

# **The Age of Digital Interdependence**

**Report of the**

**UNITED NATIONS SECRETARY-GENERAL'S  
HIGH-LEVEL PANEL ON DIGITAL COOPERATION**

**June 2019**



## Contents

Foreword	3
Executive Summary	4
1. Introduction: Interdependence in the Digital Age	8
2. Leaving No One Behind	12
2.1 Creating an inclusive digital economy	12
2.2 Rethinking how we work and learn	18
2.3 Regional and global economic policy cooperation	20
3. Individuals, Societies and Digital Technologies	23
3.1 Human rights and human agency	23
3.2 Trust and social cohesion	27
3.3 Security	29
4. Mechanisms for Global Digital Cooperation	32
4.1 Challenges and gaps	32
4.2 Three possible architectures for global digital cooperation	34
4.3 The role of the UN	40
5. Recommendations	43
Annexes	49
I. Terms of Reference of the Panel	49
II. Panel Members	51
III. Panel Secretariat and Support Teams	52
IV. Donors	53
V. The Panel's Engagement	54
VI. Principles and Functions of Digital Cooperation	57
Notes	59

## Foreword

We live in an era of increasing interdependence and accelerating change, much of it driven by technological advances such as low-cost computing, the internet and mobile connectivity. Moments of change present new opportunities to solve old problems. The efficiency, innovation, and speed of a digitally connected world can expand what is possible for everyone – including those who historically have been marginalised.

At the same time, humanity faces significant new challenges. Modern technologies can be used to erode security and violate privacy. We are also beginning to see complex impacts on education systems and labor markets.

We believe the opportunities for human progress in the digital age ultimately outweigh the challenges – if we join together in a spirit of cooperation and inclusiveness.

We urgently need to lay the foundations of an inclusive digital economy and society for all. We need to focus our energies on policies and investments that will enable people to use technology to build better lives and a more peaceful, trusting world. Making this vision a reality will require all stakeholders to find new ways of working together. That is why the Secretary General appointed this Panel and what we have sought to do with this Report.

We are grateful to each member of the Panel, the Secretariat, and the many groups and individuals we consulted; though the views expressed were not always in agreement, they were always conveyed with respect and in the spirit of collaboration.

No one knows how technology will evolve, but we do know that our path forward must be built through cooperation and illuminated by shared human values. We hope this Report will contribute to improved understanding of the opportunities and challenges ahead, so that together we can shape a more inclusive and sustainable future for all.

Jack Ma

Melinda Gates

## Executive Summary

Digital technologies are rapidly transforming society, simultaneously allowing for unprecedented advances in the human condition and giving rise to profound new challenges. Growing opportunities created by the application of digital technologies are paralleled by stark abuses and unintended consequences. Digital dividends co-exist with digital divides. And, as technological change has accelerated, the mechanisms for cooperation and governance of this landscape have failed to keep pace. Divergent approaches and ad hoc responses threaten to fragment the interconnectedness that defines the digital age, leading to competing standards and approaches, lessening trust and discouraging cooperation.

Sensing the urgency of the moment, in July 2018 the Secretary-General of the United Nations (UN) appointed this Panel to consider the question of “digital cooperation” – the ways we work together to address the social, ethical, legal and economic impact of digital technologies in order to maximise their benefits and minimise their harm. In particular, the Secretary-General asked us to consider how digital cooperation can contribute to the achievement of the Sustainable Development Goals (SDGs) – the ambitious agenda to protect people and the planet endorsed by 193 UN member states in 2015. He also asked us to consider models of digital cooperation to advance the debate surrounding governance in the digital sphere.

In our consultations – both internally and with other stakeholders – it quickly became clear that our dynamic digital world urgently needs improved digital cooperation and that we live in an age of digital interdependence. Such cooperation must be grounded in common human values – such as inclusiveness, respect, human-centredness, human rights, international law, transparency and sustainability. In periods of rapid change and uncertainty such as today, these shared values must be a common light which helps guide us.

Effective digital cooperation requires that multilateralism, despite current strains, be strengthened. It also requires that multilateralism be complemented by multi-stakeholderism – cooperation that involves not only governments but a far more diverse spectrum of other stakeholders such as civil society, academics, technologists and the private sector. We need to bring far more diverse voices to the table, particularly from developing countries and traditionally marginalised groups, such as women, youth, indigenous people, rural populations and older people.

After an introduction which highlights the urgency of improved digital cooperation and invites readers to commit to a Declaration of Digital Interdependence, our report focuses on three broad sets of interlocking issues, each of which is discussed in one subsequent chapter. As a panel, we strove for consensus, but we did not always agree. We have noted areas where our views differed and tried to give a balanced summary of our debates and perspectives. While there was not unanimity of opinion among the Panel members regarding all of the recommendations, the Panel does endorse the full report in the spirit of promoting digital cooperation.

Chapter 2, **Leaving No One Behind**, argues that digital technologies will only help progress towards the full sweep of the SDGs if we think more broadly than the important issue of access to the internet and digital technologies. Access is a necessary, but insufficient, step forward. To capture the power of digital technologies we need to cooperate on the broader ecosystems that enable digital technologies to be used in an inclusive manner. This will require policy frameworks that directly support economic and social inclusion, special efforts to bring traditionally marginalised groups to the fore, important investments in both human capital and infrastructure,

smart regulatory environments, and significant efforts to assist workers facing disruption from technology's impact on their livelihoods. This chapter also addresses financial inclusion – including mobile money, digital identification and e-commerce –, affordable and meaningful access to the internet, digital public goods, the future of education, and the need for regional and global economic policy cooperation.

Chapter 3, **Individuals, Societies and Digital Technologies**, underscores the fact that universal human rights apply equally online as offline, but that there is an urgent need to examine how time-honoured human rights frameworks and conventions should guide digital cooperation and digital technology. We need society-wide conversations about the boundaries, norms and shared aspirations for the uses of digital technologies, including complicated issues like privacy, human agency and security in order to achieve inclusive and equitable outcomes. This chapter also discusses the right to privacy, the need for clear human accountability for autonomous systems, and calls for strengthening efforts to develop and implement global norms on cybersecurity.

To take significant steps toward the vision identified in Chapters 2 and 3, we feel the following priority actions deserve immediate attention:

#### **An inclusive digital economy and society**

**1A:** *We recommend that by 2030, every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to achieving the SDGs. Provision of these services should guard against abuse by building on emerging principles and best practices, one example of which is providing the ability to opt in and opt out, and by encouraging informed public discourse.*

**1B:** *We recommend that a broad, multi-stakeholder alliance, involving the UN, create a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs.*

**1C:** *We call on the private sector, civil society, national governments, multilateral banks and the UN to adopt specific policies to support full digital inclusion and digital equality for women and traditionally marginalised groups. International organisations such as the World Bank and the UN should strengthen research and promote action on barriers women and marginalised groups face to digital inclusion and digital equality.*

**1D:** *We believe that a set of metrics for digital inclusiveness should be urgently agreed, measured worldwide and detailed with sex disaggregated data in the annual reports of institutions such as the UN, the International Monetary Fund, the World Bank, other multilateral development banks and the OECD. From this, strategies and plans of action could be developed.*

#### **Human and institutional capacity**

**2:** *We recommend the establishment of regional and global digital help desks to help governments, civil society and the private sector to understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies.*

### Human rights and human agency

**3A:** *Given that human rights apply fully in the digital world, we urge the UN Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. Civil society, governments, the private sector and the public should be invited to submit their views on how to apply existing human rights instruments in the digital age in a proactive and transparent process.*

**3B:** *In the face of growing threats to human rights and safety, including those of children, we call on social media enterprises to work with governments, international and local civil society organisations and human rights experts around the world to fully understand and respond to concerns about existing or potential human rights violations.*

**3C:** *We believe that autonomous intelligent systems should be designed in ways that enable their decisions to be explained and humans to be accountable for their use. Audits and certification schemes should monitor compliance of artificial intelligence (AI) systems with engineering and ethical standards, which should be developed using multi-stakeholder and multilateral approaches. Life and death decisions should not be delegated to machines. We call for enhanced digital cooperation with multiple stakeholders to think through the design and application of these standards and principles such as transparency and non-bias in autonomous intelligent systems in different social settings.*

### Trust, security and stability

**4.** *We recommend the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.*

If we are to deliver on the promise of digital technologies for the SDGs, including the above-mentioned priority action areas, and avoid the risks of their misuse, we need purposeful digital cooperation arrangements. To this end, in Chapter 4, **Mechanisms for Global Digital Cooperation**, we analyse gaps in the current mechanisms of global digital cooperation, identify the functions of global digital cooperation needed to address them, and outline three sets of modalities on how to improve our global digital cooperation architecture – which build on existing structures and arrangements in ways consistent with our shared values and principles.

Given the wide spectrum of issues, there will of necessity be many forms of digital cooperation; some may be led by the private sector or civil society rather than government or international organisations. Moreover, special efforts are needed to ensure inclusive participation by women and other traditionally marginalised groups in all new or updated methods of global digital cooperation.

The three proposed digital cooperation architectures presented are intended to ignite focused, agile and open multi-stakeholder consultations in order to quickly develop updated digital governance mechanisms. The 75<sup>th</sup> Anniversary of the UN in 2020 presents an opportunity for an early harvest in the form of a “Global Commitment for Digital Cooperation” enshrining goals, principles, and priority actions.

The chapter also discusses the role of the UN, both in adapting to the digital age and in contributing to improved global digital cooperation.

We feel the following steps are warranted to update digital governance:

### **Global digital cooperation**

**5A:** *We recommend that, as a matter of urgency, the UN Secretary-General facilitate an agile and open consultation process to develop updated mechanisms for global digital cooperation, with the options discussed in Chapter 4 as a starting point. We suggest an initial goal of marking the UN's 75th anniversary in 2020 with a “Global Commitment for Digital Cooperation” to enshrine shared values, principles, understandings and objectives for an improved global digital cooperation architecture. As part of this process, we understand that the UN Secretary-General may appoint a Technology Envoy.*

**5B:** *We support a multi-stakeholder “systems” approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age.*

\* \* \*

We hope this report and its recommendations will form part of the building blocks of an inclusive and interdependent digital world, with a fit-for-purpose new governance architecture. We believe in a future in which improved digital cooperation can support the achievement of the SDGs, reduce inequalities, bring people together, enhance international peace and security, and promote economic opportunity and environmental sustainability.

# 1. Introduction: Interdependence in the Digital Age

Digital technologies are rapidly transforming societies and economies, simultaneously advancing the human condition and creating profound and unprecedented challenges. How well are we managing the complex impacts on our individual and collective lives? How can we use digital technologies to contribute to the achievement of the Sustainable Development Goals? What are current best practices and gaps in digital cooperation? What new ways of working together are needed, and who should be involved?

These are among the questions the UN Secretary-General asked us to consider.<sup>1</sup> We approached our task with both humility and urgency. The challenges are multi-faceted and rapidly evolving. The potential that could be unlocked by improved digital cooperation is enormous – and so are the perils if humanity fails to create more effective and inclusive ways for citizens, civil society, governments, academia and the private sector to work together.

**“Digital cooperation”** is used in this report to describe ways of working together to address the societal, ethical, legal and economic impacts of digital technologies in order to maximise benefits to society and minimise harms.

As digital technologies have come to touch almost every aspect of modern life, a patchwork of cooperation and governance mechanisms has gradually emerged to generate norms, standards, policies and protocols in this arena. In 2014, the United Nations identified 680 distinct mechanisms related to digital cooperation,<sup>2</sup> and the number has since risen to over a thousand.<sup>3</sup> In many technical areas, these mechanisms work well. But they struggle to keep up with the unprecedented pace and increasingly wide range of change.

While digital technologies have been developing for many years, in the last decade their cumulative impacts have become so deep, wide-ranging and fast-changing as to herald the dawn of a new age. The cost of massive computing power has fallen.<sup>4</sup> Billions of people and devices have come online.<sup>5</sup> Digital content now crosses borders in vast volumes, with constant shifts in what is produced and how and where it is used.

The spread of digital technologies has already improved the world in myriad ways. It has, for example, revolutionised the ability to communicate with others and to share and access knowledge. Individuals from long-neglected populations have used mobile money and other financial services for the first time, and started businesses that reach both domestic and global markets.<sup>6</sup> If we are to achieve the flagship ambition of the Sustainable Development Goals, to end extreme poverty by 2030, improved digital cooperation will need to play a vital role.

But digital technologies have also brought new and very serious concerns. Around the world, many people are increasingly – and rightly – worried that our growing reliance on digital technologies has created new ways for individuals, companies and governments to intentionally cause harm or to act irresponsibly. Virtually every day brings new stories about hatred being spread on social media, invasion of privacy by businesses and governments, cyber-attacks using weaponised digital technologies or states violating the rights of political opponents.<sup>7</sup>

And many people have been left out of the benefits of digital technology. Digital dividends co-exist with digital divides. Well more than half the world’s population still either lacks affordable access to the internet or is using only a fraction of its potential despite being connected.<sup>8</sup> People who lack safe and affordable access to digital technologies are overwhelmingly from groups who are already



marginalised: women, elderly people and those with disabilities; indigenous groups; and those who live in poor, remote or rural areas.<sup>9</sup> Many existing inequalities – in wealth, opportunity, education, and health – are being widened further.

The speed and scale of change is increasing – and the agility, responsiveness and scope of cooperation and governance mechanisms needs rapidly to improve. We cannot afford to wait any longer to develop better ways to cooperate, collaborate and reach consensus. We urgently need new forms of digital cooperation to ensure that digital technologies are built on a foundation of respect for human rights and provide meaningful opportunity for all people and nations.

### ***Our digital interdependence***

If we want to use digital technologies to improve life for everyone, we will have to go about it consciously and deliberately – with civil society, companies and governments recognising their interdependence and working together. The unique benefits and profound risks arising from the dramatic increase in computing power and interconnectivity in the digital age reinforce our underlying interdependence. Globally and locally, we are increasingly linked in an ever-expanding digital web, just as we are increasingly linked, and mutually dependent, in the spheres of economics, public well-being and the environment.

The critical need to improve digital cooperation comes at a time when many of the mechanisms of multilateral cooperation developed since World War II are under unprecedented duress. Although far from perfect, these avenues for cooperation between national governments underpinned one of the most peaceful and productive periods in human history. Their erosion is dangerous: it will make it harder to capitalise on the benefits of digital technologies and mitigate the hazards.

Reinvigorating multilateralism alone will not be sufficient. Effective digital cooperation requires that multilateralism be complemented by multi-stakeholderism – cooperation that involves governments and a diverse spectrum of other stakeholders such as civil society, technologists, academics, and the private sector (ranging from small enterprises to large technology companies).

While only governments can make laws, all these stakeholders are needed to contribute to effective governance by cooperating to assess the complex and dynamic impacts of digital technologies and developing shared norms, standards and practices. We need to bring far more diverse voices to the table, particularly from developing countries and traditionally marginalised populations. Important digital issues have often been decided behind closed doors, without the involvement of those who are most affected by the decisions.

Managing digital technologies to maximise benefits to society and minimise harms requires a far-sighted and wide-ranging view of the complex ways in which they interact with societal, environmental, ethical, legal and economic systems. The Panel is enormously grateful to the many individuals, institutions and others who provided us with their insights and expertise as we sought to better understand how to navigate this new landscape. We endeavoured to consult as broadly as possible in the time available.

Drawing on many thoughtful reflections,<sup>10</sup> we identified the following nine values that we believe should shape the development of digital cooperation:

- *Inclusiveness* – Leaving no one behind, so that we can maximise equality of opportunity, access and outcomes to achieve the Sustainable Development Goals;

- *Respect* – Embodying respect for human rights and human dignity, diversity, the safety and security of personal data and devices, and national and international law;
- *Human-centredness* – Maximising benefits to humans, and ensuring that humans remain responsible for decisions;
- *Human flourishing* – Promoting sustainable economic growth, the social good and opportunities for self-realisation;
- *Transparency* – Promoting open access to information and operations;
- *Collaboration* – Upholding open standards and interoperability to facilitate collaboration;
- *Accessibility* – Developing affordable, simple and reliable devices and services for as diverse a range of users as possible;
- *Sustainability* – Furthering the aim of a zero-carbon, zero-waste economy that does not compromise the ability of future generations to meet their own needs; and,
- *Harmony* – The use by governments and businesses of digital technologies in ways that earn the trust of peers, partners and people, and that avoid exploiting or exacerbating divides and conflicts.

### ***About this report***

As a panel, we strove for consensus, but we did not always agree. We have noted areas where our views differed and tried to give a balanced summary of our debates and perspectives. While there was not unanimity of opinion among the Panel members regarding all of the recommendations, the Panel does endorse the full report in the spirit of promoting digital cooperation.

The next three chapters highlight issues that emerged from the Panel's deliberations, setting out the backdrop for the recommendations in the final chapter. Our report does not aim to be comprehensive – some important topics are touched briefly or not at all – but to focus on areas where we felt digital cooperation could make the greatest difference. These chapters deal broadly with the areas of economics, society and governance, while noting that many issues – such as capacity, infrastructure and data – are relevant to all.

Chapter 2, **Leaving No One Behind**, assesses the contribution of digital technologies to the Sustainable Development Goals. It addresses issues including financial inclusion, affordable and meaningful access to the internet, the future of education and jobs and the need for regional and global economic policy cooperation.

Chapter 3, **Individuals, Societies and Digital Technologies**, discusses the application of human rights to the digital age, the need to keep human rights and human agency at the centre of technological development, and the imperative to improve cooperation on digital security and trust.

Chapter 4, **Mechanisms for Global Digital Cooperation**, identifies gaps in current mechanisms of global digital cooperation, the functions of digital cooperation and principles digital cooperation

should aim to follow, provides three options for potential new global digital cooperation architectures, and discusses the role of the United Nations in promoting digital cooperation.

Drawing on the analysis in the preceding chapters, Chapter 5 shares and explains our **Recommendations** for shaping our common digital future.

\* \* \*

As members of the Panel, we brought a wide range of experience of working in government, business, academic institutions, philanthropy and civil society organisations – but we engaged in our task as equal citizens of a digitalising world, appreciating the vital role of all stakeholders and the need for humility and cooperation.

In this spirit, we invite all stakeholders to commit to a ***Declaration of Digital Interdependence***:

***Humanity is still in the foothills of the digital age. The peaks are yet uncharted, and their promise still untold. But the risks of losing our foothold are apparent: dangerous adventurism among states, exploitative behaviour by companies, regulation that stifles innovation and trade, and an unforgivable failure to realise vast potential for advancing human development.***

***How we manage the opportunities and risks of rapid technological change will profoundly impact our future and the future of the planet.***

***We believe that our aspirations and vulnerabilities are deeply interconnected and interdependent; that no one individual, institution, corporation or government alone can or should manage digital developments; and that it is essential that we work through our differences in order to shape our common digital future.***

***We declare our commitment to building on our shared values and collaborating in new ways to realise a vision of humanity's future in which affordable and accessible digital technologies are used to enable economic growth and social opportunity, lessen inequality, enhance peace and security, promote environmental sustainability, preserve human agency, advance human rights and meet human needs.***

## 2. Leaving No One Behind

The Sustainable Development Goals represent humanity's shared commitment to achieve ambitious global gains for people and the planet by 2030. Of the SDG's 17 goals and 169 targets, not a single one is detached from the implications and potential of digital technology. From ending extreme poverty, to promoting inclusive economic growth and decent work, to reducing maternal mortality, to achieving universal literacy and numeracy and doubling the productivity of small farmers – progress is intertwined with the use of digital technology and new forms of digital cooperation.<sup>11</sup>

However, technological solutions are not enough. Diverse political systems, history, culture, resource constraints and other factors which have marginalised far too many people, are – and will continue to be – of critical importance. The application of technology must be aligned with investments in human capital, infrastructure and environmental protection. Widening access to digital technologies is necessary, but not sufficient. Access needs to be affordable to be meaningful. Special efforts are needed to remove barriers for marginalised groups who often face a double bind: they already face discrimination in its many analogue forms and are least likely to be connected. Pre-existing forms of marginalisation should not be perpetuated or aggravated in the digital sphere.

Success will require a commitment by all involved stakeholders to hard work and learning over many years about how to broaden opportunity and build truly inclusive economies and societies. We believe that there is significant room for digital technology and improved cooperation to contribute to these efforts.

### 2.1 Creating an inclusive digital economy

With mobile internet and increasingly powerful and lower cost computing, every person can theoretically connect to anyone else, obtain and generate knowledge, or engage in commercial or social activity.<sup>12</sup> For organisations of whatever size, likewise, there are fewer technical barriers to global economic interaction at scale. Digital technology can support economic inclusion by breaking down barriers to information, broadening access, and lowering the level of skills needed to participate in the economy.<sup>13</sup>

Of course, this does not mean that everyone and everything should be connected or digitised. Nor does it mean that the social and economic consequences of digital technology are necessarily inclusive or beneficial. Digital technology can both provide opportunity and accentuate inequality.

The challenge for policy makers, and other stakeholders seeking to contribute to progress toward the SDGs, is how to cooperate to leverage technology to create a more inclusive society. As we emphasise in this chapter and our recommendations, we believe digital cooperation must steer how digital technologies are developed and deployed to create meaningful economic opportunities for all.

Developing an inclusive digital economy will require sustained and coherent effort from many stakeholders across all walks of life. National policy frameworks and international agreements need to find ways to promote financial inclusion, innovation, investment and growth while protecting people and the environment, keeping competition fair and the tax base sustainable.

### ***Financial inclusion: mobile money, digital identification and e-commerce***

The ability of digital technologies to empower traditionally marginalised people and drive inclusive economic development is illustrated by financial inclusion.<sup>14</sup> Mobile money, digital identification and e-commerce have given many more people the ability to save and transact securely without needing cash, insure against risks, borrow to grow their businesses and reach new markets.

According to the World Bank's Global Findex 2017 report, 69 percent of adults have an account with a financial institution, up by seven percentage points since 2014. That means over half a billion adults gained access to financial tools in three years. But many are still left behind, and there is scope for further rapid progress: a billion people who still have no access to financial services already have a mobile phone.<sup>15</sup>

Mobile money – the ability to send, receive and store money using a mobile phone – has brought financial services to people who have long been ignored by traditional banks.<sup>16</sup> It reaches remote regions without physical bank branches. It can also help women access financial services – an important aspect of equality, given that in many countries women are less likely than men to have a bank account.<sup>17</sup>

New business models enable people who have no physical collateral to demonstrate to lenders that they are creditworthy – for example, by allowing the lenders to see phone location data and online transaction and payment history.<sup>18</sup> Mobile finance matters in wealthy countries, too, where low-income and historically marginalised groups generally both pay higher interest rates and receive a narrower range of financial services.<sup>19</sup>

Well-known examples of mobile money include Kenya's M-Pesa and China's Alipay. Launched in 2007 by Vodafone, M-Pesa received support from diverse stakeholders who all have a role to play in digital cooperation. A private sector innovation with donor funding, it originally addressed microfinance clients in partnership with civil society – then citizens found new uses, including low cost person-to-person transfers.<sup>20</sup> Alipay has made millions of small business loans to online merchants, more than half of whom are aged under 30.<sup>21</sup>

What works in one country may not work in another.<sup>22</sup> Rather than try to replicate specific successes, digital cooperation should aim to highlight best practices, standards and principles that can create conditions for local innovations to emerge and grow based on local issues, needs and cultural values. India, for example, has added 300 million bank accounts in three years as new business models have been built on the India Stack, a set of government-managed online standards in areas including online payments and digital identity.<sup>23</sup>

Across many areas of financial inclusion, fragmented systems and lack of cooperation within and across states make it difficult to fully realise the benefits of digital technology. Common standards for cross-border interoperability of mobile money could unleash much more innovation: discussions to develop them should be a priority for digital cooperation.<sup>24</sup>

Digital identification (ID) can support inclusive economic development more broadly. More than a billion people today lack an official way to prove their identity: this means they may not be able to vote, open a bank account, transact online, own land, start a business, connect to utilities or access public services such as health care or education.<sup>25</sup> The consulting firm McKinsey & Company

studied seven large countries and concluded that digital ID systems could add between 3 and 13% to their gross domestic product.<sup>26</sup>

However, digital ID systems require caution. A digital ID can help unlock new opportunities but can also introduce new risks and challenges. They can be used to undermine human rights – for example, by enabling civil society to be targeted, or selected groups to be excluded from social benefits.<sup>27</sup> Data breaches can invade the privacy of millions. To minimise risks, countries should introduce a digital ID system only after a broad national conversation and allow for voluntary enrolment and viable alternatives for those who opt out. They should establish ways to monitor use and redress misuse. Countries could cooperate to share experience and best practices in this regard.

The World Bank Identification for Development (ID4D) initiative has identified ten Principles of Digital Identification covering inclusion, design and governance “to improve development outcomes while maintaining trust and privacy”.<sup>28</sup> This initiative draws on the experiences of countries that have already implemented digital ID systems. Among the most successful is Estonia, where citizens can use their digital ID to access over 2,000 online government services. Building on the positive and cautionary lessons of early adopters, the Modular Open Source Identity Platform (MOSIP) is developing open source code countries can adapt to design their own systems.<sup>29</sup>

Recent years have also seen a dramatic increase in e-commerce, including by individuals and small businesses selling products and services using online platforms. When e-commerce platforms provide technological services to small entrepreneurs, rather than compete with them, they can level the playing field: it is relatively cheap and simple to start a business online, and entrepreneurs can reach markets far beyond their local area.

Inclusive e-commerce, which promotes participation of small firms in the digital economy, is particularly important for the SDGs as it can create new opportunities for traditionally excluded groups. In China, for example, an estimated 10 million small and medium-sized enterprises (SMEs) sell on the Taobao platform; nearly half of the entrepreneurs on the platform are women, and more than 160,000 are people with disabilities.<sup>30</sup> E-commerce can support rural economic inclusion as clusters of villages can develop market niches in certain types of products: in China, an estimated 3,000 “Taobao villages” have annual online sales of more than one million dollars annually.<sup>31</sup> A growing e-commerce sector also creates demand and employment in related businesses including logistics, software, customised manufacturing and content production.

E-commerce shows how digital technologies with supportive policies can contribute to inclusive economic development – it has done best in countries where it is relatively easy to set up a business, and where traditionally neglected populations are able to get online.<sup>32</sup> As with inclusive mobile finance, as more individuals and small enterprises buy and sell internationally, there is also a need to create more supportive rules for cross-border e-commerce.

As e-commerce grows, there are also concerns about its relation to local and international markets, as discussed below in Section 2.3.

### ***Harnessing data and ‘digital public goods’ for development***

The immense power and value of data in the modern economy can and must be harnessed to meet the SDGs, but this will require new models of collaboration.

The Panel discussed potential pooling of data in areas such as health, agriculture and the environment to enable scientists and thought leaders to use data and artificial intelligence to better understand issues and find new ways to make progress on the SDGs. Such data commons would require criteria for establishing relevance to the SDGs, standards for interoperability, rules on access and safeguards to ensure privacy and security.

We also need to generate more data relevant to the SDGs. In a world which has seen exponential growth of data in recent years,<sup>33</sup> many people remain invisible. For example, the 2018 UN SDG Report notes that only 73 percent of children under the age of 5 have had their births registered.<sup>34</sup> The World Health Organization (WHO) estimated in 2014 that two-thirds of deaths are not registered.<sup>35</sup> Only 11 countries in sub-Saharan Africa have data on poverty from surveys conducted after 2015. Most countries do not collect sex-disaggregated data on internet access.<sup>36</sup>

Anonymised data – information that is rendered anonymous in such a way that the data subject is not or no longer identifiable – about progress toward the SDGs is generally less sensitive and controversial than the use of personal data of the kind companies such as Facebook, Twitter or Google may collect to drive their business models, or facial and gait data that could be used for surveillance.<sup>37</sup> However, personal data can also serve development goals, if handled with proper oversight to ensure its security and privacy.

For example, individual health data is extremely sensitive – but many people's health data, taken together, can allow researchers to map disease outbreaks, compare the effectiveness of treatments and improve understanding of conditions. Aggregated data from individual patient cases was crucial to containing the Ebola outbreak in West Africa.<sup>38</sup> Private and public sector healthcare providers around the world are now using various forms of electronic medical records. These help individual patients by making it easier to personalise health services, but the public health benefits require these records to be interoperable.

There is scope to launch collaborative projects to test the interoperability of data, standards and safeguards across the globe. The World Health Assembly's consideration of a global strategy for digital health in 2020 presents an opportunity to launch such projects, which could initially be aimed at global health challenges such as Alzheimer's and hypertension.<sup>39</sup>

Improved digital cooperation on a data-driven approach to public health has the potential to lower costs, build new partnerships among hospitals, technology companies, insurance providers and research institutes and support the shift from treating diseases to improving wellness. Appropriate safeguards are needed to ensure the focus remains on improving health care outcomes. With testing, experience and necessary protective measures as well as guidelines for the responsible use of data, similar cooperation could emerge in many other fields related to the SDGs, from education to urban planning to agriculture.

### **Data collaboration for climate change, agriculture and the environment**

The Platform for Big Data in Agriculture was launched in 2017 by the Colombia-based International Center for Tropical Agriculture after consultation with public, private and non-profit stakeholders. By providing ways to share data on agriculture, it seeks to transform research and innovation in food security, sustainability and climate change.<sup>40</sup>

More broadly, cheaper sensors generating more data – and better AI algorithms to analyse it – can further improve our understanding of how complex environmental systems interact and the likely impacts of climate change.<sup>41</sup>

Digital technologies can also be used to reduce waste. The methods of complex coordination that have lowered costs by enabling supply chains to touch every corner of the planet can also help to meet higher environmental standards and design devices with repair, reuse, upgrading and recycling in mind. For this, new forms of digital cooperation and data sharing would be needed among suppliers, customers and competitors.

Many types of digital technologies and content – from data to apps, data visualisation tools to educational curricula – could accelerate achievement of the SDGs. When they are freely and openly available, with minimal restrictions on how they can be distributed, adapted and reused, we can think of them as “digital public goods”.<sup>42</sup> In economics, a “public good” is something which anyone can use without charge and without preventing others from using it.<sup>43</sup> Digital content and technologies lend themselves to being public goods in this respect.

Combinations of digital public goods can create “common rails” for innovation of inclusive digital products and services. The India Stack is an example of how a unified, multi-layered software platform with clear standards, provided by public entities, can give government agencies and entrepreneurs the technological building blocks to improve service delivery and develop new business models which promote economic inclusion.<sup>44</sup>

There is currently no “go to” place for discovering, engaging with, building, and investing in digital public goods. Along the lines of the MOSIP model – and with the participation of civil society and other stakeholders – such a platform could create great value by enabling the sharing and adaptation of digital technologies and content across countries in a wider range of areas relevant to achieving the SDGs.

### ***Expanding access to digital infrastructure***

The proportion of people online in the developing world expanded rapidly in the last decade – from 14.5% in 2008 to 45.3% in 2018 – but progress has recently slowed.<sup>45</sup> Internet access in many parts of the world is still too slow and expensive to be effectively used.<sup>46</sup> The cost of mobile data as a percent of income increased in nearly half the countries according to a recent study.<sup>47</sup> Without affordable access, advances in digital technologies disproportionately benefit those already connected, contributing to greater inequality.

The people being left behind are typically those who can least afford it. Growth in new internet connections is slowest in the lowest-income countries.<sup>48</sup> Rural areas continue to lag, as companies prioritise improving access in more densely populated areas which will offer a better return on investment.<sup>49</sup>



The slowing progress in bringing more people online points to the urgent need for new approaches to building digital infrastructure, a complex task that requires better coordination among many stakeholders: governments, international organisations, communications service providers, makers of hardware and software, providers of digital services and content, civil society and the various groups that oversee protocols and standards on which digital networks operate.<sup>50</sup> As these actors cooperate, it also represents an important moment to re-emphasise and address the complex social, cultural and economic factors that continue to marginalise many groups.

It is not an easy task: progress is slowing despite there being an active community of donors, experts and other institutions committed to universal digital connectivity. The Alliance for Affordable Internet, for example, brings together companies, civil society organisations and governments to conduct research and policy advocacy on driving down the cost to connect and achieve universal, affordable internet access.<sup>51</sup> The International Telecommunication Union (ITU) and the United Nations Educational, Scientific and Cultural Organization (UNESCO) lead the Broadband Commission,<sup>52</sup> the United Nations Children's Fund (UNICEF)'s Project Connect maps schools using satellite data and artificial intelligence,<sup>53</sup> and the World Bank provides loans and grants for connectivity projects.<sup>54</sup>

There has also been considerable private sector activity in this arena. Loon, a project of Google's parent company Alphabet, uses internet-enabled balloons – in the aftermath of Hurricane Maria, they provided connectivity to 200,000 in Puerto Rico.<sup>55</sup> Amazon, OneWeb, Telesat, Space Norway and SpaceX are among companies considering connectivity solutions using low-earth orbit satellites.<sup>56</sup>

Some countries, such as Indonesia, have set targets that treat internet connectivity as a national priority.<sup>57</sup> While finance alone will not achieve universal internet access, it can help if invested wisely: some countries are generating financing from fees on existing communication network providers to help expand systems to those who are currently uncovered, for example through Universal Service Funds.<sup>58</sup>

Advance market commitments deserve further consideration as a possible way to incentivise investment, as they have in other areas such as vaccine developments. They involve a commitment to pay for a future product or service once it exists; the commitment in this case could come from consortia of governments, international organisations or others interested in enabling specific uses in areas such as health or education.<sup>59</sup>

Many local groups are also working on small-scale community solutions: for example, a rural community of 6,000 people in Mankosi, South Africa, built a solar-powered "mesh network" in collaboration with a university.<sup>60</sup> Such community projects are often not just about getting online but building skills and empowering locals to use technology for development and entrepreneurship.<sup>61</sup>

Digital cooperation should increase coordination among the public and private entities working in this space and help tailor approaches to economic, cultural and geographic contexts. Governments have an important role to play in creating a policy framework to enable private sector enterprise, innovation, and cooperative, bottom-up networks.

### ***Supporting marginalised groups and measuring inclusiveness***

Even where getting online is possible and affordable, extra efforts are needed to empower groups that are discriminated against and excluded. For example, digital technologies are often not easily accessible for elderly people or those with disabilities;<sup>62</sup> indigenous people have little digital content in their native languages;<sup>63</sup> and globally an estimated 12 percent more men use the internet than women.<sup>64</sup>

Responses need to address deep and complex social and cultural factors, such as those contributing to the gender gap in access to and usage of mobile phones, smart phones and digital services – gaps which persist in many cases despite increases in women’s income and education levels.<sup>65</sup> Social marketing could play a role in changing attitudes, as it has in many other areas with backing from donors, governments and civil society organisations.<sup>66</sup> Initiatives to improve access for marginalised populations should start with consultation involving these groups in the design, deployment and evaluation of such efforts.

Efforts to improve digital inclusion would be greatly helped if there were a clear and agreed set of metrics to monitor it. Initial work – notably by the Organisation for Economic Co-operation and Development (OECD), the Group of Twenty (G20), ITU, and the Economist Intelligence Unit – needs to be broadened to reflect the wide variety of global contexts and, importantly, needs greater buy-in and participation from developing countries.<sup>67</sup> The Panel urges international organisations, civil society and governments to develop action plans around reliable and consistent measures of digital inclusion with sex disaggregated data. Discussion about measurements and definitions would also focus attention on the issues underlying inclusion.

## **2.2 Rethinking how we work and learn**

Many previous waves of technological change have shifted what skills are demanded in the labour market, making some jobs obsolete while creating new ones. But the current wave of change may be the most rapid and unpredictable in history. How to prepare people to earn a livelihood in the digital age – and how to protect those struggling to do so – is a critical question for digital cooperation for governments and other stakeholders who aim to reduce inequality and achieve the SDGs.

At this stage, there appears to be limited value in attempting to predict whether robots and artificial intelligence will create more jobs than they eliminate, although technology historically has been a net job creator.<sup>68</sup> Many studies attempt to predict the impact on the jobs market but there is far from being a consensus.<sup>69</sup> The only certainty is that workers have entered a period of vast and growing uncertainty – and that this necessitates new mechanisms of cooperation.

### ***Reforming education systems and supporting lifelong learning***

Modern schools were developed in response to the industrial revolution, and they may ultimately need fundamental reform to be fit for the digital age – but it is currently difficult to see more than the broad contours of the changes that are likely to be needed.

Countries are still in early stages of learning how to use digital tools in education and how to prepare students for digital economies and societies. These will be ongoing challenges for governments and other stakeholders. Some countries are now exposing even very young children

to science and robotics. Alongside such broader digital literacy efforts, it may be even more important to focus from an early age on developing children's "soft skills", such as social and emotional intelligence, creativity, collaboration and critical thinking. One widely referenced study concludes that occupations requiring such soft skills are less likely to be automated.<sup>70</sup>

Teaching about specific technologies should always be based on strong foundational knowledge in science and math, as this is less likely to become obsolete. At a degree level, science, technology, engineering and mathematics (STEM) curricula need to borrow from the humanities and social sciences, and vice versa: STEM students need to be encouraged to think about the ethical and social implications of their disciplines, while humanities and social science students need a basic understanding of data science.<sup>71</sup> More informal approaches to learning may be needed to prepare students for working in cross-disciplinary teams, and where such informal approaches already exist in the developing world they should be fully appreciated for their value.

As the boundaries increasingly blur between 'work' and 'learning', the need to enable and incentivise lifelong learning was emphasised in many of the written contributions the Panel received.

Lifelong learning should be affordable, portable and accessible to all. Responsibility for lifelong learning should be shared between workers themselves, governments, education institutions, the informal sector and industry: digital cooperation mechanisms should bring these groups together for regular debates on what skills are required and how training can be delivered. Workers should have flexibility to explore how best to opt into or design their own approach to lifelong learning.

There are emerging examples of government efforts to use social security systems and public-private partnerships to incentivise and empower workers to learn new skills and plan for a changing labour market. Among those drawn to the Panel's attention were efforts by the International Trade Union Confederation in Ghana and Rwanda,<sup>72</sup> France's *Compte Personnel de Formation*, Scotland's Individual Training Account, Finland's transformation of work and the labour market sub-group under its national AI programme, and Singapore's Skills Framework for Information and Communication Technology (ICT).

However, reskilling cannot be the only answer to inequality in the labour market – especially as the workers most able to learn new skills will be those who start with the advantage of comparatively higher levels of education.<sup>73</sup>

### ***Protecting workers, not jobs***

New business models are fuelling the rise of an informal or "gig" economy, in which workers typically have flexibility but not job or income security.<sup>74</sup> In industrialised countries, as more and more people work unpredictable hours as freelancers, independent contractors, agency workers or workers on internet platforms, there is an urgent need to rethink labour codes developed decades ago when factory jobs were the norm.<sup>75</sup>

Promising initiatives include Germany's Crowdsourcing Code of Conduct, which sets out guidelines on fair payment, reasonable timing and data protection for internet platform workers, and employs an ombudsman to mediate disputes; and Belgium's *Titre-Services* and France's *Chèque Emploi Service Universel*, which offer tax incentives for people engaging casual workers to participate in a voucher scheme that enables the workers to qualify for formal labour rights.

There are also examples of digital technologies enabling new ways for workers to engage in collective bargaining.<sup>76</sup>

While the gig economy tends to make work less formal in industrialised countries, in the developing world the majority of people have long worked in the informal sector.<sup>77</sup> For these workers, gig economy arrangements may be more formal and transparent, and – with appropriate cooperation measures with technology firms – easier for governments to oversee.<sup>78</sup> The challenge, as with industrialised countries, is to uphold labour rights while still allowing flexibility and innovation.

In all national contexts, protecting workers and promoting job creation in the digital age will require smart regulations and investments, and policies on taxation and social protection policies which support workers as they seek to transition to new opportunities.

### **2.3 Regional and global economic policy cooperation**

Taxation, trade, consumer protection and competition are among the areas of economic policy that require new thinking in the digital age: they are the ‘guard rails’ of the digital economy. Increased cooperation could lead to effective national approaches and experience informing regional and global multilateral cooperation arrangements.

Currently, however, there is a lack of regional and global standards in these areas, and multilateral cooperation is generally not working well. This may inflict far higher costs than is widely recognised. To take one relatively simple example, regional and global standards in areas such as interoperability of mobile money systems and best practices for digital ID would have considerable benefits. To discourage misuse, such standards and practices would also need to include clear accountability.

International trade rules need to be updated for the digital age. Technologies and trade have changed dramatically since 1998, for example, when the World Trade Organisation (WTO) last brokered an agreement on e-commerce.<sup>79</sup> In January 2019, 76 WTO member states announced the initiation of plurilateral negotiations on trade-related aspects of e-commerce.<sup>80</sup> Any agreement will need to address concerns of a diverse range of countries, including lower-income countries in which the e-commerce sector is less developed.<sup>81</sup>

Consumer protection is also relevant to discussions on international e-commerce. When consumers buy goods and services locally, they need to consider only local consumer protection. As an increasing number of e-commerce transactions take place across international borders, consumer protection based on agreed principles – such as OECD guidelines – could promote greater trust and better protect citizen interest.

It has likewise proved difficult so far to establish international standards or rules for the exchange of data. Trade rules were developed for goods and services that are produced and then consumed. By contrast, data which is “produced” by individuals and devices is not “consumed”, but rather can be used repeatedly, and gains value when combined with other data.<sup>82</sup>

Some argue that restrictions on data flows should be treated like any other trade barrier and generally minimised.<sup>83</sup> However, views differ sharply, and decisions on national legislation are complicated by concerns about privacy and security – discussed in the next chapter. Countries that require companies to store and process data within their national borders argue that it

promotes local innovation and investment in technology infrastructure and makes it easier to tax global corporations.<sup>84</sup> Others argue against such approaches on the basis that they are protectionist or represent an effort to obtain access to the data.

There is growing recognition that taxation is an area where digital technology has moved faster than policy frameworks. In particular, technology firms may operate business models – such as multi-sided platforms or “freemium” models – which offer free services to some individual users and earn revenue from other users, merchants or advertisers.<sup>85</sup> A company may provide services to millions of people in a country without establishing a legal entity or paying tax there. This has become a source of growing popular resentment.<sup>86</sup>

International digital cooperation could assist countries to develop appropriate tax policies. The G20 and OECD’s Base Erosion and Profit Shifting project is currently seeking consensus on issues such as how a global company’s tax receipts should be allocated to different jurisdictions based on its business activities.<sup>87</sup> An agreement in this area could offer countries a source of revenue that they could, for example, use to invest in human capital or lower the tax burden on small businesses.

Some countries are now taking unilateral action. Countries such as Italy, France and the United Kingdom (UK) have announced the intent to impose taxes on digital sales rather than profits, at least on an interim basis.<sup>88</sup> Other countries, such as Thailand, have amended tax rules relating to offshore digital services.<sup>89</sup> The lack of cooperation and coordination among different regulators is creating a patchwork of different national rules and regulations which makes trade and e-commerce more difficult. Ensuring that such emerging tax policies do not have unintended consequences on small enterprises or poor populations deserves special attention.

An international perspective is also needed to tackle concerns about competition, which have grown as large firms have established leading positions in many digital services. This is due in part to network effects: the more users a platform already has, the more attractive it becomes for new users and advertisers.

Recent discussions have proposed three main approaches.<sup>90</sup> First, a relatively laissez-faire approach that favours self-regulation or minimal regulation. Proponents argue that government regulation is often poorly conceived and counterproductive, harming innovation and economic dynamism. Critics counter that an overly hands-off approach has led to a concentration of market power in large firms and abuses of privacy that have sparked public and government concern. A second approach calls for more active state intervention to set rules for digital companies. Experience in industrial policy shows that such an approach can either help or hinder depending on many factors, including regulators’ willingness and ability to engage varied stakeholders in a smart discourse to balance competing interests effectively.<sup>91</sup> A third approach suggests regulating digital businesses as public utilities, analogous to railroads or electricity companies. The analogy is not an exact one, however, as physical infrastructure is easier to segment and harder to replicate than digital infrastructure and lends itself more easily to hosting competition among service providers. There is also dispute about how contestable are digital markets – that is, how vulnerable are the leading firms to new competitors. Moreover, traditional competition law operates far more slowly than changes in technology.

Finding the right approach in these areas will require not only different countries to work together, but also regulators in different government agencies. Models for how agencies can come together

for peer-to-peer information sharing include the International Conference of Data Protection & Privacy Commissioners and the International Competition Network.<sup>92</sup>

Alongside existing models, new models of governance and cooperation may be needed. They will need to be multi-stakeholder, including the private sector, civil society and users. Their debates should be transparent and open to citizens, as modelled by Mexico's National Institute for Transparency, Access to Information and Personal Data Protection.<sup>93</sup>

Where possible, new regulatory approaches should be tested on a small scale before being rolled out widely – through, for example, pilot zones, regulatory sandboxes or trial periods. We stress the overall need for a “systems” approach to cooperation and regulation that is multi-stakeholder, adaptive, agile and inclusive in Recommendation 5B.

However, regulators need to have sufficient resources and expertise to engage in such an approach – and the Panel's consultations highlighted concern that many regulators and legislators have insufficient understanding of complex digital issues to develop and implement policies, engage with companies developing technologies and explain issues to the public.<sup>94</sup> This increases the risk of regulations having unintended consequences.

There are several existing examples of initiatives to develop the capacity and understanding of public officials, from countries such as Israel,<sup>95</sup> Singapore<sup>96</sup> and the United Arab Emirates (UAE).<sup>97</sup> But much more could be done, and the Panel's Recommendation 2 envisages “digital help desks” which would broaden opportunities for officials and regulators to develop the skills needed for the smart governance that will be required to create inclusive and positive outcomes for all.

### 3. Individuals, Societies and Digital Technologies

The ultimate purpose of digital technology should always be to improve human welfare. Beyond the socio-economic aspects discussed in the previous chapter, digital technologies have proved that they can connect individuals across cultural and geographic barriers, increasing understanding and potentially helping societies to become more peaceful and cohesive.

However, this is only part of the story. There are also many examples of digital technologies being used to violate rights, undermine privacy, polarise societies and incite violence.

The questions raised are new, complex and pressing. What are the responsibilities of social media companies, governments and individual users? Who is accountable when data can move across the world in an instant? How can varied stakeholders, in nations with diverse cultural and historical traditions, cooperate to ensure that digital technologies do not weaken human rights but strengthen them?

#### 3.1 Human rights and human agency

Many of the most important documents that codify human rights were written before the age of digital interdependence. They include the Universal Declaration on Human Rights; the International Covenant on Economic, Social and Cultural Rights and the International Covenant on Civil and Political Rights; the Convention on the Elimination of all forms of Discrimination against Women; and the Convention on the Rights of the Child.

The rights these treaties and conventions codify apply in full in the digital age – and often with fresh urgency.

Digital technologies are widely used to advocate for, defend and exercise human rights – but also to violate them. Social media, for example, has provided powerful new ways to exercise the rights to free expression and association, and to document rights violations. It is also used to violate rights by spreading lies that incite hatred and foment violence, often at terrible speed and with the cloak of anonymity.

The most outrageous cases make the headlines. The live streaming of mass shootings in New Zealand.<sup>98</sup> Incitement of violence against an ethnic minority in Myanmar.<sup>99</sup> The #gamergate scandal, in which women working in video games were threatened with rape.<sup>100</sup> The suicides of a British teenager who had viewed self-harm content on social media<sup>101</sup> and an Indian man bullied after posting videos of himself dressed as a woman.<sup>102</sup>

But these are manifestations of a problem that runs wide and deep: one survey of UK adult internet users found that 40 percent of 16-24 year-olds have reported some form of harmful online content, with examples ranging from racism to harassment and child abuse.<sup>103</sup> Children are at particular risk: almost a third of under-18s report having recently been exposed to “violent or hateful contact or behaviour online”.<sup>104</sup> Elderly people are also more prone to online fraud and misinformation.

Governments have increasingly sought to cut off social media in febrile situations – such as after a terrorist attack – when the risks of rapidly spreading misinformation are especially high. But denying access to the internet can also be part of a sustained government policy that itself violates

citizens' rights, including by depriving people of access to information. Across the globe, governments directed 188 separate internet shutdowns in 2018, up from 108 in 2017.<sup>105</sup>

### ***Protecting human rights in the digital age***

Universal human rights apply equally online as offline – freedom of expression and assembly, for example, are no less important in cyberspace than in the town square. That said, in many cases it is far from obvious how human rights laws and treaties drafted in a pre-digital era should be applied in the digital age.

There is an urgent need to examine how time-honoured human rights frameworks and conventions – and the obligations that flow from those commitments – can guide actions and policies relating to digital cooperation and digital technology. The Panel's Recommendation 3A urges the UN Secretary-General to begin a process that invites views from all stakeholders on how human rights can be meaningfully applied to ensure that no gaps in protection are caused by new and emerging digital technologies.

Such a process could draw inspiration from many recent national and global efforts to apply human rights for the digital age.<sup>106</sup> Illustrative examples include:

- India's Supreme Court has issued a judgement defining what the right to privacy means in the digital context.<sup>107</sup>
- Nigeria's draft Digital Rights and Freedom Bill tries to apply international human rights law to national digital realities.<sup>108</sup>
- The Global Compact and UNICEF have developed guidance on how businesses should approach children's rights in the digital age.<sup>109</sup>
- UNESCO has used its Rights, Openness, Access and Multi-stakeholder governance (ROAM) framework to discuss AI's implications for rights including freedom of expression, privacy, equality and participation in public life.<sup>110</sup>
- The Council of Europe has developed recommendations and guidelines, and the European Court of Human Rights has produced case law, interpreting the European Convention on Human Rights in the digital realm.<sup>111</sup>

We must collectively ensure that advances in technology are not used to erode human rights or avoid accountability. Human rights defenders should not be targeted for their use of digital media.<sup>112</sup> International mechanisms for human rights reporting by states should better incorporate the digital dimension.

In the digital age, the role of the private sector in human rights is becoming increasingly pronounced. As digital technologies and digital services reach scale so quickly, decisions taken by private companies are increasingly affecting millions of people across national borders.

The roles of government and business are described in the 2011 UN Guiding Principles on Business and Human Rights. Though not binding, they were unanimously endorsed by the Human Rights Council and the UN General Assembly. They affirm that while states have the duty to protect rights and provide remedies, businesses also have a responsibility to respect human rights, evaluate risk and assess the human rights impact of their actions.<sup>113</sup>

There is now a critical need for clearer guidance about what should be expected on human rights from private companies as they develop and deploy digital technologies. The need is especially



pressing for social media companies, which is why our Recommendation 3B calls for them to put in place procedures, staff and better ways of working with civil society and human rights defenders to prevent or quickly redress violations.

We heard from one interviewee that companies can struggle to understand local context quickly enough to respond effectively in fast-developing conflict situations and may welcome UN or other expert insight in helping them assess concerns being raised by local actors. One potential venue for information sharing is the UN Forum on Business and Human Rights, through which the Office of the High Commissioner for Human Rights in Geneva hosts regular discussions among the private sector and civil society.<sup>114</sup>

Civil society organisations would like to go beyond information sharing and use such forums to identify patterns of violations and hold the private sector to account.<sup>115</sup> Governments also are becoming less willing to accept a hands-off regulatory approach: in the UK, for example, legislators are exploring how existing legal principles such as “duty of care” could be applied to social media firms.<sup>116</sup>

As any new technology is developed, we should ask how it might inadvertently create new ways of violating rights – especially of people who are already often marginalised or discriminated against. Women, for example, experience higher levels of online harassment than men.<sup>117</sup> The development of personal care robots is raising questions about the rights of elderly people to dignity, privacy and agency.<sup>118</sup>

The rights of children need especially acute attention. Children go online at ever younger ages, and under-18s make up one-third of all internet users.<sup>119</sup> They are most vulnerable to online bullying and sexual exploitation. Digital technologies should promote the best interests of children and respect their agency to articulate their needs, in accordance with the Convention on the Rights of the Child.

Online services and apps used by children should be subject to strict design and data consent standards. Notable examples include the American Children’s Online Privacy Protection Rule of 2013 and the draft Age Appropriate Design Code announced by the UK Information Commissioner in 2019, which defines standards for apps, games and many other digital services even if they are not intended for children.<sup>120</sup>

### ***Human dignity, agency and choice***

We are delegating more and more decisions to intelligent systems, from how to get to work to what to eat for dinner.<sup>121</sup> This can improve our lives, by freeing up time for activities we find more important. But it is also forcing us to rethink our understandings of human dignity and agency, as algorithms are increasingly sophisticated at manipulating our choices – for example, to keep our attention glued to a screen.<sup>122</sup>

It is also becoming apparent that ‘intelligent’ systems can reinforce discrimination. Many algorithms have been shown to reflect the biases of their creators.<sup>123</sup> This is just one reason why employment in the technology sector needs to be more diverse – as noted in Recommendation 1C, which calls for improving gender equality.<sup>124</sup> Gaps in the data on which algorithms are trained can likewise automate existing patterns of discrimination, as machine learning systems are only as good as the data that is fed to them.

Often the discrimination is too subtle to notice, but the real-life consequences can be profound when AI systems are used to make decisions such as who is eligible for home loans or public services such as health care.<sup>125</sup> The harm caused can be complicated to redress.<sup>126</sup> A growing number of initiatives, such as the Institute of Electrical and Electronics Engineers (IEEE)'s Global Initiative on Ethics of Autonomous and Intelligent Systems, are seeking to define how developers of artificial intelligence should address these and similar problems.<sup>127</sup>

Other initiatives are looking at questions of human responsibility and legal accountability – a complex and rapidly-changing area.<sup>128</sup> Legal systems assume that decisions can be traced back to people. Autonomous intelligent systems raise the danger that humans could evade responsibility for decisions made or actions taken by technology they designed, trained, adapted or deployed.<sup>129</sup> In any given case, legal liability might ultimately rest with the people who developed the technology, the people who chose the data on which to train the technology, and/or the people who chose to deploy the technology in a given situation.

These questions come into sharpest focus with lethal autonomous weapons systems – machines that can autonomously select targets and kill. UN Secretary-General António Guterres has called for a ban on machines with the power and discretion to take lives without human involvement, a position which this Panel supports.<sup>130</sup>

The Panel supports, as stated in Recommendation 3C, the emerging global consensus that autonomous intelligent systems be designed so that their decisions can be explained, and humans remain accountable. These systems demand the highest standards of ethics and engineering. They should be used with extreme caution to make decisions affecting people's social or economic opportunities or rights, and individuals should have meaningful opportunity to appeal. Life and death decisions should not be delegated to machines.

### ***The right to privacy***

The right to privacy<sup>131</sup> has become particularly contentious as digital technologies have given governments and private companies vast new possibilities for surveillance, tracking and monitoring, some of which are invasive of privacy.<sup>132</sup> As with so many areas of digital technology, there needs to be a society-wide conversation, based on informed consent, about the boundaries and norms for such uses of digital technology and AI. Surveillance, tracking or monitoring by governments or businesses should not violate international human rights law.

<p>It is helpful to articulate what we mean by “privacy” and “security”. We define “<b>privacy</b>” as being about an individual’s right to decide who is allowed to see and use their personal information. We define “<b>security</b>” as being about protecting data, on servers and in communication via digital networks.</p>
--

Notions and expectations of privacy also differ across cultures and societies. How should an individual’s right to privacy be balanced against the interest of businesses in accessing data to improve services and government interest in accessing data for legitimate public purposes related to law enforcement and national security?<sup>133</sup>

Societies around the world debate these questions heatedly when hard cases come to light, such as Apple’s 2016 refusal of the United States Federal Bureau of Investigation (FBI)’s request to assist in unlocking an iPhone of the suspect in a shooting case.<sup>134</sup> Different governments are taking different approaches: some are forcing technology companies to provide technical means of access, sometimes referred to as “backdoors”, so the state can access personal data.<sup>135</sup>

Complications arise when data is located in another country: in 2013, Microsoft refused an FBI request to provide a suspect's emails that were stored on a server in Ireland. The United States of America (USA) has since passed a law obliging American companies to comply with warrants to provide data of American citizens even if it is stored abroad.<sup>136</sup> It enables other governments to separately negotiate agreements to access their citizens' data stored by American companies in the USA.

There currently seems to be little alternative to handling cross-border law enforcement requests through a complex and slow-moving patchwork of bilateral agreements – the attitudes of people and governments around the world differ widely, and the decision-making role of global technology companies is evolving. Nonetheless, it is possible that regional and multilateral arrangements could develop over time.

For individuals, what companies can do with their personal data is not just a question of legality but practical understanding – to manage permissions for every single organisation we interact with would be incredibly time consuming and confusing. How to give people greater meaningful control over their personal data is an important question for digital cooperation.

Alongside the right to privacy is the important question of who realises the economic value that can be derived from personal data. Consumers typically have little awareness of how their personal information is sold or otherwise used to generate economic benefit.

There are emerging ideas to make data transactions more explicit and share the value extracted from personal data with the individuals who provide it. These could include business models which give users greater privacy by default: promising examples include the web browser Brave and the search engine DuckDuckGo.<sup>137</sup> They could include new legal structures: the UK<sup>138</sup> and India<sup>139</sup> are among countries exploring the idea of a third-party 'data fiduciary' who users can authorise to manage their personal data on their behalf.

### **3.2 Trust and social cohesion**

The world is suffering from a "trust deficit disorder", in the words of the UN Secretary-General addressing the UN General Assembly in 2018.<sup>140</sup> Trust among nations and in multilateral processes has weakened as states focus more on strategic competition than common interests and behave more aggressively. Building trust, and underpinning it with clear and agreed standards, is central to the success of digital cooperation.

Digital technologies have enabled some new interactions that promote trust, notably by verifying people's identities and allowing others to rate them.<sup>141</sup> Although not reliable in all instances, such systems have enabled many entrepreneurs on e-commerce platforms to win the trust of consumers, and given many people on sharing platforms the confidence to invite strangers into their cars or homes.

In other ways, digital technologies are eroding trust. Lies can now spread more easily, including through algorithms which generate and promote misinformation, sowing discord and undermining confidence in political processes.<sup>142</sup> The use of artificial intelligence to produce "deep fakes" – audio and visual content that convincingly mimics real humans – further complicates the task of telling truth from misinformation.<sup>143</sup>

Violations of privacy and security are undermining people's trust in governments and companies. Trust between states is challenged by new ways to conduct espionage, manipulate public opinion and infiltrate critical infrastructure. While academia has traditionally nurtured international cooperation in artificial intelligence, governments are incentivised to secrecy by awareness that future breakthroughs could dramatically shift the balance of power.<sup>144</sup>

The trust deficit might in part be tackled by new technologies, such as training algorithms to identify and take down misinformation. But such solutions will pose their own issues: could we trust the accuracy and impartiality of the algorithms? Ultimately, trust needs to be built through clear standards and agreements based on mutual self-interest and values and with wide participation among all stakeholders, and mechanisms to impose costs for violations.

All citizens can play a role in building societal resilience against the misuse of digital technology. We all need to deepen our understanding of the political, social, cultural and economic impacts of digital technologies and what it means to use them responsibly. We encourage nations to consider how educational systems can train students to thoughtfully consider the sources and credibility of information.

There are many encouraging instances of digital cooperation being used to build individual capacities that will collectively make it harder for irresponsible use of digital technologies to erode societal trust.<sup>145</sup> Examples drawn to the Panel's attention by written submissions and interviews include:

- The 5Rights Foundation and British Telecom developed an initiative to help children understand how the apps and games they use make money, including techniques to keep their attention for longer.<sup>146</sup>
- The Cisco Networking Academy and United Nations Volunteers are training youth in Asia and Latin America to explore how digital technologies can enable them to become agents of social change in their communities.<sup>147</sup>
- The Digital Empowerment Foundation is working in India with WhatsApp and community leaders to stop the spread of misinformation on social media.<sup>148</sup>

### **How can trust be promoted in the digital age?**

The problem of trust came up repeatedly in written contributions to the Panel. Microsoft's contribution stressed that an atmosphere of trust incentivises the invention of inclusive new technologies. As Latin American human rights group Derechos Digitales put it, "all participants in processes of digital cooperation must be able to share and work together freely, confident in the reliability and honesty of their counterparts". But how can trust be promoted? We received a large number of ideas:

Articulating values and principles that govern technology development and use. Being transparent about decision-making that impacts other stakeholders, known vulnerabilities in software, and data breaches. Governments inviting participation from companies and civil society in discussions on regulation. Making real and visible efforts to obtain consent and protect data, including "security-by-design" and "privacy-by-design" initiatives.<sup>149</sup>

Accepting oversight from a trusted third-party: for the media, this could be an organisation that fact-checks sources; for technology companies, this could be external audits of design, deployment and internal audit processes; for governments, this could be reviews by human rights forums.

Understanding the incentive structures that erode trust, and finding ways to change them: for example, requiring or pressuring social media firms to refuse to run adverts which contain disinformation, de-monetise content that contains disinformation, and clearly label sponsors of political adverts.<sup>150</sup>

Finally, digital cooperation itself can be a source of trust. In the Cold War, small pools of shared interest – non-proliferation or regional stability – allowed competitors to work together and paved the way for transparency and confidence-building measures that helped build a modicum of trust.<sup>151</sup> Analogously, getting multiple stakeholders into a habit of cooperating on issues such as standard-setting and interoperability, addressing risks and social harm and collaborative application of digital technologies to achieve the SDGs, could allow trust to be built up gradually.

### 3.3 Security

Global security and stability are increasingly dependent on digital security and stability. The scope of threats is growing. Cyber capabilities are developing, becoming more targeted, more impactful on physical systems and more insidious at undermining societal trust.

“Cyber attacks” and “massive data fraud and threat” have ranked for two years in a row among the top five global risks listed by the World Economic Forum (WEF).<sup>152</sup> More than 80% of the experts consulted in the WEF’s latest annual survey expected the risks of “cyber-attacks: theft of data/money” and “cyber-attacks: disruption of operations and infrastructure” to increase yearly.<sup>153</sup>

Three recent examples illustrate the concern. In 2016, hackers stole \$81 million from the Bangladesh Central Bank by manipulating the SWIFT global payments network.<sup>154</sup> In 2017, malware called “NotPetya” caused widespread havoc – shipping firm Maersk alone lost an estimated \$250 million.<sup>155</sup> In 2018, by one estimate, cybercriminals stole \$1.5 trillion – an amount comparable to the national income of Spain.<sup>156</sup>

Accurate figures are hard to come by as victims may prefer to keep quiet. But often it is only publicity about a major incident that prompts the necessary investments in security. Short-term incentives generally prioritise launching new products over making systems more robust.<sup>157</sup>

The range of targets for cyber-attacks is increasing quickly. New internet users typically have low awareness of digital hygiene.<sup>158</sup> Already over half of attacks are directed at “things” on the Internet of Things, which connects everything from smart TVs to baby monitors to thermostats.<sup>159</sup> Fast 5G networks will further integrate the internet with physical infrastructure, likely creating new vulnerabilities.<sup>160</sup>

The potential for cyber-attacks to take down critical infrastructure has been clear since Stuxnet was found to have penetrated an Iranian nuclear facility in 2010.<sup>161</sup> More recently concerns have widened to the potential risks and impact of misinformation campaigns and online efforts by foreign

governments to influence democratic elections, including the 2016 Brexit vote and the American presidential election.<sup>162</sup>

Compared to physical attacks, it can be much harder to prove from which jurisdiction a cyber-attack originated. This makes it difficult to attribute responsibility or use mechanisms to cooperate on law enforcement.<sup>163</sup>

Perceptions of digital vulnerability and unfair cyber advantage are contributing to trade, investment and strategic tensions.<sup>164</sup> Numerous countries have set up cyber commands within their militaries.<sup>165</sup> Nearly 60 states are known to be pursuing offensive capabilities.<sup>166</sup> This increases the risks for all as cyber weapons, once released, can be used to attack others – including the original developer of the weapon.<sup>167</sup>

As artificial intelligence advances, the tactics and tools of cyber-attacks will become more sophisticated and difficult to predict – including more able to pursue highly customised objectives, and to adapt in real time.<sup>168</sup>

Many governments and companies are aware of the need to strengthen digital cooperation by agreeing on and implementing international norms for responsible behaviour, and important progress has been made especially in meetings of groups of governmental experts at the UN.<sup>169</sup>

The UN Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security have been set up by resolutions of the UN General Assembly at regular intervals since 1998. Decisions by the GGE are made on the basis of consensus, including the decision on the final report.<sup>170</sup> The 2013 GGE on Developments in the Field of Information and Telecommunications in the Context of International Security agreed in its report that international law applies to cyberspace (see text box).<sup>171</sup> This view was reaffirmed by the subsequent 2015 GGE, which also proposed eleven voluntary and non-binding norms for states.<sup>172</sup> The UN General Assembly welcomed the 2015 report and called on member states to be guided by it in their use of information and communications technologies. This marks an important step forward in building cooperation and agreement in this increasingly salient arena.

#### **Other existing initiatives on digital security**

**The Paris Call for Trust and Security in Cyberspace** is a multi-stakeholder initiative launched in November 2018 and joined by 65 countries, 334 companies – including Microsoft, Facebook, Google and IBM – and 138 universities and non-profit organisations. It calls for measures including coordinated disclosure of technical vulnerabilities. Many leading technology powers, such as the USA, Russia, China, Israel and India – have not signed up.<sup>173</sup>

**The Global Commission on Stability in Cyberspace**, an independent multi-stakeholder platform, is developing proposals for norms and policies to enhance international security and stability in cyberspace. The commission has introduced a series of norms, including calls for agreement not to attack critical infrastructure and non-interference in elections, and is currently discussing accountability and the future of cybersecurity.

**The Global Conference on Cyberspace**, also known as the 'London Process', are *ad hoc* multi-stakeholder conferences held so far in London (2011), Budapest (2012), Seoul (2013), The Hague (2015) and New Delhi (2017). The Global Forum on Cyber Expertise, established after the 2015 Conference, is a platform for identifying best practices and providing support to

states, the private sector and organisations in developing cybersecurity frameworks, policies and skills.

**The Geneva Dialogue on Responsible Behaviour in Cyberspace** provides another forum for multi-stakeholder consultation.

**The Cybersecurity Tech Accord** and the **Charter of Trust** are examples of industry-led voluntary initiatives to identify guiding principles for trust and security, strengthen security of supply chains and improve training of employees in cybersecurity.<sup>174</sup>

### ***Digital cooperation on cybersecurity***

The pace of cyber-attacks is quickening. Currently fragmented efforts need rapidly to coalesce into a comprehensive set of common principles to align action and facilitate cooperation that raises the costs for malicious actors.<sup>175</sup>

Private sector involvement is especially important to evolving a common approach to tracing cyber-attacks: assessing evidence, context, attenuating circumstances and damage. We are encouraged that the 2019 UN GGE<sup>176</sup> and the new Open-Ended Working Group (OEWG)<sup>177</sup> which deal with behaviour of states and international law, while primarily a forum for inter-governmental consultations, do provide for consultations with stakeholders other than governments, mainly regional organisations.

In our Recommendation 4, we call for a multi-stakeholder Global Commitment on Digital Trust and Security to bolster these existing efforts. It could provide support in the implementation of agreed norms, rules and principles of responsible behaviour and present a shared vision on digital trust and security. It could also propose priorities for further action on capacity development for governments and other stakeholders and international cooperation.

The Global Commitment should coordinate with ongoing and emerging efforts to implement norms in practice by assisting victims of cyber-attacks and assessing impact. It may not yet be feasible to envisage a single global forum to house such capabilities, but there would be value in strengthening cooperation among existing initiatives.

Another priority should be to deepen cooperation and information sharing among the experts who comprise national governments' Computer Emergency Response Teams (CERTs). Examples to build on here include the Oman-ITU Arab Regional Cybersecurity Centre for 22 Arab League countries,<sup>178</sup> the EU's Computer Security Incident Response Team (CSIRT)s Network,<sup>179</sup> and Israel's Cyber Net, in which public and private teams work together. Collaborative platforms hosted by neutral third parties such as the Forum of Incident Response and Security Teams (FIRST) can help build trust and the exchange of best practices and tools.

Digital cooperation among the private sector, governments and international organisations should seek to improve transparency and quality in the development of software, components and devices.<sup>180</sup> While many best practices and standards exist, they often address only narrow parts of a vast and diverse universe that ranges from talking toys to industrial control systems.<sup>181</sup> Gaps exist in awareness and application. Beyond encouraging a broader focus on security among developers, digital cooperation should address the critical need to train more experts specifically in cybersecurity:<sup>182</sup> by one estimate, the shortfall will be 3.5 million by 2021.<sup>183</sup>

## 4. Mechanisms for Global Digital Cooperation

No single approach to digital cooperation can address the diverse spectrum of issues raised in this report – and as technologies evolve, so will the issues, and the most effective ways to cooperate. We should approach digital cooperation using all available tools, making dynamic choices about the best approach based on specific circumstances. In some cases, cooperation may be initiated and led by the private sector or civil society, and in some cases by governments or international organisations.<sup>184</sup>

Most current mechanisms of digital cooperation are primarily local, national or regional. However, digital interdependence also necessitates that we strengthen global digital cooperation mechanisms to address challenges and provide opportunities for all.

This chapter identifies gaps and challenges in current arrangements for global digital cooperation and summarises the functions any future cooperation architecture could perform and what principles could underpin them. It then outlines three possible options for digital cooperation architectures and concludes with a discussion of the role the United Nations can play. There was not unanimity of opinion among the Panel members about the shape, function and operations of these different models. Instead, they are presented as useful alternatives to explore in the spirit of digital cooperation and as an input for the broad consultations we call for in Recommendation 5A.

Ultimately, success of any proposed mechanisms and architecture will depend on the spirit in which they are developed and implemented. All governments, the private sector and civil society organisations need to recognise how much they stand to gain from a spirit of collaboration to drive progress toward the achievement of the SDGs and to raise the costs of using digital technologies irresponsibly. The alternative is further erosion of the trust and stability we need to build an inclusive and prosperous digital future.

### 4.1 Challenges and gaps

The international community is not starting from scratch. It can build on established mechanisms for digital cooperation involving governments, technical bodies, civil society and other organisations. Some are based in national and international law,<sup>185</sup> others in “soft law” – norms, guidelines, codes of conduct and other self-regulatory measures adopted by business and tech communities.<sup>186</sup> Some are loosely organised, others highly institutionalised.<sup>187</sup> Some focus on setting agendas and standards, others on monitoring and coordination.<sup>188</sup> Many could evolve to become better fit for purpose.

The need for better digital cooperation is not so much with managing the technical nuts and bolts of how technologies function, as mechanisms here are generally well-established, but with the unprecedented economic, societal and ethical challenges they cause. How to tell, in context, when conversations on social media cross the line into inciting violence? How to limit the use of cyber weapons possessed not only by states but non-state actors and individuals?<sup>189</sup> How to adapt trade systems designed for a different era to the newly emerging forms of online commerce?

The 2003 and 2005 World Summit on the Information Society (WSIS) established the Internet Governance Forum (IGF) as a platform for multi-stakeholder dialogue.<sup>190</sup> Global, national and regional IGF meetings have contributed to many important digital debates. But the IGF, in its



current form, has limitations in addressing challenges that are now emerging from new digital technologies.

The need for strengthened cooperation mechanisms has been raised many times in recent years by broad initiatives – such as the NetMundial Conference,<sup>191</sup> the Global Commission on Internet Governance<sup>192</sup> and Web Foundation’s Contract for the Web<sup>193</sup> – and more narrowly focused efforts such as the Broadband Commission, the Alliance for Affordable Internet, the Internet & Jurisdiction Policy Network, the Global Commission on the Stability of Cyberspace, the Charter of Trust, Smart Africa, and the International Panel on AI recently announced by Canada and France.<sup>194</sup>

In our consultations, we heard a great deal of dissatisfaction with existing digital cooperation arrangements: a desire for more tangible outcomes, more active participation by governments and the private sector, more inclusive processes and better follow-up. Overall, systems need to become more holistic, multi-disciplinary, multi-stakeholder, agile and able to convert rhetoric into practice. We have identified six main gaps:

*First*, despite their growing impact on society, digital technology and digital cooperation issues remain relatively low on many national, regional and global political agendas. Only recently have forums such as the G20 started regularly to address the digital economy.<sup>195</sup> In 2018, the UN Secretary-General for the first time delivered an opening statement in person at the IGF in Paris.<sup>196</sup>

*Second*, digital cooperation arrangements such as technical bodies and standard-setting organisations are often not inclusive enough of small and developing countries, indigenous communities, women, young and elderly people and those with disabilities. Even if they are invited to the table, such groups may lack the capacity to participate effectively and meaningfully.<sup>197</sup>

*Third*, there is considerable overlap among the large number of mechanisms covering digital policy issues. As a result, the digital cooperation architecture has become highly complex but not necessarily effective. There is no simple entry point. This makes it especially hard for small enterprises, marginalised groups, developing countries and other stakeholders with limited budgets and expertise to make their voices heard.<sup>198</sup>

*Fourth*, digital technologies increasingly cut across areas in which policies are shaped by separate institutions. For example, one body may look at data issues from the perspective of standardisation, while another considers trade, and still another regulates to protect human rights.<sup>199</sup> Many international organisations are trying to adjust their traditional policy work to reflect the realities of the digital transformation, but do not yet have enough expertise and experience to have well-defined roles in addressing new digital issues. At a minimum there needs to be better communication across different bodies to shape awareness. Ideally, effective cooperation should create synergies.

*Fifth*, there is a lack of reliable data, metrics and evidence on which to base practical policy interventions. For example, the annual cost of cybercrime to the global economy is variously estimated at anything from \$600 billion<sup>200</sup> to \$6 trillion.<sup>201</sup> Estimates of the value of the AI market in 2025 range from \$60 billion<sup>202</sup> to \$17 trillion.<sup>203</sup> The problem is most acute in developing countries, where resources to collect evidence are scarce and data collection is generally uneven. Establishing a knowledge repository on digital policy, with definitions of terms and concepts, would also increase clarity in policy discussions and support consistency of measurement of digital inclusion, as we have noted in our Recommendation 1D.

*Sixth*, lack of trust among governments, civil society and the private sector – and sometimes a lack of humility and understanding of different perspectives – can make it more difficult to establish the collaborative multi-stakeholder approach needed to develop effective cooperation mechanisms.

Inter-governmental work must be balanced with work involving broader stakeholders. Multi-stakeholder and multilateral approaches can and do co-exist. The challenge is to evolve ways of using each to reinforce the effectiveness of the other.

### **Values and principles**

As noted in the discussion of values in Chapter 1, we believe global digital cooperation should be: *inclusive; respectful; human-centred; conducive to human flourishing; transparent; collaborative; accessible; sustainable and harmonious*. Shared values become even more important during periods of rapid change, limited information and unpredictability, as with current discussions of cooperation relating to artificial intelligence.

It would be useful for the private sector, communities and governments to conduct digital cooperation initiatives by explicitly defining the values and principles that guide them. The aim is to align stakeholders around a common vision, maximise the beneficial impacts and minimise the risk of misuse and unintended consequences.

Alongside these shared values, we believe it is useful to highlight operational principles as a reference point for the future evolution of digital cooperation mechanisms. The principles we propose for global digital cooperation mechanisms include that they should: be easy to engage in, open and transparent; inclusive and accountable to all stakeholders; consult and debate as locally as possible; encourage innovation of both technologies and better mechanisms for cooperating; and, seek to maximise the global public interest. These are set forth in more detail in Annex VI, based on the experience of internet governance and technical coordination bodies – such as the WSIS process, UNESCO and the NetMundial conference.<sup>204</sup>

Defining values and principles is only the first step: we must operationalise them in practice in the design and development of digital technology and digital cooperation mechanisms. Where the reach of hard governance is limited or ambiguous – for example, at the stage of innovation or when the long-term impact of technologies is hard to predict – values-based cooperation approaches can play a vital role.

We should look for opportunities to operationalise values and principles at each step in the design and development of new technologies, as well as new policy practices. For example, educational institutions could encourage software developers, business executives and engineers to integrate values and principles in their work and use professional codes of conduct akin to the medical profession's Hippocratic Oath. Businesses can integrate values into workflows, use values-based measures to assess risk and institute a suitable incentive structure for staff to follow shared values. Self-assessments and third-party audits can also help institutionalise a business culture based on shared values.

## **4.2 Three possible architectures for global digital cooperation**

The Panel had many discussions about possible practical next steps to improve the architecture of global digital cooperation and the merits of proposing new mechanisms or updating existing

ones. Some suggested that many cooperation challenges could be best addressed by strengthening implementation capacities of current agencies and mandates.

While no single vision emerged, there was broad agreement that improved cooperation is needed, that such cooperation will need to take multiple diverse forms, and that governments, the private sector and civil society will need to find new ways to work together to steer an effective path between extremes of over-regulation and complete laissez-faire. Based on our consultations, the Panel felt that presenting options for digital cooperation architectures would best contribute to the discourse on global digital cooperation.

Annex VI sets out functions that a digital cooperation architecture could be designed to improve. These include generating political will, ensuring the active and meaningful participation of all stakeholders, monitoring developments and identifying trends, creating shared understanding and purpose, preventing and resolving disputes, building consensus and following up on agreements.

Below three possible models are proposed that could address some of these functions. The first enhances and extends the multi-stakeholder IGF. The second is a distributed architecture which builds on existing mechanisms. The third envisions a ‘commons’ approach with loose coordination by the UN. All have benefits and drawbacks. They are put forward here to provide concrete starting points for the further discussion and broad consultation which we recommend the UN Secretary-General initiate in our Recommendation 5A.

#### **A note on inclusive representation**

All three models highlighted below would need to take special steps to ensure that they are broadly representative and develop specific mechanisms to ensure equitable participation of developing countries, women and other traditionally marginalised groups who have often been denied a voice.

#### **“Internet Governance Forum Plus”<sup>205</sup>**

The proposed Internet Governance Forum Plus, or IGF Plus, would build on the existing IGF which was established by the World Summit on Information Society (Tunis, 2005). The IGF is currently the main global space convened by the UN for addressing internet governance and digital policy issues. The IGF Plus concept would provide additional multi-stakeholder and multilateral legitimacy by being open to all stakeholders and by being institutionally anchored in the UN system.

The IGF Plus would aim to build on the IGF’s strengths, including well-developed infrastructure and procedures, acceptance in stakeholder communities, gender balance in IGF bodies and activities, and a network of 114 national, regional and youth IGFs.<sup>206</sup> It would add important capacity strengthening and other support activities.

The IGF Plus model aims to address the IGF’s current shortcomings. For example, the lack of actionable outcomes can be addressed by working on policies and norms of direct interest to stakeholder communities. The limited participation of government and business representatives, especially from small and developing countries, can be addressed by introducing discussion tracks in which governments, the private sector and civil society address their specific concerns.

The IGF Plus would comprise an Advisory Group, Cooperation Accelerator, Policy Incubator and Observatory and Help Desk.

**The Advisory Group**, based on the IGF's current Multi-stakeholder Advisory Group, would be responsible for preparing annual meetings, and identifying focus policy issues each year. This would not exclude coverage of other issues but ensure a critical mass of discussion on the selected issues. The Advisory Group could identify moments when emerging discussions in other forums need to be connected, and issues that are not covered by existing organisations or mechanisms.

Building on the current practices of the IGF, the Advisory Group could consist of members appointed for three years by the UN Secretary-General on the advice of member states and stakeholder groups, ensuring gender, age, stakeholder and geographical balance.

**The Cooperation Accelerator** would accelerate issue-centred cooperation across a wide range of institutions, organisations and processes; identify points of convergence among existing IGF coalitions, and issues around which new coalitions need to be established; convene stakeholder-specific coalitions to address the concerns of groups such as governments, businesses, civil society, parliamentarians, elderly people, young people, philanthropy, the media, and women; and facilitate convergences among debates in major digital and policy events at the UN and beyond.

The Cooperation Accelerator could consist of members selected for their multi-disciplinary experience and expertise. Membership would include civil society, businesses and governments and representation from major digital events such as the Web Summit, Mobile World Congress, Lift:Lab, Shift, LaWeb, and Telecom World.

**The Policy Incubator** would incubate policies and norms for public discussion and adoption. In response to requests to look at a perceived regulatory gap, it would examine if existing norms and regulations could fill the gap and, if not, form a policy group consisting of interested stakeholders to make proposals to governments and other decision-making bodies. It would monitor policies and norms through feedback from the bodies that adopt and implement them.<sup>207</sup>

The Policy Incubator could provide the currently missing link between dialogue platforms identifying regulatory gaps and existing decision-making bodies by maintaining momentum in discussions without making legally binding decisions. It should have a flexible and dynamic composition involving all stakeholders concerned by a specific policy issue.

**The Observatory and Help Desk** would direct requests for help on digital policy (such as dealing with crisis situations, drafting legislation, or advising on policy) to appropriate entities, including the Help Desks described in Recommendation 2; coordinate capacity development activities provided by other organisations; collect and share best practices; and provide an overview of digital policy issues, including monitoring trends, identifying emerging issues and providing data on digital policy.

**The IGF Trust Fund** would be a dedicated fund for the IGF Plus. All stakeholders – including governments, international organisations, businesses and the tech sector – would be encouraged to contribute. The IGF Plus Secretariat should be linked to the Office of the United Nations Secretary-General to reflect its interdisciplinary and system-wide approach.

#### **“Distributed Co-Governance Architecture”**

The proposed distributed co-governance architecture (COGOV) would build on existing mechanisms while filling gaps with new mechanisms to achieve a distributed, yet cohesive digital

cooperation architecture covering all stages from norm design to implementation and potential enforcement of such norms by the appropriate authorities.

COGOV relies on the self-forming 'horizontal' network approach used by the Internet Engineering Task Force, the Internet Corporation for Assigned Names and Numbers (ICANN), the World Wide Web Consortium, the Regional Internet Registries, the IEEE and others to host networks to design norms and policies. This proposal would extend this agile network approach to issues affecting the broader digital economy and society.

Given the wide range of issues which the COGOV architecture could encompass, it will be imperative to ensure there is broad representation beyond the relatively homogenous expert communities which predominate for some of the technical issues discussed above.

The COGOV architecture decouples the design of digital norms from their implementation and enforcement. It seeks to rapidly produce shared digital cooperation solutions, including norms, and publish them for stakeholders to consider and potentially adopt. These norms would be voluntary solutions rather than legal instruments. In themselves, the COGOV networks would not have governing authority or enforcement powers. However, the norms could be taken up by government agencies as useful blueprints to establish policies, regulations or laws.

The COGOV could consist of three functional elements: a) Digital Cooperation Networks; b) Network Support Platforms; and, c) a Network of Networks.

**a) Digital Cooperation Networks.** These networks would be issue-specific *horizontal* collaboration groups, involving stakeholders from relevant *vertical* sectors and institutions. They could be formed freely by stakeholders in a bottom-up way, self-governed, and share the same goal of cooperation – including potentially the design of digital norms. They could be created or supported by one or more governments and/or intergovernmental organisations with the same concerns. Their functions would include developing shared understandings and goals for a specific digital issue, strengthening cooperation, designing or updating digital norms, providing norm implementation roadmaps and developing capacity to adopt policies and norms.

Participation in digital cooperation networks should be open for all relevant and concerned stakeholders, including governments, intergovernmental institutions, the private sector, civil society, academia and the technical community. Special efforts would need to be made to include and support representatives from developing countries and traditionally marginalised groups. The digital cooperation networks may be stand-alone voluntary networks or hosted by the network support platforms described below.

**b) Network Support Platforms.** These platforms could host and enable the dynamic formation and functioning of multiple digital cooperation networks. While the digital cooperation networks would operate in defined and limited timeframes, the network support platforms are proposed as stable long-term elements of the architecture, supporting the digital cooperation networks and enabling them to evolve as necessary to update their cooperation and relevant digital norms.

The network support platforms should not interfere in the work product or composition of the self-governed and stakeholder-initiated digital cooperation networks; they should simply support the networks to operate efficiently. The platforms would help the networks to identify emerging issues, secure the commitment of relevant participants, provide necessary resources and facilities, and promote their outcomes.

**c) Network of Networks.** The network of networks would loosely coordinate and support activities across all digital cooperation networks and network support platforms. The role of the network of networks is to ensure integrity and enable coherent outcomes that account for the complex interdependencies across digital policy issues.

The network of networks would consist of: 1) a support function, which would organise an annual forum, a ‘research cooperative’ and a ‘norm exchange’; and 2) a voluntary peer coordination network, which would bring issues to the attention of the annual forum and follow up on its recommendations by promoting action from specific stakeholders to form digital cooperation networks.

The network of networks should avoid a controlling top-down form of administration: it is simply there to loosely coordinate the activities across the decentralized COGOV architecture; its decisions would not be binding.

Once norms are available, governing authorities may choose to establish enforcement mechanisms and may choose to use these norms as policy input or blueprints. The following table summarises the mechanisms across the norm design, implementation, and enforcement stages:

<b>Norm Design</b>	<b>Norm Implementation</b>	<b>Norm Enforcement</b>
Identify digital governance issues	Develop norm design and adoption capacity	Develop norms into laws/regulations
Form digital cooperation networks	Provide a ‘norm exchange’ to connect communities	Adjudicate/resolve disputes and conflicts
Support networks through digital cooperation platforms	Offer implementation incentives	Establish clear guard rails for digital technologies

### “Digital Commons Architecture”

In areas such as space, climate change and the sea, the international community has entered into treaties and developed principles, norms and functional cooperation to designate certain spaces as international ‘commons’ and then govern ongoing practice and dialogue.<sup>208</sup> For instance, the “common heritage” principle, introduced by the United Nations Convention on the Law of the Sea, imposes a duty to protect resources for the good of future generations.<sup>209</sup>

While norm-making and guidance in digital technologies will pose different challenges, some aspects of the digital realm, such as common internet protocols, already share characteristics with ‘commons’ requiring responsible and global stewardship. ‘Digital commons’ have also been mentioned recently in the context of data and AI developments.<sup>210</sup>

The proposed “Digital Commons Architecture” would aim to synergise efforts by governments, civil society and businesses to ensure that digital technologies promote the SDGs and to address risks of social harm. It would comprise multi-stakeholder tracks to create dialogue around emerging issues and communicate use cases and problems to be solved to stakeholders, and an annual meeting to act as a clearing house.

Each track could be owned by a lead organisation – a UN agency, an industry or academic consortium or a multi-stakeholder forum, with the choice of participants governed by guiding

principles of the kind listed in this report to ensure inclusiveness and broad representation. Light coordination of the tracks, and servicing of the annual meeting where their reports are considered, could be ensured by a small secretariat housed within the UN.

Analogous to processes such as the International Competition Network, the Digital Commons Architecture tracks would have flexible, project-oriented and results-based working groups. They would enable learning on governance and related capacity development to be driven by practice. Annual meetings could aggregate lessons for use in soft law or more binding approaches in the appropriate forums. This could rapidly build a repository of norms and governance practices to guide stakeholders in their respective roles and responsibilities.

The Digital Commons Architecture tracks could focus on issues agreed by the participants. For example, they might initially wish to address issues emerging from the preceding chapters, such as using data in support of the SDGs, using AI to improve agriculture and health, or developing a global values/ethics certification process for new technology.

Multi-stakeholder collaboration around these issues could pave the way for wider cooperation. For example, realising the potential of AI to provide insights to a global health challenge might require the pooling of reliable data, clear privacy measures, a common data architecture and interoperable standards. Successful outcomes could then be progressively extended to other areas. An additional benefit would be to promote transparency and build confidence.

The annual meeting would not make rules, but provide guidance to stakeholders, which they can use in the appropriate forums. The meeting would discuss the output of the various tracks as well as implementation of the governance guidance produced by these tracks through a 'soft' review of reports by stakeholders.

The Digital Commons Architecture might not specify technical solutions, but instead propose technical models, and standards of accountability and trustworthiness, which could be applied across the globe. It could also facilitate a discussion of lessons from around the globe on implementation of existing norms in specific areas.

The annual meeting could build on and connect discussions taking place in other fora and could in turn feed its results into discussions taking place in other fora. This would reduce the current burden of multiplicity of forums by clarifying who is doing what, eliminating potential overlap, and identifying partnership opportunities.

The Digital Commons Architecture could be funded through voluntary contributions. Along the lines of the International Chamber of Commerce, membership fees could be considered for private sector participation; these could be waived for certain categories such as small businesses or civil society participants.<sup>211</sup> A dedicated trust fund could assist with civil society and least developed country participation.

The three potential models share common elements, such as multi-stakeholder participation, dedicated trust funds to enhance inclusivity, reducing policy inflation by consolidating discussions across for a, and a light coordination and convening role for the UN. The values in Chapter 1 and principles and functions in Annex VI provide shared design elements that further emphasise inclusivity and multi-stakeholder participation.

Equally, there are differences in emphasis and approach. The COGOV, for example, foresees a larger role for new networks of experts and multi-stakeholder governance; the Digital Commons Architecture presumes more of a focus on iterative learning of governance through practice in both multilateral and multi-stakeholder tracks; and the IGF Plus adds functionalities to an existing multi-stakeholder forum with a UN mandate.

The common design elements across the models could be flexibly brought together once the broad thrust of a new digital cooperation architecture has been defined. As suggested in Recommendation 5A, a common starting point could be a Global Commitment for Digital Cooperation based on shared values and principles.

### 4.3 The role of the UN

The UN's three foundational pillars – peace and security, human rights and development – position it well to help spotlight issues emerging in the digital age and advocate on behalf of humanity's best interests. In our consultations, we heard that despite its well-known weaknesses, the UN retains a unique role and convening power to bring stakeholders together to create the norms and frameworks and assist in developing the capacity we need to ensure a safe and equitable digital future for all people.

Digital technologies are increasingly impacting the work of the UN in three ways: changing the political, social and economic environment in the ways this report has discussed; providing new tools for its core mandates; and creating new policy issues.

UN entities have begun to embrace the digital transformation and are revamping programmes and launching initiatives to apply digital technology to further their missions. Some UN agencies – such as UNICEF, UNESCO, the World Food Programme (WFP) and the United Nations Development Programme (UNDP) – have made a priority of exploring how the digital transformation can provide them with new approaches to achieve their mandates. The Task Force on Digital Financing of the SDGs, for example, will explore how digital technologies can be leveraged to finance the SDGs.<sup>212</sup>

When digital issues often do not fit neatly within the traditional mandates of UN agencies, some have sought to expand their mandates, causing overlaps and friction. This duplication also causes confusion for external partners and stakeholders, who find it difficult to discern among the many fora, events and initiatives hosted by various parts of the UN on science, technology and innovation issues and policy setting. Some UN entities have responded to converging mandates by launching cross-cutting initiatives. For example, in 2010 the ITU and UNESCO established the Broadband Commission for Sustainable Development; in 2016 the ITU, UN Women, the International Trade Centre (ITC), the GSM Association (GSMA), UNESCO and the United Nations University set up the EQUALS partnership to tackle the digital gender gap.

UN entities have also tended to go about digital issues in their own way, often without sharing information, at times duplicating each other's work, and not reflecting on whether the systems they are building might scale to other UN entities. UN agencies can do much more to pool their human and computing capacities and develop shared tools and common standards – for example, through joint procurement of cloud computing, to reduce price and increase interoperability, and promoting open and interoperable standards for data produced and used by the UN.

The UN has begun to engage the private sector and tech community much more directly. For example, Tech Against Terrorism, a public/private partnership launched in April 2017 by the



Counter-Terrorism Committee Executive Directorate, aims to support the technology industry to develop more effective and responsible approaches to tackling terrorists' use of the internet, while respecting human rights. However, working with stakeholders such as the private sector and civil society is still not part of the DNA of many UN agencies. More can be done to partner with other stakeholders effectively and consistently.

Created by the innovation units of several UN agencies in 2015, the UN Innovation Network is working on sharing best practices and recommending harmonisation of policies which may help reduce fragmentation across the UN system. The UN's highest-level coordination body, the Chief Executives Board for Coordination, is trying to encourage more system-wide coordination through initiatives such as the UN Data Innovation Lab and UN data privacy principles. The High-level Committee on Programmes could also have a role to enable more knowledge sharing, efficiencies of scale and scaling up of successful practices and initiatives across the UN system.

The development of the UN Secretary-General's Strategy on New Technologies, issued in September 2018, has helped identify points of overlap and convergence, and UN agencies meet regularly to track progress. The strategy notes that the Secretary-General may consider appointing a "Tech Envoy" following the work of this Panel.

The UN can play a key role in enhancing digital cooperation by developing greater organisational and human capacity on digital governance issues and improving its ability to respond to member states' need for policy advice and capacity development.

#### **How can the UN add value in the digital transformation?**

**As a convener** – The AI for Global Good Summit, the Broadband Commission for Sustainable Development, ITU's Global Symposium for Regulators, the WSIS Forum, the Multi-stakeholder Forum on Science, Technology and Innovation for the Sustainable Development Goals (STI Forum).

**Providing a space for debating values and norms** – the IGF, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Special Rapporteurs on the Right to Privacy and on the promotion and protection of the Right to Freedom of Opinion and Expression, UNESCO's Artificial Intelligence with Human Values for Sustainable Development initiative, UNICEF's efforts around children's online safety.

**Standard setting** – ITU's Telecommunication Standardization Sector, the UN Statistical Commission and its Global Working Group on Big Data for Official Statistics, WHO guidelines on digital health interventions, the Humanitarian Data Exchange – an open platform and standard for sharing data across crises and organisations.

**Multi-stakeholder or bilateral initiatives on specific issues** – EQUALS: The Global Partnership for Gender Equality in the Digital Age, the Emergency Telecommunications Cluster hosted by WFP, the UN Global Compact's Breakthrough Innovation for the SDGs Action Platform, the Famine Action Mechanism hosted by the World Bank and the UN in partnership with industry.

**Developing the capacity of member states** – UNDP's Accelerator Labs, the Technology Facilitation Mechanism, UN Global Pulse Labs, the United Nations Conference on Trade and Development's trainings, the Digital Blue Helmets initiative, the UN Office on Drugs and Crime's Global Programme on Cybercrime.

**Ranking, mapping and measuring** – the annual *E-Government Survey* produced by the United Nations Department of Economic and Social Affairs, the United Nations Institute for Disarmament Research's Cyber Policy Portal, an online reference tool that maps the cybersecurity and cybersecurity-related policy landscape, ITU's *Measuring the Information Society* report and *Global Cybersecurity Index*.

**Arbitration and dispute-resolution** – The World Intellectual Property Organization's Internet Domain Name Process, the United Nations Commission on International Trade Law.

## 5. Recommendations

The preceding chapters of this report have shown that our rapidly changing and interdependent digital world urgently needs improved digital cooperation founded on common human values. Based on our analysis and consultations with diverse stakeholders, and noting that not all Panel members were supportive of all recommendations, we make the following recommendations:

### An inclusive digital economy and society

**1A:** *We recommend that by 2030, every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to achieving the SDGs. Provision of these services should guard against abuse by building on emerging principles and best practices, one example of which is providing the ability to opt in and opt out, and by encouraging informed public discourse.*

**1B:** *We recommend that a broad, multi-stakeholder alliance, involving the UN, create a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs.*

**1C:** *We call on the private sector, civil society, national governments, multilateral banks and the UN to adopt specific policies to support full digital inclusion and digital equality for women and traditionally marginalised groups. International organisations such as the World Bank and the UN should strengthen research and promote action on barriers women and marginalised groups face to digital inclusion and digital equality.*

**1D:** *We believe that a set of metrics for digital inclusiveness should be urgently agreed, measured worldwide and detailed with sex disaggregated data in the annual reports of institutions such as the UN, the International Monetary Fund, the World Bank, other multilateral development banks and the OECD. From this, strategies and plans of action could be developed.*

In this report we have emphasised that the role of digital technologies in achieving the Sustainable Development Goals goes far beyond simply promoting greater access to the internet. With the right blend of policy, investment in infrastructure and human capacity, and cooperation among stakeholders, they can revolutionise fields as diverse as health and education, governance, economic empowerment and enterprise, agriculture and environmental sustainability.

The specific decisions needed to promote inclusivity and minimise risks will depend on local and national conditions. They should consider four main factors.

*First*, the broader national policy and regulatory frameworks should make it easy to create, run and grow small businesses. These frameworks should ensure that digital service providers – including e-commerce and inclusive finance platforms – support the growth of local enterprises. This requires enabling policies on investment and innovation, and structural policies to ensure fair competition, privacy rights, consumer protection and a sustainable tax base. Efforts to agree regional or global standards in these areas are welcome.

*Second*, investments should be made in both human capacity (see Recommendation 2 below) and physical infrastructure. Creating the foundation of universal, affordable access to electricity and

the internet will often require innovative approaches, such as community groups operating rural networks, or incentives such as public sector support.

*Third*, targeted measures should address the barriers faced by women, indigenous people, rural populations and others who are marginalised by factors such as a lack of legal identity, low literacy rates, social norms that prevent them from fully participating in civic and economic life, and discriminatory land ownership, tenure and inheritance practices.

*Fourth*, respect for human rights – including privacy – is fundamental. Panel members had divergent views on digital ID systems in particular: they have immense potential to improve delivery of social services, especially for people who currently lack legal identity, but they are also vulnerable to abuse. As digital ID becomes more prevalent, we must emphasise principles for its fair and effective use.

Achieving this ambition will require multi-stakeholder alliances involving governments, private sector, international organisations, citizen groups and philanthropy to build new models of collaboration around “digital public goods” and data sets that can be pooled for the common good. SDG-related areas include health, energy, agriculture, clean water, oceans and climate change. These alliances could establish minimum criteria for classifying technologies and content as “digital public goods” and connect with relevant communities of practice that can provide guidance and support for investment, implementation and capacity development.

We are concerned that women face particular challenges in meaningfully accessing the internet, inclusive mobile financial services and online commerce, and controlling their own digital IDs and health records. Policies should include targeted capacity development for female entrepreneurs and policy makers. We call on the technology sector to make more sustained and serious efforts to address the gap in female technology employees and management, include women’s voices when determining online terms and conditions, and act to prevent online harassment and promotion of domestic abuse, building upon the work of existing initiatives such as the High-level Panel on Women’s Economic Empowerment.

While some preliminary work is underway, there is currently no agreed set of clear metrics or standards for the inclusiveness of digital technologies and cooperation. While any metrics will evolve over time, we call for research and multi-stakeholder consultation to establish a basis of shared global understanding as promptly as possible. We encourage the UN, international development agencies and multilateral banks such as the Asian Development Bank, the New Development Bank and the World Bank to drive this process by incorporating digital inclusion as a key metric in approving and evaluating projects. Facets of digital inclusion which may be considered include gender, financial services, health, government services, national digital economy policies, use of online e-commerce platforms and mobile device penetration.

### **Human and institutional capacity**

**2: *We recommend the establishment of regional and global digital help desks to help governments, civil society and the private sector to understand digital issues and develop capacity to steer cooperation related to social and economic impacts of digital technologies.***

Many countries urgently need to make critical choices about the complex issues discussed in this report. In what types of infrastructure should they invest? What types of training do their

populations require to compete in the global digital economy? How can those whose livelihoods are disrupted by technological change be protected? How can technology be used to deliver social services and improve governance? How can regulation be appropriately balanced to encourage innovation while protecting human rights?

Policy decisions will have profound impact, but many of the decision-makers lack sufficient understanding of digital technologies and their implications. Capacity development for government officials and regulators could help to harness technology for inclusive economic development to achieve the SDGs. Priorities could include diagnostics on digital capacities and how they interact with society and the economy, and identifying skills workers will need. Capacity development initiatives with the private sector would also develop the capacity of officials and regulators to engage with the private sector so they can understand the operations of the digital economy and respond in an agile way to emerging issues (see Recommendation 5B).

For decisions to be well informed and inclusive, all stakeholders and the public need also to better understand the benefits and risks of digital technologies. Decisions around technology should be underpinned by a broad social dialogue on its costs, benefits and norms. We encourage capacity development programs for governments, civil society organisations, the private sector – including small- and medium-sized enterprises and start-ups – consumers, educators, women and youth. Existing capacity development initiatives by civil society, academia and technical and international organisations could benefit from the promotion of best practices.

A regional approach is recommended to develop capacity, to enable differing local contexts to be addressed. Regional help desks could be led by organisations such as the African Union or the Association of Southeast Asian Nations, in collaboration with UN Regional Commissions. The regional help desks would: conduct research and promote best practice in digital cooperation; provide capacity development training and recommend open-source or licensed products and platforms; and support requests for advice from governments, local private sector (particularly small and medium enterprises) and civil society in their regions. Staff would have regional expertise, and coordinate closely with the private sector and civil society.

A global help desk to coordinate the work of regional help desks could form part of the new digital cooperation architecture we recommend exploring in Recommendation 5A.

### **Human rights and human agency**

**3A:** *Given that human rights apply fully in the digital world, we urge the UN Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. Civil society, governments, the private sector and the public should be invited to submit their views on how to apply existing human rights instruments in the digital age in a proactive and transparent process.*

**3B:** *In the face of growing threats to human rights and safety, including those of children, we call on social media enterprises to work with governments, international and local civil society organisations and human rights experts around the world to fully understand and respond to concerns about existing or potential human rights violations.*

**3C:** *We believe that autonomous intelligent systems should be designed in ways that enable their decisions to be explained and humans to be accountable for their use. Audits*

***and certification schemes should monitor compliance of AI systems with engineering and ethical standards, which should be developed using multi-stakeholder and multilateral approaches. Life and death decisions should not be delegated to machines. We call for enhanced digital cooperation with multiple stakeholders to think through the design and application of these standards and principles such as transparency and non-bias in autonomous intelligent systems in different social settings.***

As discussed in Chapter 3, while human rights apply online as well as offline, technology presents challenges that were not foreseen when many foundational human rights accords were created. National laws and regulations must prevent advances in technology being used to erode human rights or avoid accountability. We need to cooperate to ensure that digital technologies advance the inherent dignity and equal and inalienable rights of every human.

Applying human rights in the digital age requires better coordination and communication between governments, technology companies, civil society and other stakeholders. Companies have often reacted slowly and inadequately to learning that their technologies are being deployed in ways that undermine human rights. We need more forward-looking efforts to identify and mitigate risks in advance: companies should consult with governments, civil society and academia to assess the potential human rights impact of the digital technologies they are developing. From risk assessment to ongoing due diligence and responsiveness to sudden events, it should be clarified what society can reasonably expect from each stakeholder, including technology firms.

In some areas there is consensus that much more needs to be done – notably, companies providing social media services need to do more to prevent the dissemination of hatred and incitement of violence, and companies providing online services and apps used by children need to do more to ensure appropriate design and meaningful data consent.

Consensus is also emerging that more needs to be done to safeguard the human right to privacy: individuals often have little or no meaningful understanding of the implications of providing their personal data in return for digital services. We believe companies, governments and civil society should agree to clear and transparent standards that will enable greater interoperability of data in ways that protect privacy while enabling data to flow for commercial, research and government purposes, and supporting innovation to achieve the SDGs. Such standards should prevent data collection going beyond intended use, limit re-identification of individuals via datasets, and give individuals meaningful control over how their personal data is shared.

We also emphasise our belief that autonomous intelligent systems should be designed in ways that enable their decisions to be explained and humans to be held to account for their use. Audits and certification schemes should monitor compliance of AI systems with engineering and ethical standards. Humans should never delegate life and death decisions to machines.

### **Trust, security and stability**

***4. We recommend the development of a Global Commitment on Digital Trust and Security to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.***

As the digital economy increasingly merges with the physical world and deploys autonomous intelligent systems, it depends ever more on trust and the stability of the digital environment. Trust

is built through agreed standards, shared values and best practices. Stability implies a digital environment that is peaceful, secure, open and cooperative. More effective action is needed to prevent trust and stability being eroded by the proliferation of irresponsible use of cyber capabilities.

The Global Commitment on Digital Trust and Security could build on and create momentum behind the voluntary norms agreed in the report of the 2015 GGE, and complement relevant global processes. It could address areas such as ways to strengthen implementation of agreed norms; developing societal capacity for cybersecurity and resilience against misinformation; encouraging companies to strengthen authentication practices, adhere to stricter software development norms and be more transparent in the use of software and components; and improving the digital hygiene of new users coming online.

### **Global digital cooperation**

**5A: We recommend that, as a matter of urgency, the UN Secretary-General facilitate an agile and open consultation process to develop updated mechanisms for global digital cooperation, with the options discussed in Chapter 4 as a starting point. We suggest an initial goal of marking the UN's 75th anniversary in 2020 with a "Global Commitment for Digital Cooperation" to enshrine shared values, principles, understandings and objectives for an improved global digital cooperation architecture. As part of this process, we understand that the UN Secretary-General may appoint a Technology Envoy.**

**5B: We support a multi-stakeholder "systems" approach for cooperation and regulation that is adaptive, agile, inclusive and fit for purpose for the fast-changing digital age.**

Enhancing digital cooperation will require both reinvigorating existing multilateral partnerships and potentially the creation of new mechanisms that involve stakeholders from business, academia, civil society and technical organisations. We should approach questions of governance based on their specific circumstances and choosing among all available tools.

Where possible we can make existing inter-governmental forums and mechanisms fit for the digital age rather than rush to create new mechanisms, though this may involve difficult judgement calls: for example, while the WTO remains a major forum to address issues raised by the rapid growth in cross-border e-commerce, it is now over two decades since it was last able to broker an agreement on the subject.

Given the speed of change, soft governance mechanisms – values and principles, standards and certification processes – should not wait for agreement on binding solutions. Soft governance mechanisms are also best suited to the multi-stakeholder approach demanded by the digital age: a fact-based, participative process of deliberation and design, including governments, private sector, civil society, diverse users and policy-makers.

The aim of the holistic "systems" approach we recommended is to bring together government bodies such as competition authorities and consumer protection agencies with the private sector, citizens and civil society to enable them to be more agile in responding to issues and evaluating trade-offs as they emerge. Any new governance approaches in digital cooperation should also, wherever possible, look for ways – such as pilot zones, regulatory sandboxes or trial periods – to test efficacy and develop necessary procedures and technology before being more widely applied.<sup>213</sup>

We envisage that the process of developing a “Global Commitment for Digital Cooperation” would be inspired by the “World We Want” process, which helped formulate the SDGs. Participants would include governments, the private sector from technology and other industries, SMEs and entrepreneurs, civil society, international organisations including standards and professional organisations, academic scholars and other experts, and government representatives from varied departments at regional, national, municipal and community levels. Multi-stakeholder consultation in each member state and region would allow ideas to bubble up from the bottom.

The consultations on an updated global digital cooperation architecture could define upfront the criteria to be met by the governance mechanisms to be proposed, such as funding models, modes of operation and means for serving the functions explored in this report.

More broadly, if appointed, a UN Tech Envoy could identify over-the-horizon concerns that need improved cooperation or governance; provide light-touch coordination of multi-stakeholder actors to address shared concerns; reinforce principles and norms developed in forums with relevant mandates; and work with UN member states, civil society and businesses to support compliance with agreed norms.

The Envoy’s mandate could also include coordinating the digital technology-related efforts of UN entities; improving communication and collaboration among technology experts within the UN; and advising the UN Secretary-General on new technology issues. Finally, the Envoy could promote partnerships to build and maintain international digital common resources that could be used to help achieve the SDGs.

\* \* \*

*We believe in a future which is inclusive and empowering; a future in which digital technologies are used to reduce inequalities, bring people together, enhance international peace and security and promote economic opportunity and environmental sustainability.*

*Our recommendations toward that future will require sustained commitment to fundamental human values. They will require leadership and political will, clarity about roles and responsibilities, shared meanings to ease communication, inclusive partnerships with capacity development, aligned incentives, greater coherence of currently fragmented efforts, and building a climate of trust.*

*We hope this report has shown why individuals, civil society, the private sector and governments urgently need to strengthen cooperation to build that better future.*



# Annexes

## I. Terms of Reference of the Panel

1. The High-Level Panel on Digital Cooperation convened by the UN Secretary-General will advance proposals to strengthen cooperation in the digital space among Governments, the private sector, civil society, international organisations, the technical and academic communities and all other relevant stakeholders. The Panel's report and its recommendations will provide a high-level independent contribution to the broader public debate on digital cooperation frameworks and support Member States in their consultations on these issues.

2. The Panel will consist of 20 eminent leaders from Governments, private sector, academia, the technical community, and civil society led by two co-chairs. Its composition will be balanced in terms of gender, age, geographic representation, and area of expertise. The Panel members will serve in their personal capacity.

3. The Panel shall meet in person at least once. Additional interactions shall be organised for the Panel as a whole by electronic means or through ad hoc group consultations. The Panel will engage and consult widely with governments, private sector, academia, technical community, civil society, and inter-governmental organisations across the world. It shall be agile and innovative in interacting with existing processes and platforms as well as in harnessing inputs from diverse stakeholders.

4. In its report to the Secretary-General, the Panel shall identify good practices and opportunities, gaps and challenges in digital cooperation. It shall also outline major trends in the development and deployment of emerging digital technologies, business models, and policies and the possibilities and challenges they generate for digital cooperation.

5. In particular, the report shall:

- Raise awareness among policy makers and the general public about the transformative impact of digital technologies across society and the economy;
- Suggest ways to bridge disciplines on digital cooperation by identifying policy, research and information gaps as well as ways to improve interdisciplinary thinking and cross-domain action on digital technologies;
- Present recommendations for effective, inclusive, accountable systems of digital cooperation among all relevant actors in the digital space.

6. The recommendations in the report shall seek to maximise the potential of digital technologies to contribute *inter alia* to the achievement of the 2030 Agenda for Sustainable Development and to support progress across a range of themes, including digital empowerment, inclusive finance, employment, entrepreneurship, trade and cross border data flows.

7. They shall also contribute to raising individual and systemic capacities to maximise the benefits of emerging digital technologies; to facilitating the participation of all stakeholder groups, especially youth and women, in the digital sphere and; to enhancing implementation of existing digital policies as well as norms.

8. The Panel shall avoid duplication with existing forums for digital cooperation. It shall fully respect current UN structures as well as national, technical community and industry prerogatives in the development and governance of digital technologies.

9. The Panel will complete its deliberations and submit its final report, including actionable recommendations, within a nine-month period.

10. The deliberations of the Panel will be supported by a small secretariat and funded by donor resources. The Secretariat shall seek to leverage existing platforms and partners, including UN agencies, working in the related domains.

## II. Panel Members

### *Co-Chairs*

- Melinda Gates (USA), Co-Chair of the Bill & Melinda Gates Foundation
- Jack Ma (China), Executive Chairman, Alibaba Group

### *Members*

- Mohammed Abdullah Al Gergawi (UAE), Minister of Cabinet Affairs and the Future, UAE
- Yuichiro Anzai (Japan), Senior Advisor and Director of Center for Science Information Analysis, Japan Society for the Promotion of Science
- Nikolai Astrup (Norway), Former Minister of International Development, now Minister of Digitalisation, Norway
- Vinton Cerf (USA), Vice President and Chief Internet Evangelist, Google
- Fadi Chehadé (USA), Chairman, Chehadé & Company
- Sophie Soowon Eom (Republic of Korea), Founder of Adriel AI and Solidware
- Isabel Guerrero Pulgar (Chile), Executive Director, IMAGO Global Grassroots and Lecturer, Harvard Kennedy School
- Marina Kaljurand (Estonia), Chair of the Global Commission on the Stability of Cyberspace
- Bogolo Kenewendo (Botswana), Minister of Investment, Trade and Industry, Botswana
- Marina Kolesnik (Russian Federation), senior executive, entrepreneur and WEF Young Global Leader
- Doris Leuthard (Switzerland), former President and Federal Councillor of the Swiss Confederation, Switzerland
- Cathy Mulligan (United Kingdom), Visiting Researcher, Imperial College London and Chief Technology Officer of GovTech Labs at University College London
- Akaliza Keza Ntwari (Rwanda), ICT advocate and entrepreneur
- Edson Prestes (Brazil), Professor, Institute of Informatics, Federal University of Rio Grande do Sul
- Kira Radinsky (Israel), Director of Data Science, eBay
- Nanjira Sambuli (Kenya), Senior Policy Manager, World Wide Web Foundation
- Dhananjayan Sriskandarajah (Australia), Chief Executive, Oxfam GB
- Jean Tirole (France), Chairman of the Toulouse School of Economics and the Institute for Advanced Study in Toulouse

### *Ex officio*

- Amandeep Singh Gill (India), Executive Director, Secretariat of the High-level Panel on Digital Cooperation
- Jovan Kurbalija (Serbia), Executive Director, Secretariat of the High-level Panel on Digital Cooperation

### **III. Panel Secretariat and Support Teams**

#### *Panel Secretariat*

- Isabel de Sola, Senior Adviser, Engagement
- Amandeep Singh Gill, Executive Director
- Jovan Kurbalija, Executive Director
- Ananita Maitra, Project Officer, Policy and Engagement
- Chengetai Masango, Senior Adviser (on loan from the IGF Secretariat, July-October 2018)
- Lisa McMonagle, Intern
- Madeline McSherry, Project Officer, Engagement
- Claire Messina, Deputy Executive Director
- AJung Moon, Senior Adviser, Research & Industry
- Athira Murali, Intern
- Anoush Rima Tatevossian, Senior Communications Officer
- Talea von Lupin, Intern
- Andrew Wright, Writer

#### *Sherpas and Support Teams*

- Co-Chair Melinda Gates: Gargee Ghosh, John Norris
- Co-Chair Jack Ma: James Song, Jason Pau, Sami Farhad, Yuan Ren

#### **IV. Donors**

The Panel gratefully acknowledges the financial and in-kind contributions of the following governments and partners, without whom it would not have been able to carry out its responsibilities:

Robert Bosch Stiftung  
Government of the People's Republic of China  
Government of Denmark  
Government of Finland  
Ford Foundation  
Global Challenges Foundation  
IGF Secretariat  
Government of Israel  
Government of Norway  
Government of Qatar  
Government of Switzerland  
Government of the United Arab Emirates  
UN Foundation

## V. The Panel's Engagement

As per its terms of reference, the Panel engaged widely with governments, private sector, academia, the technical community, civil society, and inter-governmental organisations across the world. The aims of its engagement strategy were to provide stakeholders with an opportunity to contribute meaningfully to the reflection process of the Panel; catalyse multi-stakeholder and interdisciplinary cooperation on digital issues; and co-create the report's recommendations with stakeholders, with a view to building buy-in for their implementation.

The engagement strategy was guided by three main tenets:

- **Breadth and inclusivity:** The Panel aimed to consult as broadly as possible across regions, demographics, topics, sectors and disciplines. The process strove to be as inclusive as possible of diverse groupings.
- **Depth:** The Panel worked with experts and conducted 'deep dives' on specific focus areas through virtual or in-person consultations as well as bilateral interviews.
- **Interdisciplinarity:** Many digital challenges are currently addressed in policy or agency silos; to promote more holistic approaches, the Panel's activities invited interdisciplinary and multisectoral perspectives to the table.

The Panel was conscious of the importance of avoiding duplication of efforts and 'consultation fatigue' amongst digital stakeholders. Building on existing networks and policy forums, engagement activities took place as close as possible to stakeholders on the ground. The Panel also consciously assumed the learnings of previous commissions and existing working groups while also harnessing opportunities to connect the issues in new ways.

### Activities

Conducting a global consultation in the span of few months would not have been possible without the immense support of dozens of organisations and governments worldwide who lent their resources and networks to the Panel.

Engagement proceeded in two phases: in the 'listening' phase, in the autumn of 2018, the Panel actively collected stakeholders' concerns and ideas on digital cooperation. Feedback from stakeholders was fed into the Panel's scoping of its work and formed the basis of the nine "enablers of digital cooperation" articulated mid-way through the Panel process. In the spring of 2019, the focus shifted to 'road-testing' the Panel's emerging recommendations. Stakeholders from across sectors were invited to comment on and critique the draft recommendations with a view to improving them.

Overall, the Panel and its Secretariat carried out 125 engagement activities; these included participating in 44 digital policy events and organising 10 thematic workshops (on subjects such as values and principles, digital trust and security, data, digital health), 28 briefings to various stakeholder communities, 11 visits to digital hubs and capitals, 22 virtual meetings with subject-matter experts, and 10 townhall meetings open to the public. In addition, the Panel held a large number of bilateral meetings with a variety of stakeholders.

A virtual window for consultation was opened via the Panel's website. In October 2018, an open Call for Contributions was launched; by January 2019, when the call closed, 167 stakeholders had sent written submissions. Additionally, an informal public opinion survey was set up to capture the views of stakeholders on the digital issues of greatest concern.

In total, the Panel and its Secretariat engaged with over 4,000 individuals representing 104 states, 80 international organisations, 203 private sector companies, 125 civil society organisations, 33 technical organisations, and 188 think tanks and academic institutions.

Our analysis of approximately 1200 core participants in our engagement process finds that 40% were women; 3% were aged under 30; and the regional breakdown was 20% North America, 19% Europe, 13% Sub-Saharan Africa, 8% Latin America and the Caribbean, 7% South and Central Asia, 7% Southeast and East Asia, and 4% Middle East (the rest had a global remit).

These results show that we did not wholly avoid a skew towards male and Western voices, though they compare favourably with many such exercises in the technology sector. They indicate the continuing need for digital cooperation mechanisms to make specific efforts to ensure inclusivity, and highlight in particular the challenge of bringing the "digital native" youth generation into digital policymaking.

## Partners

The Panel would like to thank the following partners for their generous assistance and support to its engagement process:

Access Now

African Union Commission

Alibaba Group

APEC China Business Council (ACBC)

Ministry of Foreign Affairs and Worship of Argentina

Asia Pacific Network Information Centre (APNIC)

Association for Progressive Communication (APC)

Government of Benin

Botnar Foundation

Business Council for the United Nations

Consulate General of Canada in San Francisco

CERN

China Chamber of International Commerce (CCOIC)

Data2x

Digital Empowerment Foundation

Digital Impact Alliance (DIAL)

Diplo Foundation

Delegation of the European Union to the United Nations and Other International Organisations in Geneva

Direction interministérielle du numérique et du système d'information et de communication de l'Etat, France

Freedom Online Coalition

Gateway House

Geneva Internet Platform

Global Commission on Stability of Cyberspace

Global Partners Digital  
Global Partnership on Sustainable Development Data  
Global Tech Panel  
GSM Association (GSMA)  
Hangzhou Normal University  
Impact Hub Basel  
Infosys  
International Chamber of Commerce (ICC)  
International Telecommunications Union (ITU)  
Internet Corporation for Assigned Names and Numbers (ICANN)  
iSPIRT  
JD.com  
JSC National ICT Holding Zerde  
Government of Kazakhstan  
King's College London  
Lee Kwan Yew School of Public Policy  
New America Foundation  
Nokia  
Observer Research Foundation  
Office of Denmark's Technology Ambassador  
Omidyar Foundation  
Organisation for Economic Cooperation and Development (OECD)  
Organisation Internationale de la Francophonie (OIF)  
Schwarzman Scholars, Tsinghua University  
Ministry of Foreign Affairs of Singapore  
Stanford University  
Tata Consultancy Services, Mumbai  
United Nations Conference on Trade and Development (UNCTAD)  
United Nations Economic Commission for Latin America and the Caribbean (ECLAC)  
United Nations Educational, Scientific and Cultural Organization (UNESCO)  
United Nations Children's Fund (UNICEF)  
United Nations Global Pulse  
United Nations Institute for Disarmament Research (UNIDIR)  
United Nations Office at Geneva  
United Nations University  
University of California, Berkeley  
University of Geneva  
Verizon Wireless  
Web Summit  
Western Balkans Digital Summit  
Wonder Ventures  
World Bank  
World Economic Forum  
World Economic Forum Center for the Fourth Industrial Revolution, San Francisco  
World Government Summit, Dubai  
World Intellectual Property Organization (WIPO)  
World Internet Conference  
World Summit AI



## VI. Principles and Functions of Digital Cooperation

In the course of our outreach, many stakeholders suggested principles to which digital cooperation mechanisms should adhere and functions they should seek to serve. Drawing also on work of previous initiatives in these areas, this annex summarises the principles and functions we suggest are most important to guide the future evolution of digital cooperation.

### Key Principles of Digital Cooperation

- **Consensus-oriented:** Decisions should be made in ways that seek consensus among public, private and civic stakeholders.
- **Polycentric:** Decision-making should be highly distributed and loosely yet efficiently coordinated across specialised centres.
- **Customised:** There is generally no “one size fits all” solution; different communities can implement norms in their own way, according to circumstances.
- **Subsidiarity:** Decisions should be made as locally as possible, closest to where the issues and problems are.
- **Accessible:** It should be as easy as possible to engage in digital cooperation mechanisms and policy discussions.
- **Inclusive:** Decisions should be inclusive and democratic, representing diverse interests and accountable to all stakeholders.
- **Agile:** Digital cooperation should be dynamic, iterative and responsive to fast-emerging policy issues.
- **Clarity in roles and responsibility:** Clear roles and shared language should reduce confusion and support common understanding about the responsibilities of actors involved in digital cooperation (governments, private sector, civil society, international organisations and academia).
- **Accountable:** There should be measurable outcomes, accountability and means of redress.
- **Resilient:** Power distribution should be balanced across sectors, without centralised top-down control.
- **Open:** Processes should be transparent, with minimum barriers to entry.
- **Innovative:** It should always be possible to innovate new ways of cooperating, in a bottom-up way, which is also the best way to include diverse perspectives.
- **Tech-neutral:** Decisions should not lock in specific technologies but allow for innovation of better and context-appropriate alternatives.
- **Equitable outcomes:** Digital cooperation should maximise the global public interest (internationally) and be anchored in broad public benefit (nationally).

## Key Functions of Digital Cooperation

- **Leadership** – generating political will among leaders from government, business, and society, and providing an authoritative response to digital policy challenges.
- **Deliberation** – providing a platform for regular, comprehensive and impactful deliberations on digital issues with the active and effective participation of all affected stakeholders.
- **Ensuring inclusivity** – ensuring active and meaningful participation of all stakeholders, for example by linking with existing and future bottom-up networks and initiatives.<sup>214</sup>
- **Evidence and data** – monitoring developments and identifying trends to inform decisions, including by analysing existing data sources.
- **Norms and policy making** – building consensus among diverse stakeholders, respecting the roles of states and international organisations in enacting and enforcing laws.
- **Implementation** – following up on policy discussions and agreements.
- **Coordination** – creating shared understanding and purpose across bodies in different policy areas and at different levels (local, national, regional, global), ensuring synchronisation of efforts, interoperability and policy coherence, and the possibility of voluntary coordination between interested stakeholder groups.
- **Partnerships** – catalysing partnerships around specific issues by providing opportunities to network and collaborate.
- **Support and capacity development** – strengthening capacity development, monitoring digital developments, identifying trends, informing policy actors and the public of emerging risks and opportunities, and providing data for evidence-based decision making – allowing traditionally marginalised persons or other less-resourced stakeholders to actively participate in the system.
- **Conflict resolution and crisis management** – developing the skills, knowledge and tools to prevent and resolve disputes and connect stakeholders with assistance in a crisis.

## Notes

<sup>1</sup> See Annex I for the Panel's terms of reference.

<sup>2</sup> United Nations Commission on Science and Technology for Development, Mapping of international Internet public policy issues, 17 April 2015, E/CN.16/2015/CRP.2, available at [https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2\\_en.pdf](https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf)

<sup>3</sup> GIP Digital Watch Observatory, May 2019, available at <https://dig.watch>

<sup>4</sup> AI Impacts, "Trends in the cost of computing", 10 March 2015, available at <https://aiimpacts.org/trends-in-the-cost-of-computing/>

<sup>5</sup> Internet World Stats, "World Internet users and population statistics", March 2019, available at <https://www.internetworldstats.com/stats.htm>; and IoT Analytics, "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating", August 2018, available at <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>

<sup>6</sup> The World Bank, Global Findex Database 2017, April 2018, available at <https://globalfindex.worldbank.org>

<sup>7</sup> Council on Foreign Relations, "Hate Speech on Social Media: Global Comparisons", 11 April 2019, available at <https://www.cfr.org/background/hate-speech-social-media-global-comparisons>; United Nations General Assembly, resolution on the right to privacy in the digital age (A/RES/73/179), December 2018, available at [https://www.un.org/en/ga/search/view\\_doc.asp?symbol=A/RES/73/179](https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/179); FireEye, M-Trends 2019 (Annual Threat Report), 2019, available at <https://content.fireeye.com/m-trends>; Freedom House, "Freedom on the Net 2018: The rise of digital authoritarianism", October 2018, available at <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism>

<sup>8</sup> Internet World Stats, "World Internet users and population statistics", March 2019, available at <https://www.internetworldstats.com/stats.htm>

<sup>9</sup> The International Telecommunication Union (ITU) is one of the many entities that recognise the multiple dimensions of the digital divide and work toward facilitating digital inclusion of marginalised groups. More details at ITU, Digital Inclusion, available at <https://www.itu.int/en/ITU-D/Digital-Inclusion/Pages/default.aspx>

<sup>10</sup> Our public call for contributions received a number of suggestions on values, available at [www.digitalcooperation.org/responses](http://www.digitalcooperation.org/responses). We also engaged a diverse set of stakeholders and experts to elicit relevant values and how they could be embedded in policy approaches and cooperation architectures. Our engagement built on a recent surge of interest in values and ethics in the digital context: see Future of Life Institute, Asilomar Principles, 2017, available at <https://futureoflife.org/ai-principles/>; WEF White Paper on Values, Ethics and Innovation, August 2018, available at [http://www3.weforum.org/docs/WEF\\_WP\\_Values\\_Ethics\\_Innovation\\_2018.pdf](http://www3.weforum.org/docs/WEF_WP_Values_Ethics_Innovation_2018.pdf)

; Montreal Declaration for a responsible development of AI, 2018, available at <https://www.montrealdeclaration-responsibleai.com/the-declaration>; the World Wide Web Foundation's Contract for the Web, available at <https://contractfortheweb.org>; the EU High-Level Expert Group on Artificial Intelligence's Ethics Guidelines for Trustworthy Artificial Intelligence, 2019, available at <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>

<sup>11</sup> WEF report "Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society", December 2018, available at [http://www3.weforum.org/docs/WEF\\_Our\\_Shared\\_Digital\\_Future\\_Report\\_2018.pdf](http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf)

<sup>12</sup> For an introduction to the underlying technology trends and impact on the economy, see "Vectors of Digital Transformation", OECD Digital Economy Papers: January 2019, No. 273.

<sup>13</sup> World Bank, World Development Report 2016: Digital Dividends, "How the Internet Promotes Development", 2016.

<sup>14</sup> Financial inclusion is defined as the ability to "access and use a range of appropriate and responsibly provided financial services offered in a well-regulated environment." (UNCDF, Financial Inclusion, available at <https://www.uncdf.org/financial-inclusion>)

<sup>15</sup> World Bank, World Bank Global Findex Database: Measuring Fintech Inclusion and the Fintech Revolution, 2017, available at <https://globalfindex.worldbank.org/>

<sup>16</sup> Mobile money serves as a tool for financial inclusion, allowing those without traditional bank accounts to participate in the economy on a greater level (McKinsey, "Mobile money in emerging markets: The business case for financial inclusion", March 2018).

<sup>17</sup> Women Deliver, "If We Want to Go Far, We Must Go Together", 21 January 2019, available at <https://womendeliver.org/2019/if-you-want-to-go-far-you-must-go-together/>

<sup>18</sup> Financial Stability Board, "FinTech and market structure in financial services: Market developments and potential financial stability implications", 14 February 2019, available at <https://www.fsb.org/wp-content/uploads/P140219.pdf>

<sup>19</sup> The Economist, "Financial inclusion in the rich world", 4 May 2018, available at <https://www.economist.com/special-report/2018/05/04/financial-inclusion-in-the-rich-world>

<sup>20</sup> M-Pesa is a mobile money service that allows users to transfer cash using their mobile phone numbers without the need for a bank account. It serves over 17 million Kenyans and offers loan and savings products as well. See The Economist, "Why does Kenya lead the world in mobile money?". 02 March 2015, available at <https://www.economist.com/the-economist-explains/2015/03/02/why-does-kenya-lead-the-world-in-mobile-money>.

<sup>21</sup> Ming Zeng, "Smart Business: What Alibaba Success Reveals about the Future of Strategy", Harvard Business Review 2018, pp 58-59.

- <sup>22</sup> Harvard Business School, “Replicating MPESA: Lessons from Vodafone (Safaricom) on why mobile money fails to gain traction in other markets”, 20 November 2016, available at <https://rctom.hbs.org/submission/replicating-mpesa-lessons-from-vodafone-safaricom-on-why-mobile-money-fails-to-gain-traction-in-other-markets/>
- <sup>23</sup> Accion, “The game-changing innovation that could bring financial services to millions in India”, 30 October 2017, available at <https://www.accion.org/the-game-changing-innovation-that-could-bring-financial-services-to-millions-in-india>
- <sup>24</sup> GSM Association, State of the Industry Report on Mobile Money 2018, available at <https://www.gsma.com/r/wp-content/uploads/2019/05/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2018.pdf>
- <sup>25</sup> World Bank, Global ID4D Dataset, 2017, and World Bank, ID4D-Findex survey.
- <sup>26</sup> MGI, “Digital Identity: A Key to Inclusive Growth”, MGI (Jan 2019). The report focuses on 7 diverse economies: Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States.
- <sup>27</sup> See for example Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St. Martin’s Press, 2018), excerpt available at <https://us.macmillan.com/excerpt?isbn=9781250074317>
- <sup>28</sup> ID4D, available at <http://id4d.worldbank.org/>
- <sup>29</sup> MOSIP, available at <https://www.mosip.io/>
- <sup>30</sup> Luohan Academy, “Digital Technology and Inclusive Growth”, 2019, available at [https://gw.alipayobjects.com/os/antfincdn/DbLN6yXw6H/Luohan\\_Academy-Report\\_2019\\_Executive\\_Summary.pdf](https://gw.alipayobjects.com/os/antfincdn/DbLN6yXw6H/Luohan_Academy-Report_2019_Executive_Summary.pdf)
- <sup>31</sup> World Bank: “E-commerce Participation and Household Income Growth in Taobao Villages”, April 2019, available at <http://documents.worldbank.org/curated/en/839451555093213522/pdf/E-Commerce-Participation-and-Household-Income-Growth-in-Taobao-Villages.pdf>; World Bank, “E-commerce for poverty alleviation in rural China: from grassroots development to public-private partnerships”, 19 March 2019, available at <http://beta-blogs.worldbank.org/eastasiapacific/e-commerce-poverty-alleviation-rural-china-grassroots-development-public-private-partnerships>; World Development Report 2016, “E-commerce with Chinese characteristics: inclusion, efficiency and innovation in Taobao villages”.
- <sup>32</sup> United Nations Conference on Trade and Development, Information Economy Report 2015, Unlocking the Potential of E-Commerce for Developing Countries, 2015, available at [https://unctad.org/en/PublicationsLibrary/ier2015\\_en.pdf](https://unctad.org/en/PublicationsLibrary/ier2015_en.pdf)
- <sup>33</sup> “Riding the Big Data Wave in 2017”, Medium, 17 April 2017, available at [https://medium.com/@Byte\\_Academy/riding-the-big-data-wave-in-2017-a-new-term-big-data-was-coined-few-8f02a5973023](https://medium.com/@Byte_Academy/riding-the-big-data-wave-in-2017-a-new-term-big-data-was-coined-few-8f02a5973023)
- <sup>34</sup> United Nations, The Sustainable Development Goals Report: 2018.
- <sup>35</sup> World Health Organization, “Civil registration: why counting births and deaths is important”, 30 May 2014, available at <https://www.who.int/news-room/fact-sheets/detail/civil-registration-why-counting-births-and-deaths-is-important>
- <sup>36</sup> The World Bank, PovcalNet, available at <http://iresearch.worldbank.org/PovcalNet/povOnDemand.aspx>
- <sup>37</sup> This definition is substantially drawn from Recital 26 of the GDPR which defines anonymized data as “data rendered anonymous in such a way that the data subject is not or no longer identifiable.”
- <sup>38</sup> United States Agency for International Development, “Fighting Ebola with Information”, available at <http://www.digitaldevelopment.org/fighting-ebola-information>
- <sup>39</sup> World Health Organization, Global Strategy on Digital Health, 26 March 2019, available at <https://extranet.who.int/dataform/upload/surveys/183439/files/Draft%20Global%20Strategy%20on%20Digital%20Health.pdf>
- <sup>40</sup> CGAIR Platform for Big Data in Agriculture, available at <https://bigdata.cgiar.org/>
- <sup>41</sup> Jason Plautz, “Cheap, Portable Sensors are Democratizing Air-Quality Data”, Wired, 7 November 2018, available at <https://www.wired.com/story/cheap-portable-sensors-are-democratizing-air-quality-data/>
- <sup>42</sup> For more information on global digital public goods, see: <https://digitalpublicgoods.net/public-goods/>
- <sup>43</sup> Paul Krugman and Robin Wells, Microeconomics (Worth Publishers, New York, NY, 2013).
- <sup>44</sup> See “About India Stack”, available at: <https://indiastack.org/about/>
- <sup>45</sup> Pathways to Prosperity Commission, 2018, available at <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>
- <sup>46</sup> WIRED, “Global Internet Access is Even More Worse than Dire Reports Suggest”, 23 October 2018, available at <https://www.wired.com/story/global-internet-access-dire-reports/>
- <sup>47</sup> The index measures 84 countries from 2018-2019. The Economist, The Inclusive Internet Index 2019, available at <https://theinclusiveinternet.eiu.com/>
- <sup>48</sup> Ibid.
- <sup>49</sup> In India nearly two-thirds of urban areas have connectivity, compared to just over a fifth of rural regions. See The Internet and Mobile Association of India (IAMAI), Mobile Internet Report, 2017.
- <sup>50</sup> World Economic Forum, “Delivering Digital Infrastructure Advancing the Internet Economy”, April 2014, available at [http://www3.weforum.org/docs/WEF\\_TC\\_DeliveringDigitalInfrastructure\\_InternetEconomy\\_Report\\_2014.pdf](http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf)
- <sup>51</sup> The Alliance for Affordable Internet, available at <https://a4ai.org/>
- <sup>52</sup> Broadband Commission for Sustainable Development, available at <https://www.broadbandcommission.org/Pages/default.aspx>

- <sup>53</sup> UNICEF, "Project Connect, in Partnership with UNICEF's Office of Innovation, Launches First of Its Kind, Interactive Map Visualizing the Digital Divide in Education", 02 November 2017, available at <http://unicefstories.org/2017/11/02/schoolmappingprojectconnect/>
- <sup>54</sup> World Bank, "Connecting for Inclusion: Broadband Access for All", available at <http://www.worldbank.org/en/topic/digitaldevelopment/brief/connecting-for-inclusion-broadband-access-for-all>
- <sup>55</sup> IEEE Spectrum, "How Project Loon Built the Navigation System That Kept Its Balloons Over Puerto Rico", 8 March 2018, available at <https://spectrum.ieee.org/tech-talk/telecom/internet/how-project-loon-built-the-navigation-system-that-kept-its-balloons-over-puerto-rico>
- <sup>56</sup> Reuters, "Amazon plans to launch over 3,000 satellites to offer broadband internet", 04 April 2019, available at <https://www.reuters.com/article/us-amazon-com-broadband/amazon-plans-to-launch-over-3000-satellites-to-offer-broadband-internet-idUSKCN1RG1YW>; Reuters, "U.S. regulator approves SpaceX plan for broadband satellite services", 29 March 2018, available at <https://www.reuters.com/article/us-spacex-fcc/u-s-regulator-approves-spacex-plan-for-broadband-satellite-services-idUSKBN1H537E>
- <sup>57</sup> The Jakarta Post, "Govt to expand broadband connectivity as internet use grows", 20 February 2018, available at <https://www.thejakartapost.com/news/2018/02/20/govt-to-expand-broadband-connectivity-as-internet-use-grows.html>
- <sup>58</sup> ITU, "Universal Service Fund and Digital Inclusion for All Study", June 2013, available at <https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU%20USF%20Final%20Report.pdf>
- <sup>59</sup> One example of building internet access around community needs, in this case health, is a collaboration between the Basic Internet Foundation and health centres in Tanzania; see Vision 2030, available at <https://www.vision2030.no/index.php/en/visjon2030-projects/non-discriminating-access-for-digital-inclusion>. The Panel has been informed that a 'common bid' for connectivity is being prepared by ITU, UNICEF and the World Bank.
- <sup>60</sup> BBC, Video: Internet access in Africa - Are mesh networks the future?, 28 March 2019, available at <https://www.bbc.co.uk/news/world-africa-47723967>. There is another example from rural England of the power of a cooperative approach: farmers waived right of way charges and volunteered to help dig up trenches for fibre optic cable in exchange for shares in the network. See ISPreview, "B4RN Set to Hit 5000 Rural UK FTTH Broadband Connections Target", 11 September 2018, available at <https://www.ispreview.co.uk/index.php/2018/09/b4rn-set-to-hit-5000-rural-uk-ftth-broadband-connections-target.html>
- <sup>61</sup> Alliance for Affordable Internet, available at <https://a4ai.org/rethinking-affordable-access/>
- <sup>62</sup> Written contribution, Centre for Socio-Economic Development. This does not take away from the tremendous role that digital technologies have played in improving the lives of people with disabilities.
- <sup>63</sup> UNESCO, "Multilingualism in Cyberspace: Indigenous Languages for Empowerment", 27-28 November 2015, available at [http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Events/multilingualism\\_in\\_cyberspace\\_concept\\_paper\\_en.pdf](http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Events/multilingualism_in_cyberspace_concept_paper_en.pdf); Brookings Institute, "Rural and urban America divided by broadband access", 18 July 2016, available at <https://www.brookings.edu/blog/techtank/2016/07/18/rural-and-urban-america-divided-by-broadband-access/>
- <sup>64</sup> ITU Facts and Figures 2017, available at <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>
- <sup>65</sup> Pathways for Prosperity Commission, Digital Lives: Meaningful Connections for the Next 3 Billion, 2018, available at [https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2018-11/digital\\_lives\\_report.pdf](https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2018-11/digital_lives_report.pdf)
- <sup>66</sup> Recognising the importance of marketing in addressing socio-cultural issues, the Unstereotype alliance, an initiative convened by UN Women, unites leaders from across business technology and creative industries to use marketing-based techniques to combat gender stereotypes. Available at <http://www.unstereotypealliance.org/en/about>
- <sup>67</sup> The OECD and WTO-led inter-agency Task Force on International Trade Statistics is one example of work being undertaken by the OECD and others to update traditional metrics of macroeconomic change and trade flows (OECD, Toward a Framework for Measuring the Digital Economy, 19-21 September 2018). The G20 Toolkit for Measuring the Digital Economy identifies methodologies to measure the digital economy as well as gaps and challenges surrounding measurement; (G20 Digital Economy Ministerial Declaration, available at <http://www.g20.utoronto.ca/2018/2018-08-24-digital.html#annex3>). The ITU's ICT Development Index (IDI) measures the level and evolution over time of ICT developments across developed and developing countries (available at <https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx>). The EIU Index covers 100 countries as of 2019 using benchmarks of national digital inclusion across readiness, relevance, affordability, and availability (Ibid).
- <sup>68</sup> The World Bank, World Development Report: The Changing Nature of Work, 2019.
- <sup>69</sup> Thereza Balliester and Adam Elsheikhi, "The Future of Work: A Literature Review", March 2018, available at [https://www.ilo.org/wcmsp5/groups/public/---dgreports/---inst/documents/publication/wcms\\_625866.pdf](https://www.ilo.org/wcmsp5/groups/public/---dgreports/---inst/documents/publication/wcms_625866.pdf)
- <sup>70</sup> Carl Benedikt Frey and Michael A. Osborne, The Future Of Employment: How Susceptible Are Jobs To Computerisation? (Oxford Martin School, 2013), available at [https://www.oxfordmartin.ox.ac.uk/downloads/academic/The\\_Future\\_of\\_Employment.pdf](https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf)
- <sup>71</sup> Towards data science, "Humanities Graduates Should Consider Data Science", 31 August 2017, available at <https://towardsdatascience.com/humanities-graduates-should-consider-data-science-d9fc78735b0c>
- <sup>72</sup> Tim Noonan, Director, International Trade Union Confederation, interview, 25 January 2019.

- <sup>73</sup> CNBC, "The future of work won't be about college degrees, it will be about job skills", 31 October 2018, available at <https://www.cnbc.com/2018/10/31/the-future-of-work-wont-be-about-degrees-it-will-be-about-skills.html>
- <sup>74</sup> The Guardian, "All flexibility, no security: why conservative think tanks are wrong on the gig economy", 23 January 2019, available on <https://www.theguardian.com/business/grogonomics/2019/jan/24/all-flexibility-no-security-why-conservative-thinktanks-are-wrong-on-the-gig-economy>
- <sup>75</sup> International Labour Organization, "Helping the gig economy work better for gig workers", available at [https://www.ilo.org/washington/WCMS\\_642303/lang--en/index.htm](https://www.ilo.org/washington/WCMS_642303/lang--en/index.htm)
- <sup>76</sup> Klaus Schoemann, "Digital Technology to Support the Trade Union Movement", Open Journal of Social Sciences, Vol. 06 No. 01 (2018), available at [https://file.scirp.org/Html/5-1761684\\_81823.htm](https://file.scirp.org/Html/5-1761684_81823.htm)
- <sup>77</sup> WIPO, "The informal economy in developing nations: a hidden engine of growth", June 2017, available at [https://www.wipo.int/wipo\\_magazine/en/2017/03/article\\_0006.html](https://www.wipo.int/wipo_magazine/en/2017/03/article_0006.html)
- <sup>78</sup> OECD, "Tax and Digitalisation", March 2019, available at [www.oecd.org/going-digital/tax-and-digitalisation.pdf](http://www.oecd.org/going-digital/tax-and-digitalisation.pdf)
- <sup>79</sup> South Center, "The WTO's Discussions on Electronic Commerce", January 2017, available at [https://www.southcentre.int/wp-content/uploads/2017/01/AN\\_TDP\\_2017\\_2\\_The-WTO%E2%80%99s-Discussions-on-Electronic-Commerce\\_EN.pdf](https://www.southcentre.int/wp-content/uploads/2017/01/AN_TDP_2017_2_The-WTO%E2%80%99s-Discussions-on-Electronic-Commerce_EN.pdf)
- <sup>80</sup> European Commission, "76 WTO partners launch talks on e-commerce", 25 January 2019, available at <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974>
- <sup>81</sup> UNCTAD, Trade and Development Report 2018: Power, Platforms and the Free Trade Delusion, Chapter III.
- <sup>82</sup> OECD, "Vectors of Digital Transformation" (OECD Publishing, Paris, 22 January 2019).
- <sup>83</sup> Michael Mandel, Data, Trade and Growth, Progressive Policy Institute, April 2014, available at [https://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel\\_Data-Trade-and-Growth.pdf](https://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf)
- <sup>84</sup> Parminder Jeet Singh, "Digital Industrialisation in Developing Countries", paper for the Commonwealth Secretariat, 2018.
- <sup>85</sup> OECD, "Tax and Digitalisation", March 2019, available at [www.oecd.org/going-digital/tax-and-digitalisation.pdf](http://www.oecd.org/going-digital/tax-and-digitalisation.pdf)
- <sup>86</sup> OECD/G20 Base Erosion and Shifting Project, Tax Challenges Arising from Digitalisation, Interim report 2018, available at: [https://read.oecd-ilibrary.org/taxation/tax-challenges-arising-from-digitalisation-interim-report\\_9789264293083-en#page3](https://read.oecd-ilibrary.org/taxation/tax-challenges-arising-from-digitalisation-interim-report_9789264293083-en#page3); Esquire, "Silicon Valley's Tax-Avoiding, Job-Killing, Soul-Sucking Machine", available at <https://www.esquire.com/news-politics/a15895746/bust-big-tech-silicon-valley/>
- <sup>87</sup> OECD, Base Erosion and Profit Shifting, available at <https://www.oecd.org/tax/beps/>
- <sup>88</sup> Bloomberg Tax, "What's Next for Countries Going it Alone on Digital Taxes", 21 March, 2019, available at <https://news.bloombergtax.com/daily-tax-report-international/whats-next-for-countries-going-it-alone-on-digital-tax>
- <sup>89</sup> KPMG, "Taxation of Digital Assets: New Laws Issued", 15 May 2018, available at <https://home.kpmg/xx/en/home/insights/2018/05/tax-news-flash-issue-380.html>
- <sup>90</sup> Jean Tirole, "Regulating Disrupters", Project Syndicate, 9 January 2019, available at [www.project-syndicate.org/onpoint/regulating-the-disrupters-by-jean-tirole-2019-01?barrier=accesspaylog](http://www.project-syndicate.org/onpoint/regulating-the-disrupters-by-jean-tirole-2019-01?barrier=accesspaylog).
- <sup>91</sup> For more on these processes, see Jean Tirole, Economics for the Common Good (Princeton University Press, 2016).
- <sup>92</sup> Since 1979, the International Conference of Data Protection & Privacy Commissioners (ICDPPC) has provided a forum for connecting the efforts of 122 data protection and privacy authorities from across the globe; and since 2001, the International Competition Network (ICN) has provided a specialised yet informal venue for maintaining regular dialogue across the global antitrust community to build procedural and substantive convergence and address practical competition concerns for the benefit of consumers and economies.
- <sup>93</sup> The National Institute for Transparency, Access to Information and Personal Data Protection (INAI) is an autonomous constitutional body responsible for upholding the right to access to public information. It is also in charge of upholding the right to protection of personal data held by the public and the private sectors. See <http://www.networkforintegrity.org/continents/america/instituto-nacional-de-transparencia-acceso-a-la-informacion-y-proteccion-de-datos-personales-inai/>
- <sup>94</sup> OECD, "Strengthening digital government", OECD Going Digital Policy Note, OECD Paris, March 2019, available at [www.oecd.org/going-digital/strengthening-digital-government.pdf](http://www.oecd.org/going-digital/strengthening-digital-government.pdf)
- <sup>95</sup> See Creators, available at <https://www.creatorspad.com/pages/govtech-program>
- <sup>96</sup> Infocomm Media Development Corporation, available at <https://www.imda.gov.sg/imtalent/training-and-courses>
- <sup>97</sup> Minister Omar Al Olama, Remarks at the World Government Summit, 10 February 2019.
- <sup>98</sup> The Verge, "The mass shooting in New Zealand was designed to spread on social media", 15 March 2019, available on <https://www.theverge.com/2019/3/15/18266859/new-zealand-shooting-video-social-media-manipulation>
- <sup>99</sup> Myanmar went from minimal connectivity in 2013 to virtually half the population in 2016 owning smartphones. Facebook became the dominant communications platform almost by accident. See Reuters, "Why Facebook is losing the war on hate speech in Myanmar", 15 August 2018, available at <https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/>
- <sup>100</sup> National Public Radio, "#Gamergate Controversy Fuels Debate On Women And Video Games", 24 September 2014, available at <https://www.npr.org/sections/alltechconsidered/2014/09/24/349835297/-gamergate-controversy-fuels-debate-on-women-and-video-games>
- <sup>101</sup> The Guardian, "Instagram bans 'graphic' self-harm images after Molly Russell's death", 7 February 2019, available at <https://www.theguardian.com/technology/2019/feb/07/instagram-bans-graphic-self-harm-images-after-molly-russells-death>

- <sup>102</sup> Hindustan Times, “24-yr-old commits suicide after being bullied for dressing up as a woman”, 19 October 2019, available at <https://www.hindustantimes.com/india-news/24-yr-old-commits-suicide-after-being-bullied-for-dressing-up-as-a-woman/story-8PIWvf0fMwcd72A5Tp8tBl.html>
- <sup>103</sup> Ofcom and UK Information Commissioner’s Office, “Internet users’ experience of harm online: summary of survey research”, July 2018, available at [https://www.ofcom.org.uk/\\_data/assets/pdf\\_file/0018/120852/Internet-harm-research-2018-report.pdf](https://www.ofcom.org.uk/_data/assets/pdf_file/0018/120852/Internet-harm-research-2018-report.pdf)
- <sup>104</sup> NSPCC, “Net Aware report 2017: ‘Freedom to express myself safely’”, 04 September 2018, available at <https://learning.nspcc.org.uk/research-resources/2017/net-aware-report-2017-freedom-to-express-myself-safely/>
- <sup>105</sup> India alone had over 100 incidents in 2018. See Freedom House, “Freedom on the Net 2018”, October 2018, available at [https://freedomhouse.org/sites/default/files/FOTN\\_2018\\_Final%20Booklet\\_11\\_1\\_2018.pdf](https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf)
- <sup>106</sup> United Nations, Office of the High Commissioner for Human Rights, “Human Rights Appeal 2019”, 17 January 2019, available at <https://www.ohchr.org/Documents/Publications/AnnualAppeal2019.pdf>
- <sup>107</sup> Electronic Frontier Foundation, “India’s Supreme Court Upholds Right to Privacy as a Fundamental Right”, 27 August 2017, available at <https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time>
- <sup>108</sup> Written contribution, the Paradigm Initiative. The bill has not received presidential assent.
- <sup>109</sup> United Nations Children’s Fund, United Nations Global Compact, Save the Children, “Children’s Rights and Business Principles”, 03 March 2012, available at [https://www.unglobalcompact.org/docs/issues\\_doc/human\\_rights/CRBP/Childrens\\_Rights\\_and\\_Business\\_Principles.pdf](https://www.unglobalcompact.org/docs/issues_doc/human_rights/CRBP/Childrens_Rights_and_Business_Principles.pdf)
- <sup>110</sup> United Nations Educational, Scientific and Cultural Organization, “Steering AI and Advanced ICTs for Knowledge Societies”, available at [https://en.unesco.org/system/files/unesco-steering\\_ai\\_for\\_knowledge\\_societies.pdf](https://en.unesco.org/system/files/unesco-steering_ai_for_knowledge_societies.pdf)
- <sup>111</sup> Council of Europe, Freedom of Expression, Standard Setting, available at <https://www.coe.int/en/web/freedom-expression/internet-standard-setting>; and European Court of Human Rights decisions, for example, in the case of Ahmet Yildirim v. Turkey, available at <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-115705%22%7D>
- <sup>112</sup> IFEX, “Saudi Arabia arrests at least 13 more human rights defenders”, 14 April 2019.
- <sup>113</sup> UN Global Compact “Guiding Principles for Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework”, 2011, available at <https://www.unglobalcompact.org/library/2>
- <sup>114</sup> The Business & Human Rights Resource Centre, available at <https://www.business-humanrights.org/>
- <sup>115</sup> A Corporate Accountability Index is published annually by Ranking Digital Rights. Available at <https://rankingdigitalrights.org/>
- <sup>116</sup> Carnegie UK Trust, “Reducing harm in social media through a duty of care”, 08 May 2018, available at <https://www.carnegieuktrust.org.uk/blog/reducing-harm-social-media-duty-care/>
- <sup>117</sup> Pew Research Trust, “Online Harassment 2017”, 11 July 2017, available at <https://www.pewinternet.org/2017/07/11/online-harassment-2017/>
- <sup>118</sup> Amanda and Noel Sharkey, “Granny and the robots: ethical issues in robot care for the elderly”, University of Sheffield, 03 July 2010.
- <sup>119</sup> United Nations Children’s Fund, “One in Three: Internet Governance and Children’s Rights”, discussion paper, 2016.
- <sup>120</sup> U.S. Government Publishing Office, “Electronic Code of Federal Regulation”, 26 April 2019, available at <https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5>; UK Information Commissioner’s Office, “Age appropriate design: a code of practice for online services”, 15 April 2019, available at <https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf>
- <sup>121</sup> Elon University, “Survey X: Artificial Intelligence and the Future of Humans”, 2018, available at [http://www.elon.edu/e-web/imagining/surveys/2018\\_survey/AI\\_and\\_the\\_Future\\_of\\_Humans.xhtml](http://www.elon.edu/e-web/imagining/surveys/2018_survey/AI_and_the_Future_of_Humans.xhtml)
- <sup>122</sup> Pedro Domingos, *The Master Algorithm: How the quest for the ultimate learning machine will remake our world* (Basic Books, 2015).
- <sup>123</sup> Cathy O’Neil, *Weapons of Math Destruction* (The Crown Publishing Group, 2016); Digital Society, “Human rights in the robot age - Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality”, 11 October 2017; Umoja Noble, “Algorithms of Oppression – How Search Engines Reinforce Racism”, 08 January 2018, available at <https://nyupress.org/9781479837243/algorithms-of-oppression/>
- <sup>124</sup> Investors and founders are finally waking up to the gender problem in tech after high-profile scandals and walkouts by employees at companies such as Google. See Aliya Ram, “Tech investors put #MeToo clauses in deals”, *Financial Times*, 22 March 2019.
- <sup>125</sup> Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin’s Press, 2018); excerpt available at <https://us.macmillan.com/excerpt?isbn=9781250074317>
- <sup>126</sup> Harvard Law Today, “Algorithms and their unintended consequences for the poor”, 07 November 2018, available at <https://today.law.harvard.edu/algorithms-and-their-unintended-consequences-for-the-poor/?fbclid=IwAR2yLUMpEYj8YKhvZDQktU0LNHNDatRtqVBgZHW45uHMEYubyQr36h08H8>
- <sup>127</sup> Institute of Electrical and Electronics Engineers, “Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems”, available at [https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead\\_v2.pdf](https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v2.pdf)

<sup>128</sup> One important discussion is on the applicability of International Humanitarian Law and accountability thereunder for the use of military systems that might deploy AI. See Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, “Report of the 2018 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems”, 23 October 2018, available at <https://undocs.org/en/CCW/GGE.1/2018/3>

<sup>129</sup> Wendell Wallach, *An Agile Ethical/Legal Model for the International and National Governance of AI and Robotics* (Association for the Advancement of Artificial Intelligence, 2018).

<sup>130</sup> António Guterres, United Nations Secretary-General, remarks at the Web Summit, Lisbon, 05 November 2018, available at <https://www.un.org/sg/en/content/sg/speeches/2018-11-05/remarks-web-summit>; “Autonomous weapons that kill must be banned, insists UN chief”, March 29, 2019, available at <https://news.un.org/en/story/2019/03/1035381>

<sup>131</sup> Provisions similar to the U.S. Fourth Amendment exist in several Constitutions and the 1980 OECD Guidelines codified 8 principles that have influenced privacy regulations since then. These were updated in 2013 as Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data and are available at [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)

<sup>132</sup> David Dodwell, “The integration of mass surveillance and new digital technologies is unnerving”, *The South China Morning Post*, 17 February 2018, available at <https://www.scmp.com/comment/insight-opinion/article/2133617/integration-mass-surveillance-and-new-digital-technologies>; United Nations General Assembly, Summary of the Human Rights Council penal discussion on the right to privacy in the digital age, 19 December 2014.

<sup>133</sup> The 2016 Privacy Shield framework (earlier Safe Harbor), which governs personal data flows between the U.S. and the E.U. and Switzerland based on self-certification by companies, is an example of the former; available at <https://www.privacyshield.gov/welcome>

<sup>134</sup> National Public Radio, “A year after San Bernadino and Apple-FBI, where are we on encryption?”, 3 December 2016, available at <https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption?t=1532518316108>

<sup>135</sup> For example, Australia’s Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, available at <https://www.legislation.gov.au/Details/C2018A00148>

<sup>136</sup> U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act, H.R. 4943).

<sup>137</sup> Brave automatically blocks ad trackers (ad trackers collect data from users’ online behaviours for the purpose of boosting the effectiveness of ads and marketing campaigns). DuckDuckGo does not track user search behaviours.

<sup>138</sup> UK Open Data Institute, “UK’s first ‘data trust’ pilots to be led by the ODI in partnership with central and local government”, 20 November 2018, available at <https://theodi.org/article/uks-first-data-trust-pilots-to-be-led-by-the-odi-in-partnership-with-central-and-local-government/>

<sup>139</sup> India Stack, “About Data Empowerment and Protection Architecture”, available at <https://indiastack.org/depa/>

<sup>140</sup> United Nations Secretary-General, Address to the General Assembly, 25 September 2018, available at <https://www.un.org/sg/en/content/sg/speeches/2018-09-25/address-73rd-general-assembly>

<sup>141</sup> Mareike Möhlmann and Andrea Geissinger, *Trust in the Sharing Economy: Platform-Mediated Peer Trust* (Cambridge University Press, July 2018), available at [https://www.researchgate.net/publication/326346569\\_Trust\\_in\\_the\\_Sharing\\_Economy\\_Platform-Mediated\\_Peer\\_Trust](https://www.researchgate.net/publication/326346569_Trust_in_the_Sharing_Economy_Platform-Mediated_Peer_Trust)

<sup>142</sup> European Political Strategy Centre, “Report from the High Level-Hearing: Preserving Democracy in the Digital Age”, 22 February 2018, available at [https://ec.europa.eu/epsc/sites/epsc/files/epsc\\_-\\_report\\_-\\_hearing\\_on\\_preserving\\_democracy\\_in\\_the\\_digital\\_age.pdf](https://ec.europa.eu/epsc/sites/epsc/files/epsc_-_report_-_hearing_on_preserving_democracy_in_the_digital_age.pdf)

<sup>143</sup> The Guardian, “You thought fake news was bad? Deep fakes are where truth goes die”, 12 November 2018, available at: <https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth>

<sup>144</sup> Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Houghton Miller Harcourt, 2018), available at <https://aisuperpowers.com/>

<sup>145</sup> Here capacity is understood as “the ability of people, organizations, systems of organizations, and society as a whole to define and solve problems, make informed choices, order their priorities, plan their futures, and to implement programmes and projects to sustain them.” See Swiss Agency of Development and Cooperation, “Glossary Knowledge Management and Capacity Development”, available at <https://bit.ly/2FwORDI>

<sup>146</sup> 5Rights Foundation, “5Rights Partner with BT to Co-Create with Children on Digital Literacy”, 2017, available at <https://5rightsfoundation.com/in-action/5rights-partner-with-bt-to-co-create-with-children-on-digital-literacy.html>

<sup>147</sup> United Nations Volunteers, “Shape the Future of Volunteering: Online Conversations”, 25 April 2019, available at <https://www.unv.org/planofaction/dialogues>

<sup>148</sup> The Times of India, “Fake news: WhatsApp, DEF host training for community leaders in Jaipur”, 19 November 2018.

<sup>149</sup> The “security by design” approach is described in the 2015 White Paper of Amazon Web Services, available at [https://www.logicworks.com/wp-content/uploads/2017/01/Intro\\_to\\_Security\\_by\\_Design.pdf](https://www.logicworks.com/wp-content/uploads/2017/01/Intro_to_Security_by_Design.pdf); the EU General Data Protection Regulation (GDPR) contains the “privacy by design” principle; some examples of what it means in practice are available at [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en).

<sup>150</sup> European Commission, *Final Report of the High Level Expert Group on Fake News and Online Disinformation*, 12 March 2018, available at <https://ec.europa.eu/digital-single-market/en/news/final-report-high->



[level-expert-group-fake-news-and-online-disinformation](#); Facebook, “Protecting Elections in the EU”, 28 March 2019.

<sup>151</sup> See for example Joseph Nye, “Nuclear Learning and U.S.-Soviet security regimes”, International Organization, 41, 3, (1987), p. 371-402; Emmanuel Adler, “The emergence of cooperation: national epistemic communities and the international evolution of the idea of nuclear arms control”, International Organization, 46, (1992), p. 101-145; Clifton Parker, “Cooperation of U.S., Russian Scientists Helped Avoid Nuclear Catastrophe at Cold War’s End, CISAC Scholar Says”, June 28, 2016, available at <https://cisac.fsi.stanford.edu/news/cooperation-us-russian-scientists-helped-avoid-nuclear-catastrophe-cold-war%E2%80%99s-end-says-cisac>

<sup>152</sup> World Economic Forum, The Global Risks Report 2019, 15 January 2019, available at <https://www.weforum.org/reports/the-global-risks-report-2019>

<sup>153</sup> World Economic Forum Global Risks Perception Survey 2018-2019.

<sup>154</sup> WIRED, “That Insane, \$81m Bangladesh Bank Heist? Here’s What We Know”, 17 May 2016, available at <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>

<sup>155</sup> CBS, “What can we learn from the ‘most devastating’ cyberattack in history?”, 22 August 2018, available at <https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/>

<sup>156</sup> Bromium, Inc., “Hyper-Connected Web Of Profit Emerges, As Global Cybercriminal Revenues Hit \$1.5 Trillion Annually”, 20 August 2018, available at <https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/>

<sup>157</sup> Business Insider, “Travis Kalanick lasted in his role for 6.5 years — five times longer than the average Uber employee”, 20 August 2017, available at <https://www.businessinsider.com/employee-retention-rate-top-tech-companies-2017-8>

<sup>158</sup> Symantec, Internet Security Threat Report, April 2016, available at <https://www.nu.nl/files/nutech/Rapport-Symantec2016.pdf>

<sup>159</sup> Europol’s Internet Organised Crime Threat Assessment (IOCTA) 2018 has a summary of the evolving threat environment; Japan’s National Institute of Information and Communications Technology (NICT) estimates on the basis of scans of the darknet that 54% of the attacks it detected in 2017 targeted IoT devices: see NICT, “The ‘NOTICE’ Project to Survey IoT Devices and to Alert Users”, 1 February 2019.

<sup>160</sup> IOT Analytics, “State of the IoT 2018, Number of IoT devices now at 7B – Market accelerating”, 08 August 2018, available at <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>

<sup>161</sup> CBS, “Stuxnet: Computer Worm Opens Era of Warfare”, 04 June 2012, available at <https://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/>

<sup>162</sup> CNN, “US announces new set of Russia Sanctions”, 20 December 2018, available at <https://edition.cnn.com/2018/12/19/politics/us-treasury-russia/index.html>; The New York Times, “Signs of Russian Meddling in Brexit Referendum”, 15 November 2017, available at <https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html>

<sup>163</sup> Gail Kent, Stanford Law School Center for Internet and Society, “The Mutual Legal Assistance Problem Explained”, 23 February 2015, available at <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained>

<sup>164</sup> Bloomberg, “Huawei Reveals the Real Trade War with China”, 6 December 2018; Associated Press, “German leader Angela Merkel testifies on alleged U.S. surveillance revealed by Snowden, 16 February 2017 and “Costs of Snowden leak still mounting 5 years later”, 4 June 2018.

<sup>165</sup> TechRepublic, “Governments and nation states are now officially training for cyberwarfare: An inside look”, 1 September 2016, available at <https://www.techrepublic.com/article/governments-and-nation-states-are-now-officially-training-for-cyberwarfare-an-inside-look/>

<sup>166</sup> The Wall Street Journal, “Cyberwar Ignites a New Arms Race”, 11 October 2015; The Wall Street Journal, “Cataloging the World’s Cyberforces”, 11 October 2015.

<sup>167</sup> The Register, “Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide”, 28 June 2017.

<sup>168</sup> IBM researchers have shown it is possible to conceal known malware in video-conferencing software and trigger it when it sees a specific individual, available at <https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/>

<sup>169</sup> Russia placed information security on the agenda of the UN in 1998. Since then several Groups of Governmental Experts have studied ICT security and three of them have adopted reports by consensus. See <https://www.un.org/disarmament/ict-security/> and [https://www.diplomatie.gouv.fr/IMG/pdf/paris\\_call\\_cyber\\_cle443433-1.pdf](https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf)

<sup>170</sup> They are composed on the basis of equitable geographical distribution, and each has included the five permanent members of the UN Security Council.

<sup>171</sup> UN GGE report of 2013 (A/68/98), paragraph 19, available at <https://undocs.org/A/68/98>; reconfirmed by the UN GGE report of 2015 (A/70/174), paragraph 24, available at <https://undocs.org/A/70/174>

<sup>172</sup> United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, report A/70/174, page 13, 22 July 2015, available at <http://undocs.org/A/70/174>

<sup>173</sup> Government of France, “Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace”, available at <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in>

- <sup>174</sup> Cybersecurity Tech Accord, available at <https://cybertechaccord.org>; Siemens, Charter of Trust, available at <https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf>
- <sup>175</sup> The case has been made strongly in recent studies such as Samir Saran (ed.), *Our Common Digital Future* (GCCS and ORF, 2017), available at <https://www.orfonline.org/research/our-common-digital-future-gccs-2017/>
- <sup>176</sup> United Nations General Assembly, “Advancing responsible State behaviour in cyberspace in the context of international security”, 18 October 2018, available at <https://undocs.org/A/C.1/73/L.37>
- <sup>177</sup> United National General Assembly, “Developments in the field of information and telecommunications in the context of international security”, 29 October 2019, available at <https://undocs.org/A/C.1/73/L.27/Rev.1>
- <sup>178</sup> Oman ITU-Arab Regional Cybersecurity Centre, available at <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.aspx>
- <sup>179</sup> CSIRTs Network, available at <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network>
- <sup>180</sup> Cathy Mulligan, “A Call to (Software) Arms”, LinkedIn, 30 March 2019.
- <sup>181</sup> International Organization for Standardization, ISO/IEC 27034, 2011; SAFECode, *Fundamental Practices for Secure Software Development*, March 2018, available at [https://safecode.org/wp-content/uploads/2018/03/SAFECode\\_Fundamental\\_Practices\\_for\\_Secure\\_Software\\_Development\\_March\\_2018.pdf](https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf); SAFECode, *Managing Security Risks Inherent in the Use of Third-Party Components*, 2017, available at [https://www.safecode.org/wp-content/uploads/2017/05/SAFECode\\_TPC\\_Whitepaper.pdf](https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf); SAFECode, *Tactical Threat Modeling*, 2017, available at [https://www.safecode.org/wp-content/uploads/2017/05/SAFECode\\_TM\\_Whitepaper.pdf](https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TM_Whitepaper.pdf); and Microsoft, *Security Development Lifecycle*. Microsoft, available at <https://www.microsoft.com/en-us/securityengineering/sdl>.
- <sup>182</sup> The Global Cybersecurity Capacity Centre at Oxford University has created a repository of existing efforts in partnership with the GFCE: the Cybersecurity Capacity Portal, available at <https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce>. The report “Cybersecurity Competence Building Trends” provides examples of public-private partnerships in OECD countries: see Diplo, *Cybersecurity Competence Building Trends*, 2016.
- <sup>183</sup> Cybersecurity Ventures, “Cybersecurity Jobs Report 2018-2021”, 31 May 2017, available at <https://cybersecurityventures.com/jobs/>. The Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building provides a framework for such efforts: see GFCE, *Delhi Communiqué*, 2017, available at <https://www.thegfce.com/delhi-communication>
- <sup>184</sup> OECD, “Unlocking the potential of e-commerce”, OECD Going Digital Policy Note, OECD, Paris, 2019, available at [www.oecd.org/going-digital/unlocking-the-potential-of-e-commerce.pdf](http://www.oecd.org/going-digital/unlocking-the-potential-of-e-commerce.pdf). Page 2 notes that “SMEs could also benefit from multistakeholder initiatives such as the Electronic World Trade Platform, which aims to foster a more effective policy environment for online trading”.
- <sup>185</sup> In the areas of cybersecurity and cybercrime, for example, national laws and regional and international conventions create frameworks for digital cooperation in addressing cyber-risks. One example is the Council of Europe Cybercrime Convention, available at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- <sup>186</sup> Content policy is one area where there are many examples of “soft law” instruments, such as the “Code of conduct on countering illegal hate speech online” (agreed in 2016 by the European Commission and major internet companies; available at [https://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=54300](https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300)), the “Manila Principles on Internet Intermediaries” (developed in 2015 by the Electronic Frontier Foundation and other civil society groups and endorsed by many entities, available at <https://www.manilaprinciples.org>), and the “Guidelines for industry on child protection online” (initially developed in 2015 through a consultative process led by the International Telecommunication Union and UNICEF, available at [https://www.unicef.org/csr/files/COP\\_Guidelines\\_English.pdf](https://www.unicef.org/csr/files/COP_Guidelines_English.pdf)).
- <sup>187</sup> The Internet Governance Forum can be seen as a loosely organised framework for digital cooperation (more details at <https://www.intgovforum.org/multilingual/tags/about>), while the Internet Corporation for Assigned Names and Numbers (with its multiple advisory committees and supporting organisations) can be seen as a more institutionalised framework (more details at <https://www.icann.org/resources/pages/groups-2012-02-06-en>).
- <sup>188</sup> The Internet Engineering Task Force, for example, develops technical standards for the internet (more details at <https://www.ietf.org/standards/>), while the European Commission’s High Level Group on Internet Governance has the role of facilitating coordination among EU member states on internet governance issues (more details at <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2450>).
- <sup>189</sup> See Anderson, C., *Cyber Security and the Need for International Governance* (Southern University Law Center 24 April 2016).
- <sup>190</sup> Paragraph 72 of the WSIS Agenda lists this and other functions of the IGF. Available at <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>
- <sup>191</sup> NETmundial, “NETmundial Multistakeholder Statement”, April 2014, available at <http://netmundial.br/netmundial-multistakeholder-statement/>
- <sup>192</sup> Global Commission on Internet Governance, “One Internet”, June 2016, available at <https://www.cigionline.org/publications/one-internet>
- <sup>193</sup> World Wide Web Foundation, “Contract for the Web”, available at <https://contractfortheweb.org>
- <sup>194</sup> Government of France, “France and Canada Create new Expert International Panel on Artificial Intelligence”, 7 December 2018, available at <https://www.gouvernement.fr/en/france-and-canada-create-new-expert-international-panel-on-artificial-intelligence>

<sup>195</sup> In 2016, at the G20 Summit in Hangzhou the G20 leaders adopted a “G20 Digital Economy Development and Cooperation Initiative”, available at <https://www.mofa.go.jp/files/000185874.pdf>. Annual G20 Digital Economy Ministerial Meetings have been held since 2017.

<sup>196</sup> UN Secretary-General António Guterres, Address to the Internet Governance Forum 2018, available at <http://www.intgovforum.org/multilingual/content/igf-2018-address-to-the-internet-governance-forum-by-un-sg-ant%C3%B3nio-guterres>

<sup>197</sup> Many documents and publications released over the past decade underline the need for better inclusion of underrepresented communities in internet governance and digital policy processes. Examples include the report of the Working Group on Improvements to the Internet Governance Forum, 2012, available at [https://unctad.org/meetings/en/SessionalDocuments/a67d65\\_en.pdf](https://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf), and the NetMundial Multistakeholder Statement, 2014, available at <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>. ICANN has also recognised the need for better inclusion of under-represented communities and is working on addressing this through initiatives such as its Fellowship Program (more details at <https://www.icann.org/fellowshipprogram>).

<sup>198</sup> According to the updated estimate of the 2014 UNCTAD study, there are more than 680 digital cooperation mechanisms developed and used by governments, businesses, technical and international organisations. See United Nations Commission Mapping of International Internet Public Policy Issues, E/CN.16/2015/CRP.2, 17 April 2015, available at [https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2\\_en.pdf](https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf)

<sup>199</sup> One recent example is the impact of the introduction of the GDPR on ICANN’s policies concerning the collection and publication of domain name registration data. When the GDPR requested that data on EU registrants be made private, ICANN was unprepared to adapt its so-called WHOIS policies to the new EU regulation. A coordination mechanism for interdisciplinary policy approaches could have helped ICANN be better prepared for the GDPR.

<sup>200</sup> CSIS, “Economic Impact of Cybercrime – No Slowing Down”, February 2018, available at <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf>

<sup>201</sup> Cybersecurity Ventures, 2017 Cybercrime Report, 2017.

<sup>202</sup> Digital Full Potential, “Artificial Intelligence Market Size Projected to Be \$60 Billion by 2025”.

<sup>203</sup> MarketWatch, “The Global Artificial Intelligence (AI) Market by Technology and Industry Vertical - A \$169.4 Billion Opportunity by 2025 - ResearchAndMarkets.com”, 24 August 2018.

<sup>204</sup> WSIS, available at <https://www.itu.int/net/wsis/>; UNESCO ROAM Principles, available at

<https://en.unesco.org/internetuniversality/indicators>; NETmundial, available at <https://netmundial.org/>

<sup>205</sup> The IGF Plus proposal builds on previous policy and academic discussions on strengthening the Internet Governance Forum, including: Report of the Working Group on Improvements to the Internet Governance Forum, 2012, available at [https://unctad.org/meetings/en/SessionalDocuments/a67d65\\_en.pdf](https://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf); Milton Mueller and Ben Wagner, “Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance,” Internet Policy Observatory, February 2014, available at <https://global.asc.upenn.edu/app/uploads/2014/09/Finding-a-Formula-for-Brazil-Representation-and-Legitimacy-in-Internet-Governance.pdf>; IGF Retreat Proceedings: Advancing the 10-Year Mandate of the Internet Governance Forum, July 2016, New York, available at <https://www.intgovforum.org/multilingual/content/igf-retreat-documents>; Wolfgang Kleinwächter, “The Start of a New Beginning: The Internet Governance Forum on Its Road to 2025”, CircleID, 3 April 2016, available at [http://www.circleid.com/posts/20160403\\_start\\_of\\_a\\_new\\_beginning\\_the\\_internet\\_governance\\_forum/](http://www.circleid.com/posts/20160403_start_of_a_new_beginning_the_internet_governance_forum/); Raúl Echeberria, “Let’s Reform the IGF to Ensure Its Healthy Future”, Internet Society blog, 17 March 2018, available at <https://www.internetsociety.org/blog/2018/03/lets-reform-igf-ensure-healthy-future/>; the WSIS Tunis Agenda for the Information Society, Tunis, United Nations, available at <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>. In addition to the IGF, the other outcomes of the WSIS process are action line follow-ups (WSIS Forum), system-wide follow-up (UN CSTD), and enhanced cooperation.

<sup>206</sup> As of 31 May 2019 there were 82 national, 17 regional and 16 youth Internet Governance Forums.

<sup>207</sup> This approach was developed by the World Bank and 4IRC. In Singapore, the Technology Office of the Prime Minister developed mechanisms that enable continuity, dialogue, feedback loops, and agility in decision-making, particularly in relation to experimentation or piloting of new technologies.

<sup>208</sup> On the applicability of the concept of global public good to the internet please refer to

<https://www.diplomacy.edu/calendar/internet-global-public-resource>

<sup>209</sup> Malta proposed that the UN consider the internet as a common heritage of mankind. See Statement by Dr. Alex Sceberras Trigona, Special Envoy of the Prime Minister of Malta, World Summit on Information Society Review Process, New York, 15 November 2015, available at [https://www.academia.edu/19974250/Protecting\\_the\\_Internet\\_as\\_Common\\_Heritage\\_of\\_Mankind](https://www.academia.edu/19974250/Protecting_the_Internet_as_Common_Heritage_of_Mankind)

<sup>210</sup> The data commons idea has emerged over the past year at the ITU’s AI for Good Summit and the World Government Summit. See <https://news.itu.int/roadmap-zero-to-ai-and-data-commons/> and <http://the-levant.com/uae-world-leader-ai-global-data-commons-roundtable>

<sup>211</sup> Members of the International Chamber of Commerce pay an annual membership fee, set either by ICC national committees (where they exist) or by the ICC itself (for direct members). More details at <https://iccwbo.org/become-a-member/joining-icc-direct-member/>

<sup>212</sup> United Nations Secretary-General’s Task Force on Digital Financing of the SDGs, available at <https://digitalfinancingtaskforce.org/>

<sup>213</sup> One of the first regulatory sandboxes was launched in 2015 in the UK; at the beginning of 2018, there were more than 20 jurisdictions actively implementing or exploring the concept. See Briefing by UN Secretary-

---

General's Special Advocate for Inclusive Finance, available at <https://www.unsgsa.org/files/1915/3141/8033/Sandbox.pdf>

<sup>214</sup> We understand 'inclusion' to be more than simple participation of a few 'missing actors' in digital events. Meaningful representation requires bottom-up capacity development, preparatory discussions and inter-ministerial coordination at the national level.