and their accelerating impact across society in a strategic and prioritised way, with present and future shifts in mind (i-SCOOP, n.d.[68]).

Driver of change or driving force

A factor causing change, affecting or shaping the future. Drivers can be characterised as direct or indirect (i.e. underlying). A direct driver influences an outcome in the system in an unambiguous way. An indirect driver – also called a moderating or mediating variable - acts more diffusely, changing one or more direct drivers (Forward Thinking Platform, 2014[3]).

Emerging pattern

A novel situation or new trend created by the same repeating signals of change (Forward Thinking Platform, 2014[3]).

Foresight

Foresight is the systematic, participatory and multi-disciplinary approach to explore mid- to long-term futures and drivers of change (Forward Thinking Platform, 2014[3]). It is a structured approach for looking beyond the expected future by: (i) Examining the strategic context. Analysing trends and drivers of possible future contexts and their inter-dependencies; (ii) Engaging a wide set of views. A diversity of perspectives helps to understand and separate the "signal from the noise", and to develop common knowledge and ownership; (iii) Exploring plausible futures (scenarios) and critical uncertainties; (iv) Identifying policy implications to help build resilience in alternative futures including new policy opportunities and challenges (OECD, 2018[4]).

Inductive method

The inductive method (or bottom-up method) in scenario-building is an approach which builds step-by-step on the data available. It allows the structure of the scenarios to emerge by itself. The overall framework is not imposed so that the storyline can grow out of the step-by-step combination of drivers (European Foresight Platform, 2020[69]).

Mega-trend

A mega-trend is a major trend that occurs at a large or global scale (Forward Thinking Platform, 2014[3]). A mega-trend also unfolds over an extended period of time. The lifespan of a mega-trend is usually a decade or longer. A mega-trend is linked to our present and can therefore be observed today. Unlike other drivers in foresight, a mega-trend can be backed up by verifiable data stretching into the past. Since a mega-trend is a development already underway, it shapes our future in a slow-moving away; one that cannot be turned around easily by humans and policy makers. As such, mega-trends are near certainties and they can serve as the backdrop against which plausible futures can be built. And while a mega-trend alone presents a high degree of measurability, a mega-trend interacting with other drivers of change can be open to interpretation (European Strategy and Policy Analysis System, 2019[70]).

Normative scenario

A normative scenario is a preferred scenario or future (Forward Thinking Platform, 2014[3]).

Plausible

Judged reasonable because of (i) its underlying assumptions; (ii) internal consistency; and (iii) logical connection. Plausibility does not imply that a future scenario will happen. It means that the combination of driving forces grounding a scenario can logically be connected to the final outcome of this scenario (Forward Thinking Platform, 2014[3]).

Scenario

A description of how the future may unfold according to an explicit, coherent and internally consistent set of assumptions about the combination and interplay of driving forces. A scenario includes two main features: (i) a description of the end-state i.e. what does the world look like at the end of the time horizon for which the scenario has been developed; (ii) a causal logic explaining how this future came about, describing a sequence of events (Forward Thinking Platform, 2014[3]).

Trend

General tendency or direction of a movement/change over time (Forward Thinking Platform, 2014[3]).

Uncertainty

A state of having limited knowledge about the future. Uncertainty is a feature of complex systems that cannot be ignored and must be engaged by exploring diverse futures and their consequences (Forward Thinking Platform, 2014[3]).

Early signal

An early indication of a potentially important new event or emerging phenomenon that could become an emerging pattern, a new trend and/or a driver of change (Forward Thinking Platform, 2014[3]).

Note: In the context of this paper, early signals were detected during a six-month period of weekly horizon scans, i.e. systematic outlooks to detect early signs of potentially important developments. Most early signals were detected in newspapers and magazines that span a wide geographic coverage.

Annex B. Collaborative and consultative process

In addition to carrying out an in-depth analysis of evidence from secondary resources and existing literature, the paper is informed by a series of consultations and collaborative efforts, including:

1. First OECD workshop on the futures of civic space (May 2019) that leveraged in-house capacity and expertise. Participants included: Ana Fernandes, Karin Fällman, Marilyn Cham, Piero Fontolan, Julia Staudt, Duncan Cass-Beggs, Holly Richards, Chiara Di Stefano, Mags Gaynor, and Nina Taka

2. Second OECD workshop on the futures of the interface of civic space and digital technologies (November 2019). Participants included: Ana Fernandes, Jacqueline Wood, Marilyn Cham, Krystel Montpetit, Alessandro Bellantoni, João Vasconcelos, Sidney Leclercq, Jessica Voorhees, Cibele Cesca, Kieran Jones, Nina Taka, Sofia Galanek and Takashi Yukizawa.

3. Written comments from experts from: the International Center for Not-for-Profit Law (Douglas Rutzen and Ona Flores), the International Civil Society Centre (Wolfgang Jamann), the School of International Futures (Cat Tully), Funders Initiative for Civil Society (Poonam Joshi) and University of Texas (Betty Sue Flowers).

4. Written consultation with CSOs through the DAC - CSO Reference Group[203] and Forus International[204].

5. Presentation and consultations on the draft paper at: the OECD Government Foresight Community Annual Meeting on 7-8 October 2019; the DAC Meeting on 15 October 2019 (written inputs were also received subsequently from DAC delegates); the Task Team on CSO Development Effectiveness and Enabling Environment meeting on 26 November 2019; and the Directorate General for International Co-operation and Development at the European Commission on 24 January 2020.

[203] Inputs were received from CSOs from India, Mongolia, Indonesia, the Philippines and Bangladesh as well as from Oxfam.

[204] Contributions from Forus reflect inputs from seven members including: Coordination Sud (France), NNGO (Nigeria), FINGO (Finland), CEPS (Seychelles), PPONG (Portugal), Accion (Chile), and NFN (Nepal).

References

Association for Progressive Communications (2019), *The rights to freedom of peaceful assembly and of association in the digital age: APC submission to the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association*, https://www.apc.org/en/pubs/rights-freedom-peaceful-assembly-and-association-digital-age-apc-submission-united-nations. [9]

Badie, B. (2019), *New Perspectives on the International Order: No Longer Alone in This World*. [89]

BBC News (2019), *Christchurch shootings: Social media races to stop attack footage*, https://www.bbc.com/news/technology-47583393. [31]

BBC News (2019), *Hong Kong protests: Twitter and Facebook remove Chinese accounts*, https://www.bbc.com/news/technology-49402222. [71]

BBC News (2019), *Hong Kong protests: YouTube shuts accounts over disinformation*, https://www.bbc.com/news/technology-49443489. [61]

Berger, C. (2017), *Content and platform regulation: The German case and what's to come in 2018*, https://medium.com/@_cberger_/will-germanys-approach-to-content-and-platform-regulation-prevail-in-2018-d7e6e2db5cb. [94]

Bernholz, L. (2018), *Philanthropy and Digital Civil Society: Blueprint 2019*, https://pacscenter.stanford.edu/publication/philanthropy-and-digital-civil-society-blueprint-2019/. [59]

BMZ (2019), *The digital transformation and development cooperation*, http://www.bmz.de/en/issues/wirtschaft/nachhaltige_wirtschaftsentwicklung/ikt/index.html. [65]

Broadband Commission for Sustainable Development, ITU, UNESCO (2019), *The State of Broadband: Broadband as a Foundation for Sustainable Development*, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf. [43]

Brookings (2019), *Democracy and disorder: the struggle for influence in the new geopolitics*, https://www.brookings.edu/wp-content/uploads/2019/02/FP_20190226_democracy_report_WEB.pdf. [66]

Carnegie (2017), *Global Civic Activism in Flux*, https://carnegieeurope.eu/2017/03/17/global-civic-activism-in-flux-pub-68301. [47]

Carnegie Endowment for International Peace (2020), *Civil Society and the Coronavirus: Dynamism Despite Disruption*, https://carnegieendowment.org/2020/04/21/civil-society-and-coronavirus-dynamism-despite-disruption-pub-81592. [21]

Carnegie Endowment for International Peace (2019), *Defending Civic Space: Is the International Community Stuck?*, https://carnegieendowment.org/2019/10/22/defending-civic-space-is-international-community-stuck-pub-80110. [95]

Carnegie Endowment for International Peace (2019), *The Global Expansion of AI Surveillance*, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847. [50]

Carothers, T. and S. Brechenmacher (2019), *Defending Civic Space: Four unresolved questions*, OECD Development Matters, https://oecd-development-matters.org/2019/05/31/defending-civic-space-four-unresolved-questions/. [72]

Center for American Progress (2019), *Mapping China's Global Governance Ambitions: Democracies Still Have Leverage to Shape Beijing's Reform Agenda*, https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/. [74]

Center for Strategic and International Studies (2019), *The Growing Need for U.S. Leadership on Technology Regulation*, https://www.csis.org/growing-need-us-leadership-technology-regulation. [57]

Charities Aid Foundation (2018), *Machine-Made Goods: Charities, Philanthropy and Artificial Intelligence*, https://www.cafonline.org/docs/default-source/about-us-policy-and-campaigns/ai-philanthropy-and-civil-society-discussion-paper-final-correct_vp.pdf. [39]

CIVICUS (n.d.), *Guide to reporting on civic space*, http://www.civicus.org/documents/reports-and-publications/reporting-civic-space/Guide-to-Reporting-Civic-Space-Media-Toolkit.pdf. [6]

CIVICUS Monitor (2019), *Tracking civic space*, https://monitor.civicus.org/PeoplePowerUnderAttack2019/. [88]

CONCORD Europe, FOND Romania (2018), *Development is going digital*, https://concordeurope.org/wp-content/uploads/2018/10/CONCORD_FOND_DevelopmentGoingDigital_Report_2018.pdf. [32]

Council on Foreign Relations (2019), *Hate Speech on Social Media: Global Comparisons*, https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons. [30]

Dalberg (2018), *Future of Digitalization: Impacts on NGOs and ICSOs*, https://partos.nl/fileadmin/files/Pdfs/Strategizing_for_Digitalisation___Connectivity_-_Dalberg.pdf. [76]

DanChurchAid & DareDisrupt (2019), *Civic Tech*, http://dx.doi.org/file:///C:/Users/Cham_M/Downloads/Civic%20tech%20mapping%20final_FEB19_PDFa.pdf. [48]

Digital Civil Society Lab - Stanford PACS (2017), *Closing Civic Space in the Digital Age*, https://vimeo.com/247522795. [51]

DW Akademie (2018), *Digital Rights: Civic space continues to be constrained*, https://www.dw.com/en/digital-rights-civic-space-continues-to-be-constrained/a-43625163. [58]

EDRi (2019), *The digital rights of LGBTQ+ people: When technology reinforces societal oppressions*, https://edri.org/the-digital-rights-lgbtq-technology-reinforces-societal-oppressions/. [55]

European Center for Not-for-Profit Law (2020), *COVID-19 RESPONSES – WHY WE NEED TO PROTECT THE HUMAN RIGHT TO ASSEMBLE AND ACT ONLINE*, http://ecnl.org/covid-19-responses-why-we-need-to-protect-the-human-right-to-assemble-and-act-online/. [8]

European Economic and Social Committee (2017), *The future evolution of civil society in the European Union by 2030*, https://www.eesc.europa.eu/sites/default/files/files/qe-04-17-886-en-n.pdf. [49]

European Foresight Platform (2020), *n/a*, http://www.foresight-platform.eu/. [69]

European Journal of Law and Technology (2016), *AstroTurfing, 'CyberTurfing' and other online persuasion campaigns*, http://ejlt.org/article/view/501/635. [29]

European Parliamentary Research Service - Scientific Foresight Unit (2019), *A governance framework for algorithmic accountability and transparency*, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf. [45]

European Strategy and Policy Analysis System (2019), *Global Trends to 2030: Challenges and choices for Europe*, https://ec.europa.eu/epsc/sites/epsc/files/espas_report2019.pdf. [70]

Forbes (2020), *Coronavirus: How Artificial Intelligence, Data Science And Technology Is Used To Fight The Pandemic*, https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/#2e8209785f5f. [46]

Foreign Policy (2018), *Life Inside China's Social Credit Laboratory*, https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/. [25]

Forward Thinking Platform (2014), *A Glossary of Terms commonly used in Futures Studies*, http://www.fao.org/docs/eims/upload/315951/Glossary%20of%20Terms.pdf. [3]

Freedom House (2019), *Freedom on the Net 2019: the crisis of social media*, https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf. [28]

Freedom House (2018), *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism. [27]

Front Line Defenders (2019), *Global Analysis Report*, https://www.frontlinedefenders.org/sites/default/files/global_analysis_2019_web.pdf. [18]

Global Citizen (2017), *8 Massive Moments Hashtag Activism Really, Really Worked*, https://www.globalcitizen.org/en/content/hashtag-activism-hashtag10-twitter-trends-dresslik/. [13]

Global Voices (2019), *Chat bot lets Russians detained at protests request legal assistance*, https://globalvoices.org/2018/09/25/chat-bot-lets-russians-detained-at-protests-request-legal-assistance/. [60]

Heinrich Böll Foundation (2016), *The Future of Civic Space: Towards a Re-solidarisation and Re-politisation of Civil Society*, https://www.boell.de/en/2016/10/26/future-civic-space-towards-re-solidarisation-and-re-politisation-civil-society. [12]

ICNL, CSRG, CIPESA (2019), *Digital Space and the Protection of Freedoms of Association and Peaceful Assembly in Africa*, https://cipesa.org/?wpfb_dl=295. [24]

ICSW Civil Society Summit (2019), *The Belgrade Call to Action*, https://www.civicus.org/April-24-Final-Belgrade-Call-to-Action.pdf. [86]

International Center for Not-for-Profit Law (2020), *Coronavirus and civic space: preserving human rights during a pandemic*, https://www.icnl.org/post/analysis/coronavirus-and-civic-space. [2]

International Center for Not-for-Profit Law (2020), *Emerging Technology: Civic Space Future Trend Report*, https://mk0rofifiqa2w3u89nud.kinstacdn.com/wp-content/uploads/CS2040-Trend-Report-Emerging-Tech-vf.pdf?_ga=2.17579001.1331742450.1584901303-676892050.1580814069. [63]

i-SCOOP (n.d.), *Digital transformation: online guide to digital business transformation*, https://www.i-scoop.eu/digital-transformation/. [68]

ITU (2018), *Emerging Trends, ICT4SDG, Infrastructure, Regulation*, https://news.itu.int/itu-statistics-leaving-no-one-offline/. [40]

Journal of Civil Society (2019), *Conceptualizing government-organized non-governmental organizations*, http://dx.doi.org/file:///C:/Users/Cham_M/Downloads/ConceptualizingGovernmentOrganizedNonGovernmentalOrganizations.pdf. [83]

Journal of Democracy (2019), "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression", Vol. 30. [52]

Lawfare (2017), *The Policy Dimension of Leading in AI*, https://www.lawfareblog.com/policy-dimension-leading-ai. [53]

Lawley, C. (2019), *How The Social Media Tax Is Worsening Uganda's Digital Divides*, https://medium.com/goodthingsfoundation/how-the-social-media-tax-is-worsening-ugandas-digital-divides-7663adeec245. [42]

Lember, V., T. Brandsen and P. Tõnurist (2019), "The potential impacts of digital technologies on co-production and co-creation", *Public Management Review*, Vol. 21/11, pp. 1665-1686, http://dx.doi.org/10.1080/14719037.2019.1619807. [92]

Maplight (2019), *Digital Deception and Our Democracy*, https://maplight.org/story/digital-deception-and-our-democracy/. [34]

Media support (2016), *The chilling effects of online harassment and how to respond*, https://www.mediasupport.org/chilling-effects-online-harassment-address/. [81]

OECD (2020), *Development Assistance Committee Members and Civil Society*, The Development Dimension, OECD Publishing, Paris, https://dx.doi.org/10.1787/51eb6df1-en. [1]

OECD (2019), *Aid for Civil Society Organisations*, http://www.oecd.org/dac/financing-sustainable-development/development-finance-topics/Aid-for-CSOs-2019.pdf. [84]

OECD (2019), *Enabling Civil Society: Select survey findings*, https://doi.org/10.1787/54903a6a-en. [93]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264312012-en. [5]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [17]

OECD (2019), *Written consultation on 'the impacts of digital transformation on civic space' - Inputs from Forus International*. [14]

OECD (2019), *Written consultation on 'the impacts of digital transformation on civic space' - Inputs from the DAC-CSO Reference Group*. [10]

OECD (2018), *Development Co-operation Report 2018: Joining Forces to Leave No One Behind*, OECD Publishing, Paris, https://dx.doi.org/10.1787/dcr-2018-en. [4]

OECD (2016), "Economic and Social Benefits of Internet Openness", *OECD Digital Economy Papers*, No. 257, OECD Publishing, Paris, https://dx.doi.org/10.1787/5jlwqf2r97g5-en. [16]

OECD (2016), "Megatrends affecting science, technology and innovation", in *OECD Science, Technology and Innovation Outlook 2016*, OECD Publishing, Paris, https://dx.doi.org/10.1787/sti_in_outlook-2016-4-en. [44]

OECD (2012), *Partnering with Civil Society: 12 Lessons from DAC Peer Reviews*, https://www.oecd.org/dac/peer-reviews/12%20Lessons%20Partnering%20with%20Civil%20Society.pdf. [67]

OECD (2011), "An Overview of Growing Income Inequalities in OECD Countries: Main Findings", in *Divided We Stand: Why Inequality Keeps Rising*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264119536-3-en. [90]

OECD & UNDP (2019), *GPEDC Report: Making development co-operation more effective*, http://effectivecooperation.org/wp-content/uploads/2019/07/GPEDC_2019-Report_Glossy_EN_web-1.pdf. [85]

OECD Development Matters (2019), *Civic space is shrinking, yet civil society is not the enemy*, https://oecd-development-matters.org/2019/06/18/civic-space-is-shrinking-yet-civil-society-is-not-the-enemy/. [82]

Open Global Relations (2019), *How civil society can work to improve our technological future*, https://www.openglobalrights.org/how-civil-society-can-work-to-improve-our-technological-future/. [73]

Open Global Relations (2018), *How can AI amplify civic freedoms?*, https://www.openglobalrights.org/how-can-AI-amplify-civic-freedoms/. [23]

Open Government Partnership (2019), *Digital governance*, https://www.opengovpartnership.org/policy-area/digital-governance/. [33]

Open Government Partnership (n.d.), *Strengthening Democracy and Protecting Civic Rights in the Digital Era*, https://www.opengovpartnership.org/strengthening-democracy-and-protecting-civic-rights-in-the-digital-era/. [75]

OSCE (2019), *Joint Declaration on Challenges to Freedom of Expression in the Next Decade*, https://www.osce.org/representative-on-freedom-of-media/425282. [35]

Quartz (2018), *Say goodbye to grassroots politics. The future is made of Astroturf*, https://qz.com/1383626/say-goodbye-to-grassroots-politics-the-future-is-astroturf/. [78]

RAND Europe (2017), *Civic engagement: How can digital technologies underpin citizen-powered democracy?*, https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF373/RAND_CF373.pdf. [15]

Ranking digital rights (2018), *Corporate Accountability Index*, https://rankingdigitalrights.org/index2018/. [36]

Shahyan Khan (2017), *Leadership in the Digital Age - a study on the effects of digitalization on top management leadership*, Stockholm Business School. [96]

Tactical Tech (n.d.), *Shrinking Civil Space: A Digital Perspective*, https://ourdataourselves.tacticaltech.org/posts/shrinking-civil-space-a-digital-perspective. [26]

TechRadar (2019), *Majority of companies still aren't GDPR-compliant*, https://www.techradar.com/news/majority-of-companies-still-arent-gdpr-compliant. [37]

The Guardian (2019), *Facebook usage falling after privacy scandals, data suggests*, https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows. [80]

The Guardian (2019), *Think only authoritarian regimes spy on their citizens?*, https://www.theguardian.com/commentisfree/2019/sep/22/think-only-authoritarian-regimes-spy-on-their-citizens. [54]

The New York Times (2020), *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html?auth=link-dismiss-google1tap&campaign_id=51&emc=edit_MBE_p_20200302&instance_id=16401&nl=morning-briefing&regi_id=79621833tion%3DtopNews&section=topNews&segment_id=21778&te=1&. [91]

The New York Times (2019), *'We're at War': A Covert Social Media Campaign Boosts Military Rulers*, https://www.nytimes.com/2019/09/06/world/middleeast/sudan-social-media.html. [20]

The New York Times (2017), *Dilemma for Uber and Rival: Egypt's Demand for Data on Riders*, https://www.nytimes.com/2017/06/10/world/middleeast/egypt-uber-sisi-surveillance-repression-careem.html. [62]

UN Human Rights Council (2018), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (HRC/38/35)*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement. [77]

UNESCO (2019), *UNESCO'S Internet Universality Indicators: A Framework for Assessing Internet Development*, https://unesdoc.unesco.org/ark:/48223/pf0000367617. [56]

United Nations (2020), *COVID-19 and Human Rights*, https://www.un.org/sites/un2.un.org/files/un_policy_brief_on_human_rights_and_covid_23_april_2020.pdf. [22]

UN-OHCHR (2019), *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/141/02/PDF/G1914102.pdf?OpenElement. [7]

Unwin, T. (2019), *Can digital technologies really be used to reduce inequalities?*, https://oecd-development-matters.org/2019/02/28/can-digital-technologies-really-be-used-to-reduce-inequalities/. [38]

USAID (2020), *Digital Strategy*, https://www.usaid.gov/usaid-digital-strategy. [64]

Varieties of Democracy (V-DEM) Institute (2019), *Democracy Facing Global Challenges; Section 2: Threats to democracy in the digital age*, https://www.v-dem.net/media/filer_public/99/de/99dedd73-f8bc-484c-8b91-44ba601b6e6b/v-dem_democracy_report_2019.pdf. [11]

World Economic Forum (2017), *5 challenges for civil society in the Fourth Industrial Revolution*, https://www.weforum.org/agenda/2017/12/5-challenges-facing-civil-society-in-the-fourth-industrial-revolution/. [19]

World Economic Forum (2016), *4 billion people still don't have internet access.*, https://www.weforum.org/agenda/2016/05/4-billion-people-still-don-t-have-internet-access-here-s-how-to-connect-them/. [41]

World Economic Forum (2016), *More than half of the world's population is still offline. Here's what we're doing about it.*, https://www.weforum.org/agenda/2016/05/4-billion-people-still-don-t-have-internet-access-here-s-how-to-connect-them/. [87]

Youngs, R. (2015), *Rethinking Civil Society and Support for Democracy*, https://eba.se/wp-content/uploads/2015/04/Rapport-2015-01-med-framsida_f%C3%B6r_web.pdf. [79]