3

Vector of hope, source of fear

BY ROBERTO BISSIO, SOCIAL WATCH

The 2030 Agenda is enthusiastic about the "great potential" for accelerating human progress brought by information and communications technology and global interconnectedness. At the same time, however the UN now acknowledges "the dark side of innovation" and the new challenges of cybersecurity threats, the risks to jobs and privacy unleashed by artificial intelligence and the use of military related 'cyber operations' and cyber-attacks.

As with climate change, increasing inequalities or power concentration, those challenges cannot be solved by countries acting in isolation and urgently require strengthened multilateralism.

At the same time, a major technological shift is necessary to implement the global transition - required by the 2030 Agenda - towards less resource-intensive and more resilient economic and social development models. Most of that technology already exists, but new strategies are needed to generalize it at global level.

"Technology is transforming how we live and work – from bio-engineering to synthetic biology to artificial intelligence to data analytics and to many other aspects" said UN Secretary-General António Guterres in a recent speech.[1] Yet, he added, "as much as technology is a vector of hope, it is also a source of fear."

In acknowledging this, Guterres also called on Member States to "address the dark side of innovation". This is a significant shift, since new technologies have appeared in the official discourse on sustainable development only as embodying progress and encouraging optimism.

Guterres made clear those issues are not isolated, since "as long as we cling to an economic and social model that drives exclusion and environmental destruction, people die, opportunities are missed, the seeds of division and future conflicts are sown and the full force of climate change becomes ever more likely."

Those are deep and remarkably candid concepts that go beyond the usual enthusiasm about innovation. In 2015, the 2030 Agenda adopted at the highest level by UN Member States, stated that "the spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies, as does scientific and technological innovation across areas as diverse as medicine and energy".[2] Simultaneously, a joint report by The Earth Institute of Columbia University and the Swedish telecommunications company Ericsson found that "in essence, ICTs are ‚leapfrog' and transformational technologies, enabling all countries

1 United Nations (2018).

2 United Nations (2015), para. 15.

to close many technology gaps at record speed."[3] Not a word about potential dangers, whereas now "the downsides of technology's inexorable march are becoming clear" to the point that a "neo-Luddism" is seen by some analysts as emerging.[4]

Box 3.1

Half of humanity is NOT online

If the spread of ICTs only brings good things there is no need to regulate it and the only question is how to accelerate its expansion so that everybody in the world can benefit from it. Thus, under SDG 9 on industrialization and innovation, target 9.c commits to „significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020."

This formulation is a bit awkward. It seems to imply that there would be complete world coverage by 2020, if even the poorest countries have universal access by then. But since a majority of the people living in poverty are citizens of G20 countries, the forecast by Cisco is that by 2020 only half of the world population will be online (4.1 billion Internet users, of a total population of 8 billion). By that date, the number of connected devices will have surpassed 26 billion, thanks to the fast expansion of the "Internet of Things".[1]

1 Cisco (2017).

Hands-off...

The Internet started in the 1970s as a research project funded mainly by the US Department of Defense and the National Science Foundation. In 1995, the US government announced it was ending its subsidies to the operation of the Internet backbone and, simultaneously allowed commercial use of the network, previously restricted to educational and research purposes.

Governments were supposed to better serve the global public interest by keeping their hands off cyberspace. The network expanded at fast speed and quite soon came to be described as a "global public good".[5] Yet, keeping with the hands-off spirit, the only decision that governments collectively made over the new realm was the 1998 declaration of the World Trade Organization (WTO) stating that members "will continue their current practice of not imposing customs duties on electronic transmissions".[6] Thus, a disk carrying videos, music or software can be subjected to a customs tariff when crossing borders, but that same content being transmitted to a paying consumer by Netflix or iTunes continues to remain untaxed.

The technical difficulties in controlling the cross-border flow of data (short of a total communications shut down) added an element of necessity to that decision, as in "if you can't beat them, join them".

The value of cross-border data flows, which was insignificant when the decision not to tax them was

3 Earth Institute/Ericsson (2015), p. 2.

4 Bartlett (2018).

5 Kaul et al. (1999).

6 WTO (1998).

taken, is growing exponentially. In 2014, the USA exported US$ 399.7 billion and imported US$ 240.8 billion in digitally deliverable services. That surplus is even bigger if we add the digital delivery of services through affiliates of U.S. companies located abroad. In 2011, U.S. affiliates in Europe sold digital services for US$ 312 billion.[7] Total cross-border online purchases of physical goods, meanwhile, was estimated by UNCTAD to be US$ 189 billion in 2015, a mere 1.1 percent of total merchandise imports.[8] 93 percent of global e-commerce is still domestic.

That US economic advantage helps explain their support to the idea of cyberspace as a separate realm, where no (other) government should exercise authority (including taxation). Yet, cyberspace is just a metaphor. All devices exist somewhere and all information is stored somewhere, no matter how fast it might circulate. The difficulties (and sometimes impossibility) faced by duty-bearers to fulfill their responsibilities towards rights-holders (starting with their own citizens) does not dilute rights or obligations, it only emphasizes the need to multilaterally deal with the threats identified by Secretary-General Guterres. Without addressing those threats, ICTs could become obstacles to achieving the 2030 Agenda instead of contributing to its achievement.

Cybersecurity threats

In a blog published in March 2018 by the Rand Corporation, a think tank created in 1948 by Douglas Aircraft Company to offer research and analysis to the US Armed Forces, Isaac R. Porche argues that "nation-states and their proxies are spying and attacking in cyberspace across national borders with regularity".[9] The indictment of 13 Russian citizens in the USA for attempting to interfere in the 2016 election is offered as an example, together with the indictment of seven Iranian nationals in 2012 for installing malicious code on a computer that controls a dam in New York State and of a number of Chinese hackers accused of stealing from US companies in November 2017.

Steve Ranger, UK editor-in-chief of the specialized website ZDNet notices however, that the country with "the most significant cyber defense and cyber-attack capabilities" is the USA.[10] During the G20 Summit in Hangzhou, China in 2016, US President Barack Obama said, „We're moving into a new era here, where a number of countries have significant capacities. And frankly we've got more capacity than anybody, both offensively and defensively."[11]

The distinction between offensive and defensive tools is, in this case, rhetorical. In 2014, Dan Geer, a security expert from the Massachusetts Institute of Technology and advisor to the CIA , published an essay on "Cybersecurity as Realpolitik," basically demonstrating that "all cybersecurity technology is dual use".[12] Geer emphasized that "perhaps dual use is a truism for any and all tools from the scalpel to the hammer to the gas can – they can be used for good or ill – but I know that dual use is inherent in cybersecurity tools." The corollary of that perception is that "offense is where the innovations that only States can afford is going on." Needless to say, very few States can afford the enormous investment in equipment and research required to develop these capabilities.

The US Department of Defense considers cyberspace as its fifth realm of operations, after land, sea, air and space. Its current Law of War Manual includes a long chapter on cyber operations, which it defines as operations as those that "use computers to disrupt, deny, degrade, or destroy information…or the computers and networks themselves" if they have "a primary purpose of achieving objectives or effects in or through cyberspace" usually preceding or supporting the main military assault, but carefully excluding from the definition the use of computers "to facilitate command and control" or "operations to distribute information broadly using computers…."[13]

This is an important distinction, because the UN Charter and international law ban the use of force

7 Nicholson (2016).
8 UNCTAD (2017).
9 Porche (2018).
10 Ranger (2017).
11 White House (2016).
12 Geer (2014).
13 US Department of Defense (2015), p. 995.

except in two situations, self-defense and explicit actions agreed upon by the Security Council. The US Defense Department states clearly that "the term ‚attack' often has been used in a colloquial sense in discussing cyber operations to refer to many different types of hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services". Operations described as 'cyber attacks' or 'computer network attacks,' therefore, are not necessarily 'armed attacks' for the purposes of triggering a State's inherent right of self-defense under *jus ad bellum*."[14]

That the US Defense Department goes to such lengths in limiting potentially escalating hostilities and counter hostilities in cyberspace can be seen both as an attempt to only retort to force as a last resort, as required by the UN Charter, or could also be seen as making sure that operations regularly carried out in cyberspace by the National Security Agency (NSA) of the Defense Department are not defined as 'casus belli' that could legitimize other powers' retaliation.

The idea of promoting international collaboration on cybersecurity or on regulating (and ultimately outlawing) cyberwar has been appearing at different fora for at least a decade. The difficulties are enormous. The two obstacles most frequently raised are the complexities linked to determining what would constitute a cyber weapon (as opposed to software for peaceful purposes, including that of defense against cyber attacks) and to the difficulties of verification.

In practically all of the cases cited as cyber attacks that have reached the public, not only is the exact location of the origin questionable, but also the attribution to a State or to an independent group is debatable.

Activities not carried out by States but by individuals or private groups cannot strictly qualify as 'warfare', but since the origin of the attacks might be difficult to attribute in cyberspace, the UN Interregional Crime and Justice Research Institute seems to lean towards a definition of cyberwarfare as including 'cyberhooliganism', 'cybervandalism', and 'cyberterrorism'.[15]

But the analogy between weapons of mass destruction and cyber weapons can be misleading. While no government would even think of using atomic bombs on their own populations, the same military agencies that prepare (and most likely also conduct) cyber attacks are systematically using those tools on their own citizens. As national borders are diluted in cyberspace, the issues of peace and basic human rights merge. And they are both indispensable to achieving the SDGs because "there can be no sustainable development without peace and no peace without sustainable development".[16]

The revelations by Edward Snowden of the magnitude of mass surveillance conducted by intelligence agencies led the UN General Assembly to adopt a Resolution on the Right to Privacy in the Digital Age,[17] in which it expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. The General Assembly affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communications. The Office of the High Commissioner on Human Rights concluded that "(D)omestic oversight mechanisms, where they exist, often are ineffective as they fail to ensure transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."[18]

The Human Rights Council created the mandate of a Special Rapporteur on the right to privacy and Professor Joseph Cannataci, from Malta, was appointed in July 2015. In his report to the Human Rights Council in March 2018, Cannataci recommends the creation of an international Legal Instrument on Government

14 Ibid. (2015), p. 996.

15 See: www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations/

16 United Nations (2015), Preamble.

17 United Nations (2013).

18 UN OHCHR (2018), para. 6.

Led Surveillance with legal authority to balance the legitimate security needs of governments with their obligations to protect human rights.[19]

Data as the new oil

Surveillance by a State (whether one's own or not) is not the only threat to privacy. Corporations running digital platforms are increasingly obtaining, processing and re-selling information about people in ways that extend any authorization users may have given, might infringe on their rights – and makes those platforms enormously rich and powerful.

On the one hand, the open nature of the Internet (anybody can access without requesting authorization) and its neutrality (all traffic is treated as equal, a principle now being challenged in the USA) is a democratizing factor: anybody can publish, buy or sell on equal terms and millions of people have found a channel to make themselves heard or access markets that were out of their reach before. At the same time, a handful of powerful players (Google, Amazon, Facebook, Apple, collectively known as GAFA, now GAFA-A with the addition of the Chinese Alibaba) concentrate enormous power. Google knows that you're sick before you call the doctor, Amazon brags that your next delivery is being packed before you buy it and Facebook has experimented with controlling your moods by offering you good or bad news.

UK mathematician and market analyst Clive Humby stated in 2006 that "data is the new oil".[20] And just like oil, data needs to be processed for it to become valuable gas or plastic. And one could add that just like oil, those that refine and sell it benefit from it more than those from where it is extracted. Awareness of that situation is leading some groups to propose that individuals or communities should be compensated for the value generated from data they provide,[21] while many countries are considering ways to exert 'data sovereignty' (see Box 3.2).

19 Human Rights Council (2018).

20 Palmer (2006).

21 Tarnoff (2018).

Box 3.2

Data sovereignty

BY IT FOR CHANGE[1]

In a platformizing economy, e-commerce platforms need to be understood not merely as marketplaces, but also as digital ecosystems that provide a new architecture for the economy. Platforms like Amazon orchestrate and control entire market ecosystems comprising providers, producers, suppliers and consumers/users.[2]

E-commerce companies bank on the data produced through their ecosystem for generating value, using such data to create the hold-all digital intelligence to completely transform the DNA of the market and attain a position of dominance. Amazon may have started out as an online book retailer, but it has become a 'super platform', a monopsony extending itself across and beyond its ecommerce portal to providing cloud services, a digital wallet, video

1 Extracted from the Submission to UNCTAD's Intergovernmental Group of Experts on E-Commerce and the Digital Economy by members of the Research Network on Policy Frameworks for Digital Platforms - Moving from Openness to Inclusion, led by Anita Gurumurthy, Geneva, April 2018. The complete text is available at: http://unctad.org/meetings/en/Contribution/tdb_ede2018_c03_ITforChange_en.pdf

2 See: www.itforchange.net/sites/default/files/1516/Platform_Policies_Research_Framework2018.pdf

on-demand service and devices.[3]

Developing countries need to recognize that in the datafying economy, any step towards creating a level playing field for local platforms must foreground and tackle the question of data in digital trade regimes. The discourse of free data flows is premised upon the economic value of data and possibilities for innovation that a global data regime can give rise to. However, developing nations are the mining grounds for data, at worst, and the back offices or server farms for low-end data processing, at best. Even nations that have distinguished themselves as tech hubs often develop innovation products and services only to release intellectual control[4] and economic dividends to the tech giants of the global North. Thus, the free data flows discourse disregards the unequal footing[5] on which 'intelligence rich' and 'intelligence poor' nations compete.

Fostering local platforms is not about simplistic fixes that come from pre-digital thinking. Data sovereignty and control over data of critical sectors is vital for businesses and governments in the global South so that they can truly benefit from possibilities in e-commerce/ digital trade. Public support is necessary to catalyse and enable local market ecosystems in which small and marginal players can compete. This involves not only creating open and public data sets that are available for public and commercial uses, but also support in the form of public digital intelligence infrastructure.

Moreover, an agile legal and policy framework to curb platform excess is the need of the hour. The global South risks becoming an unregulated innovation playground for technology giants to experiment in if adequate and comprehensive policy measures are not developed that can govern their operations. Critical policy frontiers such as labour, consumer protection, privacy, foreign investments and other areas that directly impact the livelihood rights of citizens and platform users cannot be conceded to immediate short term gains that big platforms often usher in.

Dubious contracts, Terms of Service and privacy policies emanating from platforms should not do the heavy lifting for state developed well-rounded policy frameworks. Mandating that platform companies share some of the data they collect with public agencies in key sectors is important for curbing their anti-competitive practices and promoting the space for smaller local start-ups or innovators to use these data sets for coming up with their own innovative niche products.

3 See: www.forbes.com/sites/gregpetro/2017/08/02/amazons-acquisition-of-whole-foods-is-about-two-things-data-and-product/#740451d7a808

4 See: www.forbes.com/sites/venkateshrao/2012/09/03/entrepreneurs-are-the-new-labor-part-i/#36a53d3f4eab

5 See: www.itforchange.net/index.php/grand-myth-of-cross-border-data-flows-trade-deals

Jobs: threats and hopes

Since the first industrial revolution, machines have both destroyed jobs and created new ones. The net result is a productivity increase and the big social and political question is how those gains are distributed in society.

But the spread of ICTs does not only substitute machines for human labour, it also facilitates the splitting of complex jobs into multiple minor tasks and distributing them around the world through digital labour platforms in which clients post jobs and workers bid on them. The market for digital work was US$ 4.8 billion in 2016, and it is growing at a rate of 25 percent a year. [22] An estimated 112 million workers are offering their services in that market, but only

22 Graham et al. (2017).

one out of ten completed at least one paid task in the year.

Millions of unemployed graduates hope to transcend some of the constraints of their local labour markets, and compete globally for tasks such as translations, transcriptions, lead generation, marketing, data entry and personal assistance. With globalization so far widening the global reach of capital at the cost of place-bound labour, this could mean that not just capital, but also labour can compete in a global market. In practice, however, since the offer of labour that is ten times greater than actual demand, digital workers have little bargaining power. Workers are classified as independent contractors and in cross-borders transactions the confusion as to which labour legislation to apply usually results in that no social protection whatsoever is in place.

Empirical studies have showed that instead of a frictionless economy, between employers in high-income countries and workers in developing countries (mainly India, the Philippines, Pakistan and Bangladesh) "intermediaries use geographic location, networks, and other positional advantages to mediate between buyers and sellers, potentially contributing to (and reinforcing) global inequalities".[23]

Nevertheless, "governments like those of Nigeria, Malaysia and the Philippines, and large organizations like the World Bank, are increasingly coming to view digital labour as a mechanism for helping some of the world's poorest escape the limited opportunities for economic growth in their local contexts".[24] The benefits that some workers actually obtain should not obscure the intrinsic inequality in this market, emphasized by the role of the platforms that intermediate. Digital work is only one of the aspects in which the new technologies are transforming the future of work, but to envision alternatives and strategies for this extreme form of cross-border human relations is necessary to bring a fairer world of work into being everywhere.

23 Ibid., p. 149.

24 Ibid., pp. 158-159.

Box 3.3

Machines (algorithms) are already deciding our future

BY PRABIR PURKAYASTHA[1]

Machine algorithms are taking over decisions that were made by governments, business and even ourselves.

Today, algorithms decide who should get a job, which part of a city needs to be developed, who should get into a college, and in the case of a crime, what should be the sentence. It is not the super intelligence of robots that is the threat to life as we know it, but machines taking over thousands of decisions that are critical to people's lives and deciding social outcomes.

What decides you getting a loan or not is finally a machine score – not who you are, what you have achieved, how important is your work for the country (or society); for the machine, you are just the sum of all your transactions to be processed and reduced to a simple number. The worst part is that some of the algorithms are not even understandable to those who have written them; even the creators of such algorithms do not know how a particular algorithm came out with a specific score!

Mathematician and data scientist Cathy O'Neil, in recent a book, "Weapons of Math Destruction", tells us that the apparent objectivity of processing the huge amount of data by algorithms is false. The algorithms themselves are nothing but our biases and subjectiveness that are being coded – "They are just opinions coded into maths."

1 A longer version was originally published on https://newsclick.in/.

What happens when we transform the huge amount of data that we create through our everyday digital footprints into machine 'opinions' or 'decisions'? Google served ads for high-paying jobs disproportionately to men; African Americans got longer sentences as they were flagged as high risk for repeat offences by a judicial risk assessment algorithm. It did not explicitly use the race of the offender, but used where they stayed, information about other family members, education and income to work out the risk, all of which put together, was also a proxy for race.

The problem is not just the subjective biases of the people who code the algorithms, or the goal of the algorithm, but much deeper. They lie in the data and the so-called predictive models we build using this data. Such data and models simply reflect the objective reality of the high degree of inequality that exist within society, and replicates that in the future through its predictions.

What are predictive models? Simply put, we use the past to predict the future. We use the vast amount of data that are available, to create models that correlate the 'desired' output with a series of input data. The output could be a credit score, the chance of doing well in a university, a job and so on. The past data of people who have been 'successful' – some specific output variables – are selected as indicators of success and correlated with various social and economic data of the candidate. This correlation is then used to rank any new candidate in terms of chances of success based on her or his profile. To use an analogy, predictive models are like driving cars looking only through the rear-view mirror.

A score for success, be it a job, admission to a university, or a prison sentence, reflects the existing inequality of society in some form. An African American in the USA, or a dalit or a Muslim in India, does not have to be identified by race, caste or religion. The data of her or his social transactions are already prejudiced and biased. Any scoring algorithm will end up with a score that will predict their future success based on which groups are successful today. The danger of these models are that race or caste or creed may not exist explicitly as data, but a whole host of other data exist that act as proxies for these 'variables'.

Such predictive models are not only biased by the opinion of those who create the models, but also the inherent nature of all predictive models: it cannot predict what it does not see. They end up trying to replicate what they see has succeeded in the past. They are inherently a conservative force trying to replicate the existing inequalities of society.

The Artificial Intelligence community is waking up to the dangers of such models taking over the world. Some of these models are even violations of constitutional guarantees against discrimination. There are now discussions of creating a US Algorithm Safety Board, such that algorithms can be made transparent and accountable. We should know what is being coded, and if required, find out why the algorithm came out with a certain decision: the algorithms should be auditable. It is no longer enough to say "the computer did it".

What's next?

As half of humanity communicates, informs itself and increasingly works and buys online, the original democratization promise of ICTs is being replaced by concern over the enormous power these technologies have concentrated in a few governments and a handful of mega-corporations. The public is concerned everywhere and the question is no longer if regulation is needed but how to do it.

Recognizing knowledge and the Internet as a global public good should imply a multilateral approach, which can only be based on the primacy of human rights and the recognition of sovereignty (after all, 'cyberspace' or 'the cloud' are just metaphors, all

computers and the people operating them are actually somewhere).

Computers, algorithms and the laws that govern our use of them, they are all human creations, the result of a cultural construction and political decisions. And as such they can be changed. It will not be an easy task, but what experience has demonstrated so far is that the Internet is not viable as the property of a single country and that the corporations have failed to regulate themselves.

The major asset of the digital corporate giants is not physical capital but intellectual property over their algorithms and the data (provided by the users) over which they operate. Instead of facilitating exchange, as the name suggests, a new generation of 'free trade' reinforces and extends artificial monopolies over data and technology to the extent that as Nobel economist Joseph Stiglitz says, "In fields such as information technology, a whole set of weak patents and an epidemic of over-patenting has made subsequent innovation difficult and has eroded some of the gains from knowledge creation."[25]

The perception that a different approach to innovation and intellectual property is needed, added to the fear of unfair appropriation of locally generated data by corporations that do not even have representation in their countries led many developing countries to reject the idea of launching e-commerce negotiations at the WTO in 2017.[26]

'More of the same' is not acceptable any longer. The 2030 Agenda proposes a paradigm shift in development that is not possible with the technologies prevailing today, continued reliance on fossil fuels and further unsustainable (mis)use of resources.

To address the technology needs of "a global transition towards less resource-intensive and more resilient economic and social development models," in 2017 the Belgian research and technology organization VITO, together with partners in Africa, India and Brazil started a series of Global Science Technology and Innovation conferences. Their initial findings are optimistic: "Many technologies needed to achieve many SDG-related targets are readily available."[27] They add that the effectiveness of alternative solutions having been demonstrated under real-life conditions, what is needed is "to develop strategies for deployment at scale to a level necessary to achieve the SDGs."

In the case of energy and food, they state that a key requirement for achieving the SDGs is to prioritize "widely distributed and bottom-up technological solutions that are appropriate for communities' needs and circumstances". Ultimately a "circular economy" is to be put in place. In this new model, ICTs are recognized as "an indispensable tool" and "resource recovery and use from waste" becomes "the new normal".

References

Bartlett, Jamie (2018): Will 2018 be the year of the neo-luddite? In: The Guardian, 4 March 2018. www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite

Cisco (2017): Cisco Visual Networking Index: Forecast and Methodology, 2016–2021. www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

Earth Institute/Ericsson (2015): ICT and SDGs: How Information and Communications Technology Can Achieve The Sustainable Development Goals. New York. http://unsdsn.org/wp-content/uploads/2015/09/ICTSDG_InterimReport_Web.pdf

Geer, Dan (2014): Cybersecurity as Realpolitik. http://geer.tinho.net/geer.blackhat.6viii14.txt

Graham, Mark/Hjorth, Isis/Lehdonvirta, Vili (2017): Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. In: Transfer: European Review of Labour and Research 23:2. http://journals.sagepub.com/doi/10.1177/1024258916687250

25 Stiglitz et al. (2017).

26 See: www.twn.my/title2/wto.info/2017/ti171232.htm

27 See: https://2018.gstic.org/insights/2017-key-findings

Human Rights Council (2018): Report of the Special Rapporteur on the right to privacy, Appendix 7: Draft Legal Instrument on Government Led Surveillance. Geneva (A/HRC/37/62). www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf

Kaul, Inge/Grunberg, Isabelle/Stern, Marc A., ed. (1999): Global Public Goods. International Cooperation in the 21st Century. New York: Oxford University Press. https://www.researchgate.net/profile/Eugenio_Bobenrieth/publication/46440722_The_Political_Economy_of_International_Environmental_Cooperation/links/55ddb07308ae79830bb531ed.pdf#page=488

Nicholson, Jessica (2016): Measuring the Economic Value of Cross-Border Data Flows. Presentation at UNCTAD/WTO/UPU Measuring E-Commerce Day, 22 April 2016. Washington, D.C.: U.S. Department of Commerce, Office of the Chief Economist. http://unctad.org/meetings/en/Presentation/dtl_eweek2016_JNicholson_en.pdf

Palmer, Michael (2006): Data is the New Oil. In: ANA Marketing Maestros, 3 November 2006. http://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Porche, Isaac R. (2018): Getting Ready to Fight the Next (Cyber) War. In: The RAND Blog, 3 March 2018. www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html

Ranger, Steve (2017): Cyberwar: A guide to the frightening future of online conflict. In: ZDNet, 29 August 29 2017. https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Stiglitz, Joseph/Baker, Dean/Jayadev, Arjun (2017): Innovation, Intellectual Property, and Development: A better set of approaches for the 21st century. Azim Premji University, University of Cape Town, Fundação Osvaldo Cruz. http://cepr.net/images/stories/reports/baker-jayadev-stiglitz-innovation-ip-development-2017-07.pdf

Tarnoff, Ben (2018): Big data for the people: it's time to take it back from our tech overlords. In: The Guardian, 14 March 2018. www.theguardian.com/technology/2018/mar/14/tech-big-data-capitalism-give-wealth-back-to-people

United Nations (2018): Remarks of the Secretary-General to the Economic and Social Council, Operational Activities for Development Segment. Tuesday, 27 February 2018. New York. www.un.org/sg/en/content/sg/speeches/2018-02-27/remarks-ecosoc-activities-development-segment

United Nations (2015): Transforming our world: the 2030 Agenda for Sustainable Development. New York (UN Doc. A/RES/70/1). https://sustainabledevelopment.un.org/post2015/transformingourworld

United Nations (2013): The right to privacy in the digital age. Resolution adopted by the General Assembly on 18 December 2013 [on the report of the Third Committee (A/68/456/Add.2)]. New York (UN Doc. A/RES/68/167). www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

UNCTAD (2017): Information Economy Report 2017: Digitalization, Trade and Development. Geneva (UNCTAD/IER/2017/Corr.1). http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf

UN OHCHR (2018): Concept Note. Expert workshop with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, 19 & 20 February 2018, Geneva. www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf

US Department of Defense (2015): Law of War Manual. Washington, D.C. www.defense.gov/Portals/1/Documents/law_war_manual15.pdf

White House (2016): Press Conference by President Obama after G20 Summit, September 5, 2016, J.W. Marriott Hotel Hangzhou, China. https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/press-conference-president-obama-after-g20-summit

WTO (1998): Electronic Commerce: Declaration of the Second Ministerial Conference, 25 May 1998. Geneva (Wt/Min(98)/Dec/2). www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm

Roberto Bissio is Executive Director of the Instituto del Tercer Mundo (Third World Institute) and coordinator of the Social Watch network.