



unieri
United Nations
Interregional Crime and Justice
Research Institute

1 0 0

1

1 0

1 0 0

1 0

1 0 0

1

1 0

1 0 0

1 0 0

1

SDG 16

Through a Digital Lens

0

1 1 0

SDG 16

Through a Digital Lens



DISCLAIMER

The opinions, findings, conclusions, and recommendations expressed herein are those of the authors and do not necessarily reflect the views and positions of the United Nations, or any other national, regional or international entity involved. Contents of the publication may be quoted or reproduced, provided that the source of information is acknowledged. The designations employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area of its authorities, or concerning the delimitation of its frontiers and boundaries.

ACKNOWLEDGEMENTS

This report has been prepared by Mr. David Andersson, UNICRI consultant and independent analyst and adviser on conflict, fragility, and sustainable development, under the guidance of Mr. Odhran McCarthy, New York Liaison Officer, UNICRI and Mr. Leif Villadsen, Senior Programme Officer (Deputy Director), UNICRI.

© United Nations Interregional Crime and Justice Research Institute (UNICRI), 2023

Viale Maestri del Lavoro, 10
10127 Turin, Italy

Website: www.unicri.org

E-mail: unicri.publicinfo@un.org

November 2023

Funded with the support of Italy



Foreword

Our world is increasingly digital, interconnected, and reliant on technology, and as we journey further into the 21st century, the transformative potential of digitalization becomes ever more undeniable. It touches all aspects of life, altering how we communicate, conduct business, and govern our societies. In this ever-evolving landscape, it is imperative that we strive to harness the power of digitalization to create a more just, inclusive, and sustainable future for all.

The 2030 Agenda for Sustainable Development, comprised of 17 Sustainable Development Goals (SDGs), is a commitment to address the world's most pressing challenges. Our work at the United Nations Interregional Crime and Justice Research Institute (UNICRI) falls under the umbrella of SDG 16, which seeks to promote peaceful and inclusive societies, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels. In many ways, SDG 16 is the cornerstone for achieving a sustainable, equitable, and just world, as enhancing good governance, human rights, and justice is imperative for peace and development. Consequently, in this digital era, achieving SDG 16 takes on a renewed and dynamic significance.

For many years now, UNICRI has explored the promise and pitfalls of traditional information communications and technology and, more recently, emerging technologies in the context of justice, security, and the rule of law. In fact, our 2023-2026 Strategic Programme Framework identifies promoting the responsible use of new and emerging technologies to address crime and exploitation as one of the Institute's key pri-

orities. In line with this, our Centre for Artificial Intelligence and Robotics in The Hague has been at the forefront of the discourse around the use of artificial intelligence (AI) in the context of law enforcement, exploring how we define, institutionalize, and foster responsible AI innovation in policing.

This report, *SDG 16 Through a Digital Lens*, zooms out from UNICRI's niches in justice, security, and the rule of law to explore broadly the intricate interplay between the trend toward digitalization and the pursuit of peace, justice, and strong institutions. It delves into the complexities, providing much needed analysis as we reach the half-way mark for the SDGs, and outlines a high-level vision for how we can ensure that digital transformation advances, rather than hinders, our progress towards SDG 16. As the title suggests, this report emphasizes that we must look at SDG 16 'through a digital lens'. Failure to consider both the digital enablers and barriers of progress will only result in the international community falling short of its commitments to the SDGs.

This report, however, is an initial contribution in terms of the research, analysis, and action needed on digitalization and SDG 16. We will continue to explore the digitalization aspects of our work at UNICRI through research and training, and we hope that this report also serves as a catalyst for others to do likewise.

Antonia Marie De Meo
Director, United Nations Interregional Crime
and Justice Research Institute

Table of Contents

	Foreword	iii
--	----------	-----

1	Introduction	2
	Background: SDG 16 in the digital space	2
	SDG 16: an enabling goal	5
	Advancing SDG 16 in the digital space	6
	Approaching the SDG16-digitalization nexus	6

2	Universal connectivity & the digital divide	8
	Digital divisions	8
	Meaningful connectivity and the inequalities that prevent it	10
	A challenge of inclusive governance	13

3	Legal identity: a foundational inequality challenge	14
	The imperative of legal identity for all	14
	Legal identity: the state of play	16
	Legal identity as a governance priority	17

4	Illicit financial flows and their digital enablers	18
	An intractable form of theft	18
	The far-reaching impact of IFFs	20
	The digital dimensions of IFFs	22
	Tackling IFFs in the digital era	24



5	Impacts of online disinformation & misinformation	26
	A fragmented information landscape	26
	Impacts of mis- and disinformation on freedom of expression and democratic processes	28
	Oversight and regulation: a complex task	29
<hr/>		
6	Perspectives on conflict in the digital space	32
	How digitalization and conflict intersect	32
	Conflict risks and information ecosystems	34
	Digitally enabled conflict actors and spoilers	35
	Responding to conflict in the digital space	36
<hr/>		
7	Reflections moving forward	38
	Digital social contracts	38
	Responsive and people-centred digital governance	40
	Issues for further exploration	42
<hr/>		
	Endnotes	43

1.

Introduction

Background: SDG 16 in the digital space

In 2015, with the adoption of the 2030 Agenda and Sustainable Development Goals (SDGs), all UN Member States committed to building more peaceful, just, and inclusive societies (Goal 16). This commitment reflects a global consensus that often-sensitive issues pertaining to conflict and violence, governance, human rights, and justice are also development concerns. The state of global development in 2023 – halfway to 2030 – illustrates this connection well. Half of the around 140 SDG targets with data that can be evaluated show moderate or severe deviations from the desired tra-

jectory with some 30 per cent recording either no progress or regression since 2015.¹ These trends are taking place in a context of multiple, cascading crises on a global scale, contributing to diminished trust in public institutions and strained relationships between these institutions and the populations they are supposed to serve. These crises include the war in Ukraine and its impacts on global food and energy supplies, the climate crisis, high-levels of violence, forced displacement and a debt crisis, all of which have been aggravated by the COVID-19 pandemic.



These interconnected crises are occurring at a time when digital technologies and tools are advancing at an unconstrained and unprecedented pace, giving rise to profound global transformations. This *digitalization* has broadened economic and livelihood opportunities and enabled improved access to services for people across the globe, who may otherwise not have had them. On this basis it also holds immense potential for achieving development outcomes.² Estimates published by the International Telecommunication Union suggest that “*equalizing internet access between developing and developed countries could generate around US\$2.2 trillion in gross*

domestic product (GDP) and 140 million new jobs.”³ Conversely, unchecked digitalization has enabled social polarization, exacerbated inequalities, and aided government surveillance and new forms of autocracy. It equally brings the potential to reinforce existing fault lines (for better or worse) while also affording government, non-state, and private actors new forms of power and influence. These combined dynamics stress the relevance of SDG 16 in the digital space, and show that efforts to advance more peaceful, just, and inclusive societies must apply a digital lens to remain relevant and have impact.

► Figure 1: SDG 16 targets



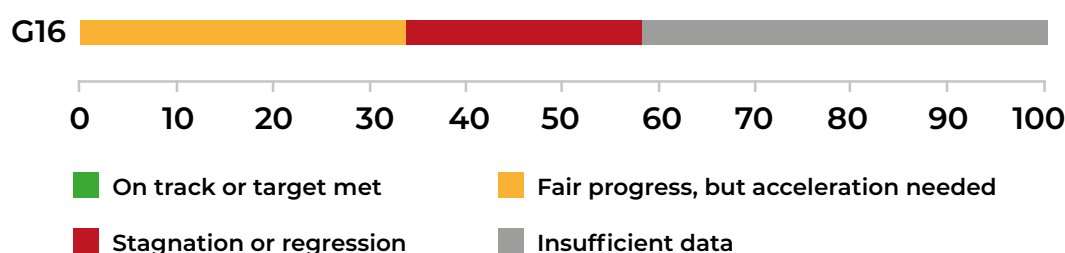
SDG 16: an enabling goal

SDG 16 is commonly known as an *enabling* goal - meaning that leveraging its core features to make progress on peaceful, just, and inclusive societies can enable outcomes across the SDG spectrum. This phenomenon is also referred to as *SDG 16+*, a term reflecting how SDG 16's 12 official targets and associated indicators correlate with numerous other goals and targets.⁴ In addition, the targets and indicators of SDG 16 are considered unique in large part for incorporating [political and] governance dimensions, which the Millennium Development Goals, for instance, did not. While unprecedented, they are nevertheless considered by many to be limited in their reflection of global conflict, inequality, and injustice challenges (and the relatively limited availability of data). This has led many, notably civil society actors, to also advocate for and measure unofficial, complementary indicators and data sets covering a wider range of issues premised on the goal's underlying features.⁵

In 2023, SDG 16 is among the most off-track goals, notwithstanding regional and country variations, making its (and

related) targets increasingly challenging to meet by 2030. For instance, global homicide rates (captured in indicator [16.1.1](#)), which were on the decline between 2015 and 2020, have since seen a significant resurgence reaching the highest numbers in two decades. This is in part due to the economic impacts of COVID-19-related restrictions as well as gang-related and socio-political violence.⁶ Broader assessments of the state of peace, justice, and inclusion are equally bleak. Some 60 per cent of respondents in a recent global civil society-focused survey felt there was backsliding or little progress on SDG 16+ both at the domestic and international levels.⁷ And access to quality and timely justice around the world appears to be increasingly out of reach for people around the globe.⁸ As noted in the UN's 2023 Sustainable Development Goals Report: "*structural injustices, inequalities and emerging human rights challenges are putting peaceful and inclusive societies further out of reach.*"⁹ The goal's sombre state in 2023 is further compounded by only 40 per cent of countries or areas having internationally comparable data on SDG 16 since 2015 (see Figure 2 below).¹⁰

► **Figure 2: Progress assessment for SDG 16 targets (for 2023 or latest data)**



Source: United Nations, *The Sustainable Development Goals Report: Special Edition, 2023*, p8.



Advancing SDG 16 in the digital space

As the world grapples with these challenges, achieving SDG 16 outcomes increasingly calls for understanding and leveraging trends in the digital space. This was made especially clear during the pandemic as reliance on digital technologies dramatically increased, including for information related to the virus, equitable access to social protection and other key services.¹¹ Today, digital platforms and technologies have come to mediate nearly every facet of modern life, from healthcare, education, and employment to justice and security – being the domain in which UNICRI primarily operates. Common governance chal-

lenges linked to the distribution of state power and resources, and accountability for decision-making are also reflected and often amplified in the digital space. Therefore, advancing SDG 16 is in some ways a question of *digital governance*, or more accurately the ‘governance of the digital’ as opposed to focusing on the digital aspects of governance alone. Accordingly, it is incumbent on SDG 16 advocates to account for the laws, policies, and regulations (or lack thereof) that can act as guardrails for *digital harms* that can for example polarize societies or incentivize violence and conflict.

Approaching the SDG16-digitalization nexus

In view of these dynamics, this paper explores the intersection between digitalization and SDG 16. Specifically, it considers five different yet complementary issues that illustrate how digital trends can adversely affect the goal, namely: i) universal connectivity, the digital divide and inequality; ii) inclusion and the imperative of [digital] legal identity; iii) illicit financial flows and their digital enablers; iv) online misinformation and disinformation and its consequences; and v) the intersection of digitalization and conflict. These topical issues reflect core themes linked to SDG 16, including the 2030 Agenda’s commitment to leave no one behind, and access to information and fundamental free-

doms. They are also characterized and informed by digitalization. Although these issues are unique, they all speak to the importance of inclusive, responsive, and accountable governance systems in achieving the goal - themes that will also be explored in the following pages.

Accordingly, this paper explores SDG 16 from a broad perspective. It accounts for official targets and indicators, the goal’s core themes of peace, justice, and inclusion as well as underpinning principles such as accountability and inclusion. Similarly, the paper takes a broad view of digitalization, which is here understood in the context of development and as a process of using digital tech-

nology (or tools, processes, solutions) for greater operational impact. In addition, the term accounts for the societal factors that enable the use, or misuse, of digital technology.¹² Definitions notwithstanding, the paper does not address all notably high-tech features of digitalization but is rather intended as a snapshot of SDG 16 from digital per-

spectives that are less frequently explored. In this sense, it complements the range of analytical and policy materials that cover the state of the goal, halfway to 2030. The paper seeks to illustrate the urgency of reversing negative trends on SDG 16 and the importance of focusing collective efforts in the digital space as a means of doing so.

2.

Universal connectivity & the digital divide

Digital divisions

At the heart of debates around digitalization and development lies the ambition to achieve universal digital connectivity, i.e., to connect all people to the internet and close the 'digital divide' - a core commitment in the UN Secretary-General's Roadmap for Digital Cooperation.¹³ In 2022, some 66 per cent of individuals worldwide were using the internet, and this figure has been continuously rising over the past two decades, particularly since the onset of the COVID-19 pandemic. In 2005 the figure was 16 per cent.¹⁴ Despite this major digital leap, an estimated 2.9 billion people globally remain offline

today, in part due to the rapid expansion of coverage having outpaced the number of people actually using the internet. This points to an internet usage gap as opposed to a coverage gap alone. As the World Bank's 2021 World Development Report (WDR) points out, a substantial majority of the 40 per cent of the world's population who do not use data services live within the range of a broadband signal. The WDR also notes that over two thirds of [surveyed] people living in low- and middle-income countries who do not access the internet do not know what it is or how to use it.¹⁵



As these discrepancies show, there is more to the digital divide than a technical, binary distinction between ‘haves and have-nots’. It is also a matter of frequency and quality of internet usage, and factors such as the relevance of available content, and the readiness of the population to use it. This speaks to the importance of digital skills and literacy to internet usage, which is reflected in SDG 4 (quality education). In addition, the digital divide is a matter of affordability, i.e., price, and a competitive environment. The Inclusive Internet Index, a global dataset (and survey) found that perceptions of internet affordability improved in 2022, when 37 per cent of survey respondents noted an improvement in affordability since the

early days of the pandemic, compared to 30 per cent in 2021.¹⁶ That said, the affordability of internet connectivity remains a hurdle for many. The average consumer in a low-income economy pays over six times the global average for the cheapest mobile broadband basket, while fixed broadband service cost over 30 per cent of average incomes, compared to two per cent in high-income countries.¹⁷ In considering factors such as education and income, a more comprehensive understanding of the digital divide that accounts for *meaningful* internet connectivity and the social, political, and economic factors that make such connectivity possible is essential.

■ **Box 1: 2022 Kigali Declaration on universal and meaningful connectivity**

In 2022, at the eight World Telecommunication Development Conference in Kigali, Rwanda organized by the International Telecommunication Union, 150 Member States and 340 sector members and partners endorsed the 'Kigali Declaration.'¹⁸ . The declaration, which underscores a commitment for universal and meaningful connectivity also outlines what such connectivity must entail. This includes availability, affordability, up-to-date digital infrastructures, as well as capacity, as: *"insufficient digital capacity and lack of digital skills are core barriers to digital transformation and the digital economy."*

Meaningful connectivity and the inequalities that prevent it

These various manifestations of the digital divide can be seen as different reflections of inequality. Therefore, efforts to ensure *meaningful* connectivity, must also reasonably apply an inequality lens. This means, according to the Broadband Commission, emphasizing affordable services and devices for *"anyone, anywhere, regardless of geographic location, socio-economic status, race, gender, or any other differentiating demographic."*¹⁹

Challenges vis-à-vis unequal internet access and usage are not new but continuously evolve with the pace of technological developments, as well as the state of [broader] inequality and exclusion. Arguably, the digital divide deepens and amplifies other forms of inequality. Consider how, for instance, investments in technology are rarely matched in terms of spending on infrastructure and education, while the immense value generated by proliferating digital technologies does not result in

shared prosperity. This was notably the case in the aftermath of the pandemic.

The pandemic clearly illustrated how discrepancies in access to internet connectivity and digital technologies (as reliance on these increased) accentuated the socio-economic and political gaps both between and within countries.²⁰ In many country contexts, adequate and accessible internet connectivity was not only a necessity for critical information about the pandemic, but also to access basic social services like health and education. Here, digital divides most evidently impacted poor and already marginalized, vulnerable or excluded groups. This included prisoners, refugees, migrants and undocumented people, and persons with disabilities who faced additional barriers to internet access and assistive technologies due affordability challenges and limited accessibility of technological devices, programs, and websites.²¹



“The digital divide remains a challenge and reinforces inequalities, pushing those furthest behind even further as access to technology is an additional stumbling block to accessing services or political participation.”

– Southern Voice²²

Findings from a Pew Research Center survey on global internet usage during the pandemic found that people with higher incomes were more likely to use the internet, at least occasionally, or report owning a smartphone. These digital inequalities were notably pronounced in low-income countries. Data from the pandemic’s first three months show how burdens on the labour sector were disproportionately shouldered by disadvantaged groups (i.e., lower educated workers, women and youth) who were far more likely to lose their jobs. In the education sector, limited access to learning during school closures disproportionately impacted larger, less educated households. In high-income countries, those at the lower end of income distribution also bore the brunt of the crisis, while those at the top saw high levels of income and wealth growth (including from technology heavy industries such as e-commerce). These short-term pandemic impacts on livelihoods and education may further constrain prospects for longer-term inequality and social mobility.²³

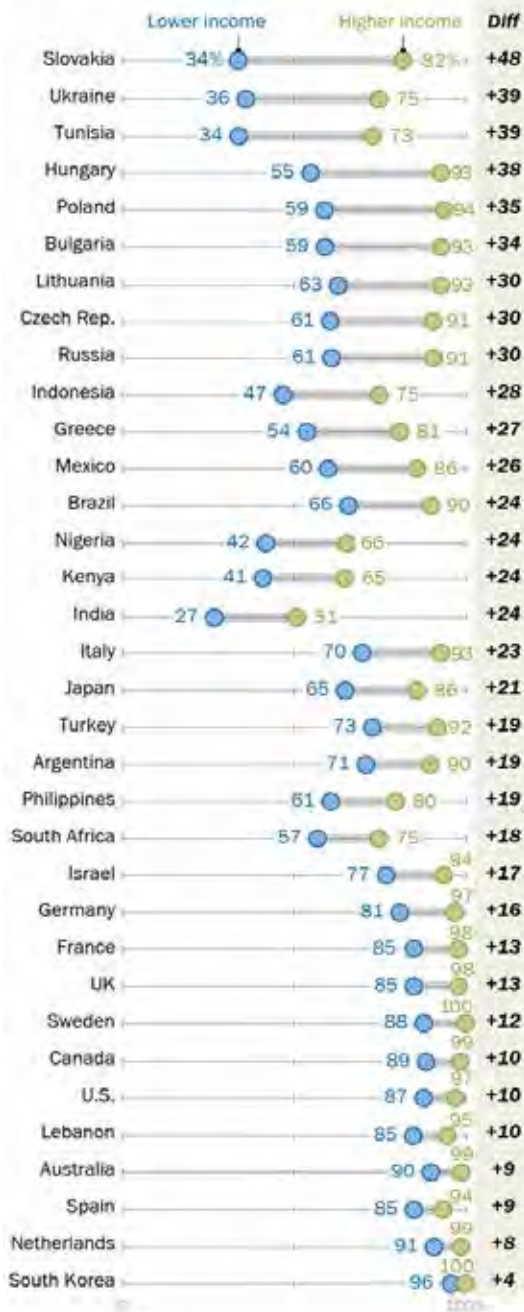
The digital divide is also highly gendered as women and girls face unique connec-

tivity barriers, which are often extensions of different forms of discrimination. Over the past year, 259 million more men than women were online - indicating modest steps towards gender parity though in absolute terms reflecting a gap increase of 20 million.²⁴ Obstacles to women’s and girls’ equal online access in many countries include digital literacy challenges and [patriarchal] social norms, expressed through e.g., lack of family approval for women owning a cellphone.²⁵ UN Women points out that women are 18 per cent less likely to own a smart phone than their male counterparts, limiting opportunities and compounding gender inequalities as a result.²⁶ The gender digital divide has become so pronounced that it is a key priority of the Commission on the Status of Women (CSW), the UN’s principal gender equality forum. In its 67th session (2023), it unanimously adopted ‘Agreed Conclusions’, calling for increased financing, capacity-building and other targeted measures to close the gender digital divide and remove barriers to equal access to science, technology, and innovation for all women and girls.²⁷

► Figures 3 & 4: The digital divide vis-à-vis education and income

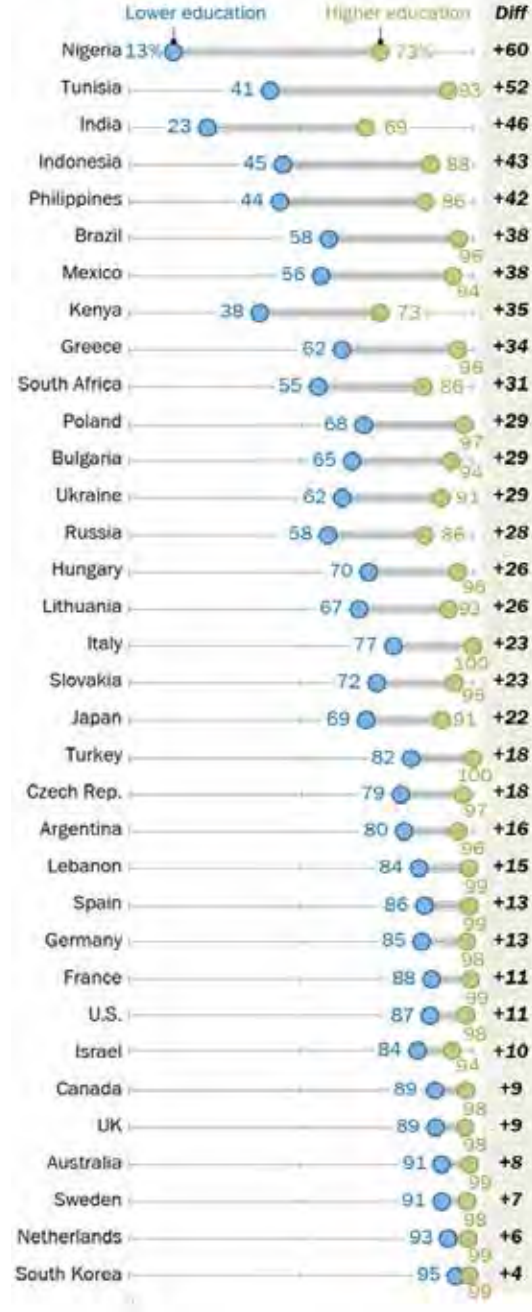
People with higher incomes more likely to use the internet

% who use the internet, at least occasionally, or report owning a smartphone



Those with higher levels of education more likely to use the internet

% who use the internet, at least occasionally, or report owning a smartphone



Source: Pew Research Centre, Spring 2019 Global Attitudes Survey. Q51 & Q53. U.S. data from a Pew Research Centre survey conducted Jan. 8-Feb. 7, 2019²⁸

A challenge of inclusive governance

Expanding meaningful connectivity calls for measures that account for the unique economic and social contexts that exist in different country settings yet are all bound to include policies and financial models that are appropriately inclusive. Such measures may include providing financial incentives to expand digital infrastructure or encouraging telecommunications operators to bring connectivity to remote or hard-to-reach areas.²⁹ Relatedly, ensuring that the poorest and most sidelined groups in society can go online requires making it sufficiently affordable to do so. In practice this can mean subsidizing internet access in rural areas, incentivizing or funding [pro-poor] innovation, or enabling the design of digital products and services for disabled persons. Achieving universal digital connectivity also requires ensuring digital literacy across the entire population - from school-aged children developing skillsets complementary to technologies to vocational training and education for adults.³⁰ As noted in the Agreed Conclusions for CSW 67, this must comprise inclusive and equitable quality education, including digital literacy, for all women and girls to tackle the gender digital divide.³¹ This requires, by necessity, enhancing the use of enabling technology to e.g., promote women's empowerment as outlined in [SDG target 5.b](#).

These are more than mere technical solutions. At their core, they reflect a challenge of inclusive (and participatory) governance as the factors that reduce the

digital divide are largely economic and political in nature and will entail some form of societal transformation. They necessitate governance processes accompanied by political, legal, and regulatory frameworks to ensure that new technologies can benefit the public interest and be used equitably among all groups in society. For the most part, such regulatory systems have not been able (or designed) to catch up with the rapid pace of digitalization and exercise meaningful oversight. The UN Secretary-General refers to this as a “massive governance gap” and points to underinvestment in state capacities and public institutions, which are unable to compete with comparatively well-resourced private actors on equal terms.³²

This challenge also calls for us to consider the normative aspects of universal connectivity, including the extent to which the internet should be considered a public good or a commercial product (or a combination, or variation of both).³³ Proponents of the former are increasingly vocal in the policy space and are applying rights-based language to further the cause. Universal access to the internet as a human right is, while not a new idea, proposed in the Secretary-General's report 'Our Common Agenda.'³⁴ In March 2023, UN High Commissioner for Human Rights Volker Türk, while referencing the digital divide, asserted that “*it may be time to reinforce universal access to the internet as a human right and not just a privilege.*”³⁵

3.

Legal identity: a foundational inequality challenge

The imperative of legal identity for all

Another important illustration of the intersection between inclusion, equality and digitalization can be found in efforts to provide legal identity for all, including birth registration. This issue, which is an explicit objective of [SDG Target 16.9](#), and features in the Universal Declaration of Human Rights³⁶ does not always receive the coverage or attention it deserves. Nevertheless, it is integral to safeguard people's human rights from their birth until their death, ensure evidence-based policy making, as well as inclusive development. In this regard,

legal identity can be a useful illustration of SDG 16's enabling qualities and how advancing the goal can catalyse and accelerate development progress across the SDG spectrum.

Verifiable legal identity covering a person's entire life (e.g., via civil registration, vital statistics, and identity management systems) is critical to providing access to the most essential services. These include social protection (SDG 1), health services and medical care (SDG 3), educational opportunities (SDG 4), finan-



cial services such as digital payments or bank accounts (SDG 8), and access to justice (SDG 16). Conversely, the absence of legal identification can significantly impede equitable and inclusive development. To illustrate, in the context of the pandemic, low levels of legal identity and poorly functioning registration systems saw some governments unable

to register deaths and issue death certificates.³⁷ Similarly, legal identity systems were critical to manage COVID-19 vaccine distributions and certificates in a cost-effective, secure, and trusted way.³⁸ Identity is, of course, also relevant – and lucrative – for other reasons, with identity theft becoming a fast-growing illicit domain.



Legal identity: the state of play

In 2022, some 850 million people globally were estimated not to have access to any form of legal identity. Reasons include arduous documentary requirements, inaccessible registration centres and unaffordable costs. These obstacles are in part linked to legal identity in many instances being a *digital affair* and access to legal ID requiring digital technologies, online connectivity in addition to the skillsets and financial resources to effectively use it. Those most impacted tend to be marginalized groups, including migrants, refugees, and trafficked people as well as under-privileged groups at the bottom of the income distribution scale, mainly in lower and lower middle-income countries in Sub-Saharan Africa and South Asia. Women are also disproportionately impacted and are estimated to be eight per cent less likely to possess legal identity than men. However, some progress has been registered vis-à-vis gender parity in this regard.³⁹ Given this, removing barriers to digitally accessible legal identity for all is also critical to meeting the 2030 Agenda's commitment to Leave No One Behind.

As with the digital divide, access to legal identity (or lack thereof) is not a simple binary issue. Instead, it is contingent on numerous criteria that determine its *quality*, such as whether it is inclusive by design, trusted, or verifiable. And the importance of quality identity takes on

new meaning when considering the speed and scope of digitalization. By one estimation, some 3.4 billion people in possession of legal identity have limited ability to use it in the digital world.⁴⁰ Digital or 'smart' legal IDs can prove beneficial in several ways (in addition to those listed above). They can help people access public services remotely, which is essential during crises like the pandemic. It is also beneficial for vulnerable or remote communities or people with mobility challenges.⁴¹

However, from this vantage point, a deepening digital divide also runs the risk of exacerbating inequalities by making the services and benefits enabled by digital legal IDs (and the digital tools they require) further inaccessible for those who remain unconnected. Moreover, digital identity is also a sensitive topic as it can contribute to concerns around state surveillance in poorly regulated environments, for instance when combined with controversial technologies such as facial recognition technology.⁴² It equally presents risks from the perspective of data breaches. Indeed, recent history is littered with examples of high-profile data breaches involving the leakage of individuals' personal data, which can lead to financial loss, reputational damage, loss of trust, enable identity theft and even present security risks in some cases.

Legal identity as a governance priority

Access to legal identification, and the formal recognition and participation in economic and political life it brings, holds much promise in reducing inequality. And this access can be further boosted by more inclusive and equitable forms of digitalization. But efforts to expand this access require more than inclusive decision-making alone. It necessitates strong *foundational* systems and [digital] infrastructure that can serve as anchors for relevant laws, policies, and regulations (and enable *functional* systems like vaccine programs or electoral rolls).⁴³ Foundational systems (e.g., digital ID systems or population registers) must, in turn, not only be efficient but sufficiently inclusive, secure, and trusted by people for them to help achieve development outcomes that benefit all, not just the few. And such trust is a critical factor in ensuring that digital identity systems are not exploited or used for malicious or nefarious purposes.

While essential, these regulatory systems and processes are neither easy nor cheap to put in place. They require eliminating barriers to access, reducing duplicative systems (e.g., between different institutions), improving regular and timely data collection while also ensuring comprehensive data privacy.⁴⁴ Furthermore, they require building and strengthening [digital] partnerships across all strata of society, including between central and local authorities, communities, and civil society. Hurdles notwithstanding, ensuring access to legal identity for all is entirely feasible from a technical point of view, and the relevant international legal and policy frameworks to do so are in place. Significantly reducing the number of people who lack quality legal and digital forms of identity is therefore a policy imperative that merits increased political attention and financial support.

■ Box 2: Building a foundational legal ID system in Malawi

In 2017, Malawi implemented a whole-of-society initiative to build its foundational digital identification system. Prior to this, only a small percentage of citizens had access to legal identity and the government faced several service delivery challenges and high levels of fraud as a result (e.g., payments of salaries and benefits to 'ghost workers'). By some estimates, up to 99 per cent of the adult population of nine million had their biometric data registered to receive a national ID card or passport all within a short, six month timeframe. This new system, which was inter-operable with other functional registries, enabled the expansion of electoral rolls, health services, and other cost-saving measures due to reduced fraud, which in turn enabled subsidies in the agricultural sector. It also set the stage for other public infrastructure measures such as case management handling in the judicial system.⁴⁵ In recent years, the Government has endeavoured to expand registration to include (8.4 million) children under the age of 16. This process has, however, raised concerns about privacy and data protection and the safe and legal collection and processing of children's data, as a comprehensive, general data protection law has yet to pass.⁴⁶

4.


Illicit financial flows and their digital enablers

An intractable form of theft

Illicit Financial Flows (IFFs) are intractable challenges that are global in scope. Despite their prevalence, there is no consensus on the definition of IFFs as they cover a diverse set of activities, reflecting the scale and complexities of illicit international trade and finance. Further, they are notoriously difficult to measure given their opacity and illicit nature.⁴⁷ Limitations notwithstanding, IFFs can be generally defined as the movements of money or capital [across borders], which are illicit in their origin, transfer, or in their use.⁴⁸ They are commonly generated by the following diverse and often

overlapping activities: i) *corruption*, including bribery, theft, graft, and embezzlement; ii) *commercial and tax practices*, such as tax evasion, misreporting and mis-invoicing linked to trade-activities, and money laundering; iii) *exploitation-type actions*, including extortion, trafficking in persons and financing for terrorism; and iv) *illegal market-related flows*, such as smuggling of arms and drugs.

IFFs can broadly speaking be understood as forms of theft in so far as they entail the illegal seizure or misappropriation



tion of funds, which in turn deprives their intended beneficiaries of sustainable development outcomes. They can differ widely by country and involve a diverse range of actors operating in the public, private, and criminal sectors – and often comprise a convergence of the three. Money laundering, for instance, entails concealing the proceeds of crime and integrating these into the legitimate financial system, often by separating [illicit] funds from their source using anonymous shell companies. It also takes place in trade-related processes whereby illegally earned funds are co-mingled with legitimate proceeds (e.g., through

trade-misinvoicing).⁴⁹ In this regard, IFFs are rarely conducted by criminals alone but enabled by an array of professionals, including from the legal and financial sectors.

The organization of IFFs typically requires the aid of banks who are either unable (or unwilling) to perform requisite checks and monitoring of transactions,⁵⁰ or other types of ‘corporate vehicles’ - legal structures that enable the creation, maintenance, and movement of assets. While fully legal, they can help obscure the illicit source of finances and identity of the owner (“beneficial owner-

ship”) thereby allowing their perceived legitimacy to avoid law enforcement. To illustrate, files leaked from the so-called ‘Panama Papers’ in 2016 revealed offshore companies and legal entities in jurisdictions acting as conduits for IFFs through the global financial system. The files demonstrated how asymmetries in legal and enforcement frameworks between jurisdictions can enable the use of legal entities to conceal corrupt funds by public officials, money laundering as well as tax evasion and avoidance.⁵¹

This confluence of legality and illegality is also evident in commercial and

tax-related IFFs, which include practices that may only sometimes be subject to [enforceable] laws given legal grey areas and differences in standards and interpretations between jurisdictions.⁵² They remain an area of concern for international organizations in that they may be both unethical and a source of societal harm.⁵³ For instance, aggressive tax avoidance practices (e.g., shifting corporate profits to low-tax jurisdictions, often non-transparently) are in many instances not strictly illegal but nevertheless significantly undermine sustainable development prospects, exacerbate inequalities and damage social cohesion.

■ Box 3: Illicit flows and SDG 16

Preventing IFFs and mitigating their effects is critical to building and maintaining peaceful, just, and inclusive societies. SDG target 16.4 (indicator 16.4.1) states that “by 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime.” This indicator is, however, inherently difficult to measure given the secrecy and opacity surrounding IFFs. In 2018, UNODC and UNCTAD, as custodian agencies of this indicator jointly developed a framework for statistical measurement to estimate IFFs.⁵⁴ The first preliminary measurements of IFFs (covering 2018-2022) took place in 22 countries across three continents. Another nine countries are expected to do so in 2023-2026, showing that while challenging, IFFs can be measured.⁵⁵

The far-reaching impact of IFFs

While the first measurements of official data on IFFs data (see box above) do not reflect global or regional trends, they point to criminal as well as commercial and tax-related IFFs as being of significant scale. In Mexico from 2016 to 2018, the smuggling of foreign irregular migrants to the United States generated over \$1.1 billion in inward IFFs (i.e.,

entering the country) for Mexico-based smugglers - much of which could be reinvested in illicit activity. In Namibia, trade misinvoicing was preliminarily estimated at \$19.6 billion in inward IFFs and \$4.7 billion in outward IFFs (i.e., flows leaving the country) between 2018 and 2020.⁵⁶ Global (unofficial) estimates of IFFs are even more astonishing. Up to

10 per cent of global GDP is thought to be held in offshore financial assets, while up to \$7 trillion of the world's private wealth is funnelled through tax havens and secrecy jurisdictions.⁵⁷ This problem, while global in scope, disproportionately impacts developing countries. Global Financial Integrity estimates that the annual value of trade-related IFFs flowing in and out of developing countries amounts to 20 per cent of their trade with advanced economies.⁵⁸

The above examples of illicit capital flowing in and out of countries represent massive and mostly illegal expropriation, or theft, of funds, which contributes to draining foreign exchange reserves, reduces government revenue and levels of productive public and private investment. These economic impacts in turn obstruct, distort, and delay the pursuit of sustainable development outcomes. UNCTAD has estimated that roughly 3.7 per cent of the joint annual GDP of African economies during 2013-2015 was lost to capital flight. This includes trade misinvoicing and other balance-of-payment transactions and represents nearly half of its annual \$200 billion SDG financing gap.⁵⁹ It further found that some African countries with excep-

tionally high levels of IFFs spend 25 per cent less than countries with low IFFs on health and 58 per cent less on education, with women and girls bearing the brunt of the adverse fiscal effects.⁶⁰ Put differently, IFFs prohibit adequate spending on essential services and critical investments in schools, teachers, healthcare facilities, doctors and nurses.

The illicit flight of capital also has critical political and governance dimensions, which re-emphasizes the importance of SDG 16 and the pursuit of peaceful, just, and inclusive societies. IFFs have adverse impacts on the capacity of public institutions to control corruption, implement and enforce relevant laws, and exercise accountability for the use (and misuse) of taxpayer funds. The scale and persistence of IFFs also impact legitimacy and trust in institutions, as reduced social cohesion, increased inequalities and political discontent impede governments' ability to provide services and foster resentment linked to high levels of corruption.⁶¹ Countries dependent on extractive industries are particularly vulnerable, partly due to poor implementation and enforcement of legal and regulatory frameworks.⁶²

Box 4: IFFs during the COVID-19 pandemic

The economic downturns brought by the COVID-19 pandemic, combined with dramatic measures taken by countries to stave off economic collapse and rises in poverty and inequality, saw increased opportunities for corruption to thrive alongside other criminal financial opportunities. Six months into the pandemic, Transparency International had documented cases of corruption and misconduct involving public funds amounting to \$1.1 billion across 17 countries.⁶³

The digital dimensions of IFFs

IFFs are heterogenous by nature, and commonplace in both developed and developing countries, including in country settings where institutional and regulatory systems are weak and oversight, such as by law enforcement, is limited. Additionally, increasing digitalization and the prevalence of digital technologies across all sectors of national economies enable these illicit flows, though digitalization alone cannot be seen as a driver of IFFs in any causal sense. Rather, such dynamics play an important role in facilitating IFFs at each stage of the process – from the illegal acquisition of money or value creation (e.g., illicitly extracted commodities) to the cross-border transfer and use of its proceeds.⁶⁴ The increasing reliance on digital technologies in the growing share of the service sector in the global economy is an important enabler in this regard. Similarly, the speed and opacity of financial transactions brought by digitalization further complicate accountability and enforcement efforts to ‘follow the money’.⁶⁵

Consider, for instance, the rapid global uptake of cryptocurrencies (particularly during the pandemic), which has become a popular means of payment,

notably in developing economies.⁶⁶ The use and trade in such private, digital currencies is argued to facilitate speedy and affordable remittances, promote financial inclusion, and protect against currency depreciations and inflationary risks. Some critics note that the speed of cryptocurrency transactions may produce some financial instability and offer channels for criminal activities like money laundering, though there is no statistical evidence that criminality in the use of digital currencies is greater than traditional fiat currencies.⁶⁷

Cryptocurrencies may also facilitate tax-related IFFs through the anonymity or pseudonymity of accounts, lacking fiscal oversight and limited enforcement to stem the problem.⁶⁸ Such flows, which as noted above can both be illegal and of dubious legality, are among the most common and harmful form of IFFs and are notably intertwined with the digitalization of the economy. Notwithstanding this, digital transactions leave digital footprints and the ability of cryptocurrencies to play a significant added role in IFFs relies greatly on the means available for law enforcement and regulators to follow such movements.

Additionally, digitalization has reduced the need for companies to be physically present in the markets and countries where they operate, which further complicates efforts to determine where taxable value is created and where it should (and can) be taxed.⁶⁹ Such tax challenges are compounded by the increased reliance on intangible (non-physical) assets such as patents or copyrights, as well as business models that rely on user-generated value, which may facilitate profit shifting to jurisdictions with lower tax burdens and transparency requirements.⁷⁰ The limited global rules and norms vis-à-vis taxation of the digitalized economy further reinforce these dynamics.

One reason developing countries are particularly disadvantaged vis-à-vis IFFs, is their limited ability to impose [sufficient] taxation on digital services as they

are more likely to import digital goods and services yet less likely to host (and tax) digital businesses. Countries that are dependent on natural resources are particularly vulnerable to IFFs, as noted above. This is not only due to their reliance on extractives exports, poor regulatory capacities, and high levels of corruption but also because they often lack the [digital] capacities and resources needed for accurate and verifiable monitoring of natural resource extraction. These are required to avoid under-reporting of extracted resources and to effectively negotiate [and enforce] contracts in a sector known for its secrecy and political influence of industry stakeholders.⁷¹ In 2015, UNCTAD estimated that IFFs linked to extractive commodities exports from Africa (covering 21 countries and eight commodity groups) amount to \$40 billion annually.⁷²



“Fair taxation of digital economic activity requires equitable treatment of digital businesses and business models with traditional business.”

-FACTI Panel Report⁷³

Tackling IFFs in the digital era

Challenges vis-à-vis defining IFFs, and their not entirely illegal status, make effective policy responses a challenge, and point to the need for multifaceted, and holistic responses in ‘sending’ and ‘receiving’ countries alike. Preventing IFFs and mitigating their impacts thus require a combination of criminal and non-criminal (including regulatory, institutional policy and technological) approaches alongside sustained engagement from civil society and media actors. It also requires concerted international cooperation to address their cross-border components.⁷⁴ IFFs have for this reason featured on the multilateral policy agenda for years. Key global initiatives include the [Financial Action Task Force](#) aimed at addressing money laundering and terrorist financing, the [Global Forum on Transparency and Exchange of Information for Tax Purposes](#) to end bank secrecy and tax evasion, and the [Extractive Industry Transparency Initiative](#) to promote open, accountable natural resource management.⁷⁵ Despite these vital initiatives, international action remains inadequate and is often insufficiently coordinated and enforced. This is partly due to a lack of resources (at all levels) to address the issue – a challenge compounded by the COVID-19 pandemic.⁷⁶

Effective coordination on IFFs also requires inclusive investment in digitalization and the practical application of digital technologies. While they are not a substitute for the legal and policy

frameworks, coordination and capacity required to address the problem, digital tools are crucial for preventing, detecting, and disrupting IFFs. They are, for instance, critical for accurate and consistent data collection and monitoring to prevent crimes, and to ensure that legal and regulatory frameworks are ‘fit for purpose’ and able to exercise effective oversight in the digital economy. In this regard, capacity-building efforts in developing countries are important, including to enhance the technical expertise and digital capacities of key institutions such as tax authorities and law enforcement agencies, which further stresses the importance of bridging the digital divide. And in building capacity and strengthening [digitally informed] legal and regulatory frameworks, it is equally important to account for and mitigate risks vis-à-vis data privacy and human rights.⁷⁷

Several initiatives on the global policy agenda (e.g., the [Tax Justice Network](#)) seek to curtail tax avoidance, promote fairness of taxation, and raise domestic tax revenues, including from digital services.⁷⁸ They include efforts to promote digital financial inclusion to broaden the tax base and speed the transition from cash payments, which are more susceptible to extortion and money laundering⁷⁹, to secure digital systems. Some initiatives seek specifically to promote digital (including data) transparency and accountability to reduce the opacity of financial transfers, which are frequently

leveraged to minimize tax burdens. One notable example is the OECD Inclusive Framework on Base Erosion and Profit Shifting (BEPS). Pending full implementation, it seeks to address tax-related IFFs and profit shifting to low tax jurisdictions and increase global corporate income tax revenues (by setting a 15 per cent minimum rate) through the allocation of taxing rights, improved coherence of global norms and rules, as well as transparency in tax environments

and information exchanges.⁸⁰ While groundbreaking, BEPS also faces some criticisms linked to the limited role of developing countries in decision-making, the complexity of standards, and that the proposals are inadequate to shift corporate tax burdens.⁸¹ Nevertheless, BEPS and other efforts to set global corporate minimum tax rates appear to be steps in the right direction and important components in addressing the intractable challenge of IFFs.

5.

Impacts of online disinformation & misinformation

A fragmented information landscape

Disinformation can be understood as the deliberate production and spread of false or misleading information, often for political gain or profit.⁸² In contrast to *misinformation*, it centres on the intent to mislead. The two phenomena, however, tend to overlap as large-scale dissemination of misinformation can also perpetuate disinformation (and vice versa). Disinformation is by no means new but is in today's digital landscape proliferating at a faster pace, in greater volumes, and with increasingly detrimental impacts - influencing the very nature of information that is made pub-

licly available and to whom. It is spread by non-state and state actors alike who conduct (or facilitate) targeted disinformation campaigns⁸³ perpetuated by those who are reluctant or unable to regulate its dissemination.

Today, disinformation is increasingly disseminated by such actors via technology and social media companies who hold much of the world's information. The process usually entails the dissemination of content to users through algorithms⁸⁴ that are designed to increase their engagement with the platform



(thereby increasing advertising revenue). Such engagement-driven algorithms, which tend to be opaque and not subject to much transparency, often promote (or permit) the spread of information that is sensational, divisive, false, or even expounds hateful or extremist narratives. By way of this amplification, disinformation (and misinformation) has the potential to spread faster and generate greater societal impact than traditional news outlets or more trustworthy sources of information, and it

often does.⁸⁵ The uptake of such *information pollution*⁸⁶ can be especially impactful if certain enabling conditions are present. Insights from a UNDP programme found such conditions to include politically polarized environments, the presence of influential diaspora communities, and the existence of information supply gaps (e.g., in how the demand for credible medical information outweighed supply in the early days of the pandemic).⁸⁷

Impacts of mis- and disinformation on freedom of expression and democratic processes

The global proliferation of disinformation and misinformation at scale has come at a high societal cost. It has in different contexts and ways contributed to eroding trust in public institutions and among groups in society, undermining social cohesion. A notable consequence is the public's reduced capacity (and sometimes willingness) to verify the accuracy and credibility of information. This has a direct impact on the public's fundamental ability to “access information and protect fundamental freedoms,” which is an objective explicitly anchored in SDG target [16.10](#). In doing so, disinformation arguably imposes important limitations on the human right to freedom of expression as this right is by necessity predicated on the ability to have access to such expression.⁸⁸ It does so in numerous ways, including by making relevant, timely and truthful information more difficult to access, and by leveraging algorithms to intentionally mislead users or consumers of online content. It also impacts freedom of expression by suppressing speech and opinion of target victims through e.g., harassment or crowding out words or ideas from digital platforms.⁸⁹

Another consequence of disinformation restricting access to information lies in how it exacerbates political and social polarization. Today, societal divisions are [in many countries] starker than in the past, and this is, according to the 2023

Edelman survey, much a consequence of online disinformation. The global survey found, for instance, notable public mistrust in government institutions and media, especially social media, as “a shared media environment has given way to echo chambers, making it harder to collaboratively solve problems.”⁹⁰ And this polarization is increasingly evident in contexts of democratic processes as the amount and virality of disinformation and misinformation often increases during elections, government formations and high-profile debates.⁹¹ A direct consequence of this is limited accessibility and accuracy of information, which inhibits people's ability to make informed political decisions.⁹² In the context of elections, this can take the form of dissemination of false news stories about candidates and the absence of fact-based political debate – both of which can amplify voter confusion and stymie the informed participation required for polls to be free and fair.⁹³

Evidence from the 2023 Varieties of Democracy dataset illustrates how disinformation, polarization and autocratization (or democratic backsliding) reinforce each other. It found that ‘autocratizing’ governments are increasing their use of disinformation to steer citizens' preferences, foment division and garner political support, as polarization in turn induces citizens to abandon democratic principles. Data also showed that

governments' spread of disinformation decreased most in democratizing countries (along with levels of polarization) though the extent of change was more limited, demonstrating how the spread of disinformation is a strain on

democratic resilience.⁹⁴ By perpetuating political disenfranchisement of vulnerable groups, disinformation (and its enablers) presents a significant obstacle to meeting the commitment to leave no one behind.

Oversight and regulation: a complex task

Exercising oversight to address disinformation and misinformation is a complex task, not least because significant economic and political interests are often at stake. And there are no one-size fits all approaches to do so either. Consider, for instance, how specific and contextual (e.g., historical, cultural, or geographic) factors influence how different forms of disinformation are produced, enabled, and disseminated. Moreover, the methodologies and technologies that are used to spread it are continuously evolving, often at a faster pace than the ability of governments to regulate it. These factors stress the importance of flexible and adaptable counter-efforts to increase the amount and reach of truthful and credible information, especially during politically contentious or charged moments like elections.

Such efforts can involve different forms of content moderation or curation, including by social media companies, aimed at blocking user accounts, labeling debunked content, or removing inciteful material.⁹⁵ After the pandemic, several social media platforms expanded their disinformation policies.⁹⁶ While

important, such voluntary 'self-regulation' efforts arguably have limited effect, not only given the sheer volume of disinformation circulating online, but as they don't necessarily address the financial incentives linked to engagement-driven algorithms.⁹⁷ While the scale and scope of regulations vary by context, their impact tends to be limited, compounded by technology companies having opaque disinformation policies subject to limited scrutiny. Other regulatory challenges pertain to enforcement, for instance, jurisdictional challenges and the transboundary nature of digital platforms. Consider also challenges vis-à-vis liability and establishing responsibility of harm: does one, e.g., hold the originator of content or the digital platform that distributed it at fault – and what status do human actions hold when augmented by bots? Similarly, how does one exercise accountability where e.g., sole instances of disinformation feed large-scale misinformation?⁹⁸

Effectiveness and enforcement notwithstanding, regulatory frameworks hold the potential to cause harms greater than those they seek to solve. Even

well-intentioned regulatory responses aimed at restricting [certain] flows of information also risk constraining access to truthful information, thereby subverting people's freedom of expression, while contributing to a shrinking civic space.⁹⁹ Such restrictions have in many instances proved legally and politically contentious, further fortifying political fault lines. For instance, in the context of COVID-19, efforts to reduce pandemic-related disinformation in many places generated heated partisan legal battles over the nature and parameters of freedom of expression.¹⁰⁰ And where regulations have malicious intent, efforts to combat disinformation can be weaponized, e.g., by justifying censorship or delegitimizing political opponents.¹⁰¹

Despite the risks inherent in regulatory responses, safeguarding the right to

freedom of expression and mitigating the harms posed by disinformation are not mutually exclusive acts.¹⁰² Rather, they are integral to broader efforts aimed at building inclusive, and responsive governance systems premised on trust in public institutions and among individuals and groups in society. In this spirit, some observers recommend proactive *community-based methods* to curate internet content (in addition to content moderation). This entails entrusting impartial and trusted human actors (not just algorithms) such as journalists, librarians, or civil society members to help determine accurate and trustworthy sources and content that should be available online with the aim to improve oversight and promote truth oversensationalism.¹⁰³

■ **Box 5: Addressing algorithmic bias and harm**

Some [mostly voluntary] forms of content moderation and curation aim to *(re-)design* algorithms to reward positive interactions across diverse audiences or topics, to 'up-rank' authoritative content or demote harmful posts.¹⁰⁴ Other methods involve [benign] algorithmic profiling to *counter harmful algorithms* (e.g., redirecting searches for harmful content to materials that debunk such themes).¹⁰⁵ These efforts can serve to complement regulatory frameworks aimed at disrupting the flow of information that feeds particular algorithms (i.e., by requiring companies to *only* collect data needed to provide their product or service).¹⁰⁶ Other more far-reaching proposals focus on the financial incentives behind the dissemination of divisive content (and preventing its spread). One such proposal aims to disincentivize the spread of disinformation by taxing social media platforms commensurate with their "polarization footprint" (i.e., measuring aggregate interactions and content not individual violations).¹⁰⁷ The [technical and political] feasibility of such approaches is subject to much debate but points to the complex and intractable factors enabling the spread of harmful disinformation.



6.

Perspectives on conflict in the digital space

How digitalization and conflict intersect

The intersection between digitalization and SDG 16 is notably apparent in the conflict and security domain. It is evident in the increasingly common hybrid forms of warfare,¹⁰⁸ and in the evolution of lethal autonomous weapons systems, new prospects for conflict in outer space, and other hostilities in cyberspace.¹⁰⁹ While these topics are receiving due attention in international policy forums, it is equally important to account for how digitalization enables and perpetuates different forms of conventional conflict, their features and drivers, which is the focus of this section.

Not only does SDG 16's official targets speak directly to violence and conflict (see e.g., **target 16.1**, which aims to “*significantly reduce all forms of violence and death rates everywhere*”), but its core aspiration is to address their root causes. In understanding common conflict drivers and dynamics from a digital perspective, it is important to consider how digital technologies are rarely neutral tools that exist in a vacuum and can simply be deployed for either constructive or nefarious purposes (as they are often held to be). The digital space should not be seen as independent or



external to a given conflict context but rather an integral part of it, and in this sense, 'online' and 'offline' drivers of conflict cannot easily be distinguished.¹¹⁰

This confluence is evident in how algorithm-driven technology companies that possess enormous amounts of people's data can influence the information they present to inform opinions or behaviours. The administration of such data can have a precise bearing on how power and political influence are mediated in society, which can impact how conflicts begin, persist, and end. This

tells us that technology companies can be significant peace and security actors but also points to the social, economic, and political contexts in which they operate. Puig and Morrison label this a 'socio-technological' context and highlight how technology can create enabling conditions that eventually lead to violent conflict.¹¹¹ Only by accounting for the interaction between technology and social or political conflict drivers (e.g., polarizing interactions among social media users) can we identify suitable [peacemaking] responses to these challenges.

Conflict risks and information ecosystems

Socio-technological contexts or issues that bring a heightened risk of conflict can be likened to digital forms of *fragility*. In the sustainable development field, this term is commonly used to identify exposure to different forms of risk (e.g., violence) combined with insufficient mechanisms (e.g., by public institutions) to manage or mitigate those risks.¹¹²

Such digital fragility can be found in the vulnerability of *information ecosystems*, which facilitate the flow of [accurate and timely] information across society.¹¹³ Here, social media platforms stand out as the volume, nature, and speed of information they disseminate can be key sources of digital fragility and pose new challenges for initiating and sustaining peace.¹¹⁴ Consider, for instance, online efforts to recruit violent extremists or how misinformation and disinformation contribute to human rights abuses and can destabilize already fragile contexts. Research in this area has pointed to linkages between social media misinformation, political instability and risks of mass violence and atrocities.¹¹⁵ Such risks are prominent enough for the UN Secretary-General to label disinformation “*a clear and present global threat*” noting that “*digital platforms are being misused to subvert science and spread disinformation and hate to billions of people, fueling conflict, threatening democracy and human rights...*”¹¹⁶

Social media platforms and content not only amplify conflict risk but also bring

the potential to compound and alter existing conflict landscapes by shifting the dynamics between opposing parties, including by capitalizing on divisions, frustrations, and fears and feeding divisive narratives of militias and armed groups, including terrorist and violent extremists.¹¹⁷ Mercy Corps has found that social media can be particularly weaponized under certain conditions, including where sectarian and ethnic tensions are rife, or where multiple identities overlap with existing conflicts. Social media also brings a high propensity for violence and conflict where dysfunctional or oppressive government systems foster grievances and trust deficits, or sanction mass violence.¹¹⁸

A well-publicized example of this are the accusations against Meta (Facebook’s parent company) of profiting from the display and amplification of inflammatory content against the Rohingya minority in Myanmar – as the government pursued a targeted campaign of mass violence against them in the years leading up to 2017.¹¹⁹ As noted in the Report of the independent international fact-finding mission on Myanmar: “*The role of social media is significant. Facebook has been a useful instrument for those seeking to spread hate, in a context where, for most users, Facebook is the Internet*”.¹²⁰ Following the coup in February 2021, the platform has taken significant steps to remove pages linked to the military junta.¹²¹

Digitally enabled conflict actors and spoilers

Digital forms of fragility can also be attributed to key actors and influencers with the ability to drive or alter conflict trajectories. The type of actors, their interests and operational capacities will inevitably vary by context, but one feature they have in common is the ability to generate and exploit [digital] risk factors, including by shaping perceptions of contentious issues or mobilizing constituencies.¹²²

Low barriers to entry offered by social media platforms enable these risk factors and provide actors with avenues to e.g., manipulate elections or influence media narratives that they may otherwise not have had. Importantly, they bring new opportunities for potential spoilers (conflict actors whose power or interests are vested in the continuation of conflict) to derail peace processes or undermine the peaceful settlement of disputes.

Digitally enabled conflict actors may also include powerful state actors and government bodies who can significantly influence and control information ecosystems. This may take the form of propaganda and information campaigns aimed at silencing dissent, discrediting reformers, or meddling in external affairs -- efforts which are all premised on strict control of the flow of information.¹²³

As Mandawille and Schiwal of the United States Institute for Peace (USIP) point out, counter to commonly held views *“most people experience the internet as a rigid, highly organized and closely monitored medium of expression and connection dominated by corporate tech giants and – perhaps somewhat counterintuitively – state actors.”*¹²⁴

Box 6: Digitalization as an enabler of violent extremism

Vulnerability in [digital] information ecosystems has also enabled the proliferation of violent extremist organizations who capitalize on [perceived] political and economic exclusion and divisive issues in society for their recruitment and engagement.¹²⁵ The pandemic provides a unique opportunity in this regard, as observed by UNICRI: *“Violent extremist actors have adapted their online and offline narratives in response to the pandemic”* adding that *“notably those located in Western Europe – have exploited the pandemic for recruitment and propaganda purposes.”*¹²⁶ Extremist views and hate speech in the digital space are spread in numerous ways, including via social media and online platforms, as well as entertainment channels with seemingly benign purposes.

Here [USIP](#) points to [social clubs and gaming channels](#) as sites of political and ideological indoctrination for extremist groups who leverage these for recruitment purposes or to generate financial support. The UN Office of Counter-Terrorism (UNOCT) has echoed this issue and noted that with over three billion gamers worldwide, violent extremists exploit gaming platforms for their own ends, including propaganda, communication, recruitment, and the perpetration of violence. UNOCT however, points out that while there is increasing evidence of extremists from varying ideological backgrounds using gaming related content and platforms, *“research on the reasons for and implications of the gaming-extremism nexus is slim and largely theoretical.”*¹²⁷



Responding to conflict in the digital space

A necessary first step in preventing and responding to [digitally enabled] conflict for all actors is to apply a digital lens in *understanding and analysing* it. With respect to conflict fuelled by social media, there are several approaches that merit attention.

For starters, it is important to account for the digital divide and *variations in social media access and usage* over time, and across different geographies, demographics, and social groups. Here USIP notes there are considerable variations in misinformation and disinformation between non-state and state-actors, as well as limited research on effective strategies (including peacebuilding strategies) to counter them.¹²⁸

It is equally important to understand *patterns of social media usage* in different settings and the extent to which social media channels are strictly controlled, insufficiently regulated, or among the only avenues to access the internet. Furthermore, it is instructive to distinguish between *threats emanating from social media platforms and the users of those platforms*. Just as social media content can be weaponized by shaping off-line narratives, the opposite also holds true in how [off-line] social networks can inform social media narratives. Research by Mercy Corps found that “*societal relationships provide a shortcut for assessing the plausibility of social media news stories.*”¹²⁹

Accurate, nuanced conflict analysis is a pre-requisite for targeted programme and policy responses, be it to social media fuelled conflict or violent extremism. Common responses include ‘signalling’ measures to fact-check or counter hateful messaging through online platforms or [traditional] media outlets (as illustrated in section 4 above) and are mainly aimed at removing or diminishing the content in question.¹³⁰ Regulatory challenges notwithstanding, such efforts can be hugely difficult (and costly), particularly in regions with limited media freedom, and considering how context (and language) specific hate speech can be.

To illustrate, according to a whistleblower some 87 per cent of Facebook’s spending to counter misinformation is aimed at English speakers, which only represents nine per cent of users.¹³¹ And as noted above, moderating, or curating content to make it less visible and impactful does not necessarily address underlying conflict drivers. Mindful of this, many look to social cohesion campaigns and education to mitigate online conflict drivers or counter extremist propaganda, by equipping citizens with critical thinking skills.¹³² Others seek to shape the [digital] parameters of peace processes themselves, such as the Centre for Humanitarian Dialogue, which as part of its mediation work develops e.g., social media standards and codes of

conduct in elections to counter the negative impacts of disinformation.¹³³

Relatedly, peacemakers and advocates must be adept at *using* digital technology, including social media, and have the skills, capacities, and resources to do identify digital forms of fragility and conflict risk (especially considering how digital technology tools are rarely neutral). This point is particularly salient for policymakers and regulators who must be sufficiently flexible to 'catch up' with innovations and developments in the information landscape, including in unstable and at-risk environments. To this end, it is also critical that relevant legal, policy and programmatic frameworks apply a risk-informed and conflict-sensitive lens to ensure that responses do not inadvertently contribute to so-

cial divisions and reinforce the very dynamics they seek to overcome. In this regard, the launch of the ECOWAS Commission's initiatives to leverage technology-informed programming to strengthen early warning systems and build peace in the region is a positive example.¹³⁴ With respect to countering and preventing violent extremism, this means avoiding overly securitized responses that can lead to human rights abuses and further marginalize vulnerable groups (including in the digital space). Instead, such efforts must emphasize development and political strategies aimed at addressing grievances (real or perceived) used to motivate further recruitment, including issues linked to discrimination, exclusion, and lack of state accountability.¹³⁵

7.

Reflections moving forward

Digital social contracts

In 2023, amidst multiple and cascading global crises, hard fought development gains are either stalling or reversing, notably in areas pertaining to peace, justice, and inclusion. As illustrated in the sections above, such challenges relating to inequality, freedom of expression, polarization, extremism, and conflict are all characterized by digitalization in different ways. These challenges, and the digital factors that inform them, also reflect strains on social contracts in society, i.e., the rules and obligations dictating the relationships between those who govern and the governed. Conven-

tional understandings of the social contract tend to have a somewhat binary 'state-society' emphasis.¹³⁶ But in understanding the fractured nature of today's social contracts, and in devising solutions to strengthen them, we must take a broader view and recognize their digital components as well. This means accounting for the different ways in which power is exercised in society, including online, and how such power is mediated between all actors, including powerful technology companies and the entities that [can] check their power when used for unfair or harmful purposes.



A manifestation of such digitally informed social contracts, and how they can be strengthened in practice, can be found in a National Digital Compact. Such a Compact, as advocated by the Pathways for Prosperity Commission¹³⁷ can take different forms, e.g., goals or commitments. But at its core, it entails a shared [and ideally codified] vision amongst stakeholders from government, the private sector and civil society of the nature and process of digital transformation in society.¹³⁸ Such a

wholesale transformation may reasonably be accompanied by large-scale economic, social [and political] change, and will require coordination and balancing of complex trade-offs as some segments of society may benefit and others lose out. To mitigate different forms of exclusion (e.g., via investments, regulations, or other prioritizations), the process must be people-centred to ensure buy-in and that all parties have a stake in digitalization and technology enabled development and growth.

Box 7: A Global Digital Compact

A scaled, multilateral version of a National Digital Compact can be found in the UN Secretary-General's call for a Global Digital Compact for which global consultations are underway.¹³⁹ Anchored in international legal and normative frameworks, it would articulate a shared vision for an open, free, secure, and human-centred digital future. The Compact would be led by UN Member States and create a framework based on existing digital cooperation processes, setting out principles and objectives for achievable, multi-stakeholder actions. The Secretary-General has proposed a series of objectives to this end, which include (but are not limited to) universal meaningful connectivity, digital cooperation to advance the SDGs, putting human rights at the heart of digital transformation, and safeguarding the free and shared nature of the internet.

Responsive and people-centred digital governance

A [digitally informed] social contract also requires governance systems that are sufficiently inclusive, responsive, and accountable to ensure that digital transformation accommodates people's everyday needs and generates equitable societal benefit. Such systems must reasonably include legal and regulatory frameworks that can exert timely, and meaningful accountability over all actors, including technology companies (and the online content under their purview) albeit without stifling innovation. This may entail, for instance, enacting policies and laws to incentivize affordable and equitable internet connectivity (as new technologies develop) while also ensuring competitive markets and reasonable taxation.¹⁴⁰ Further, it calls for addressing contentious issues linked to data governance and striking a balance in responding to disinformation while defending freedom of expression.¹⁴¹

There are no templates or one-size-fits-all approaches to these challenges. It is, however, important that they reflect societal norms and public expectations while adhering to fundamental human rights and principles of accountability, transparency, and inclusion. As digitalization has a clear bearing on human rights outcomes (be it their violation or protection and enjoyment), [digital] governance frameworks must be firmly anchored in human rights norms, laws, and standards.¹⁴² To this end, National Human Rights Institutions, independent bodies established by law to advise and hold governments to account in promoting and protecting human rights (in line with SDG target 16.a), can play an important role in e.g., ensuring policy coherence on digital matters and in addressing hate speech and discrimination on digital platforms.

A people-centred perspective is also key in identifying groups that are left behind and ensuring their meaningful inclusion in all aspects of digitalization and digital transformation. This means accounting for the perspectives, concerns, and priorities of all people and communities, including marginalized and excluded groups, and making sure that [digital] policies are inclusive in both substance and process. Priorities in this regard include (per the Pathways for Prosperity's Digital Roadmap)¹⁴³ digitally empowering citizens (e.g., through trainings),

building accountable digital systems to ensure personal data is secure, and ensuring that anyone left behind benefits from a social safety net. It also means building foundational digital systems (e.g., for legal ID's), to enable citizens to access basic services and equal opportunities. Finally, ensuring inclusivity in digital governance requires tackling harmful social norms that can replicate or amplify existing inequalities. This includes removing all barriers, including for women and girls, to freely use and access digital technologies.

Issues for further exploration

The challenges highlighted in this paper are illustrative of the nexus between SDG 16 and digitalization, but they are by no means exhaustive. There are several emerging disciplines and important areas of inquiry that speak to this

nexus and merit further exploration and analysis. Several of these align with existing priorities held at UNICRI and will continue to feature in future research and analysis.¹⁴⁴ These include, but are not limited to:

-
- i. Evolving manifestations of inequality (of opportunity and outcome) and exclusion in the digital era and their implications for the commitment to leave no one behind.
-
- ii. Frontier technologies, including artificial intelligence and quantum technologies, and the risks they bring vis-à-vis building more peaceful, just, and inclusive societies.
-
- iii. How rapid digitalization is both expanding and constraining the parameters of democratic systems, and how to safeguard the principles of equality, accountability, and voice.
-
- iv. The ways in which advanced technologies and digital developments are changing the nature of armed conflict, and warfare, including hybrid and cyber-focused conflict.
-
- v. The role of digital transformation in delivering basic services in a more equitable, and inclusive manner and strengthening (gender-responsive) public institutions.
-
- vi. How digital tools are used in the furtherance of organized crime, and the role of such tools in combating organized crime.
-
- vii. Online human rights-abuses, including discrimination, hate speech and gender-based violence online, and applying human rights frameworks in addressing these challenges.

Endnotes

- 1** United Nations, *The Sustainable Development Goals Report 2023: Special Edition*, 2023, p8.
- 2** For examples of how digitalization can advance sustainable development, see ITU webpage, *Digital technologies to achieve the UN SDGs*: www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx.
- 3** International Telecommunication Union (as part of #ICT4SDG campaign), *Fast-forward progress – Leveraging tech to achieve the global goals*, September 2017, p10.
- 4** See Pathfinders for Peaceful, Just and Inclusive Societies, *The Roadmap for Peaceful, Just and Inclusive Societies*, 2019. For more on SDG 16 interlinkages, see: UNDP, Oslo Governance Centre, *SDG 16 Interlinkages - Summary of Findings*, July 2021.
- 5** For an example of how complementary data sources and monitoring processes to are used to track progress on SDG 16, see SDG 16 Data Initiative Report 2022, *Are we on track to meet the 2030 Agenda?* 2022.
- 6** Based on the decline in homicide rates between 2015-2020, the UN projected an overall 19% decline by 2030. For more on global homicide rates, see UNODC, *Data 4 Matters: Monitoring SDG 16, A gender perspective*, September 2022, p.4. See also United Nations, *The Sustainable Development Goals Report 2023: Special Edition*, 2023, p44.
- 7** Transparency, Accountability, and Participation (TAP) for 2030 Network, *Halfway to 2030 Report on SDG 16+, A Civil Society Assessment of Progress Towards Peaceful, Just and Inclusive Societies*, 2023, p58-59.
- 8** While figures on the global ‘justice gap’ are imprecise given data limitations, it is thought to be considerable. See Pathfinders for Peaceful, Just and Inclusive Societies, *Justice for All and the Social Contract in Peril*, July 2021.
- 9** United Nations, *The Sustainable Development Goals Report 2023: Special Edition*, 2023, p44.
- 10** Report of the Secretary-General (Advanced unedited version), *Progress towards the Sustainable Development Goals: Towards a Rescue Plan for People and Planet*, May 2023, p7.
- 11** Southern Voice, UNDP, *Emerging Trends on SDG 16 in the Context of COVID-19*, July 2021, summary of online discussions, available at: www.undp.org/policy-centre/oslo/publications/emerging-trends-sdg-16-context-covid-19.
- 12** There is no universal or commonly applied definition of digitalization. This understanding draws *in part* on the definition of the term used in UNDP’s Digital Strategy (2022-2025) and places additional emphasis on the societal factors that enable the use or misuse of digital technologies.

- 13** United Nations, Secretary-General's Roadmap for Digital Cooperation, June 2020, p5-8, p23.
- 14** International Telecommunication Union Datahub webpage, available at: <https://datahub.itu.int/data/?e=701&c=&i=11624>. This figure “refers to the proportion of individuals who used the internet from any location in the last three months” (via fixed or mobile network).
- 15** World Bank Group, *World Development Report 2021: Data for Better Lives*, 2021, p11.
- 16** Economist Impact, *The Inclusive Internet Index 2022* (commissioned by Meta); for more on this topic, see International Peace Institute (Roesch), *SDG Zero? A People-Centered Approach to Universal Connectivity*, April 2021, p3.
- 17** International Telecommunication Union, *Measuring digital development, Facts and Figures, 2022*, piii.
- 18** Declaration of the Eighth World Telecommunications Development Conference, *Connecting the Unconnected to Achieve Sustainable Development*, Kigali, Rwanda, June 2022.
- 19** Broadband Commission, *What is Universal Connectivity?* Available at: www.broadband-commission.org/universal-connectivity/#:~:text=Meaningful%20Universal%20Connectivity%20means%20that,to%20reliable%20and%20safe%20internet.
- 20** International Peace Institute (Roesch), *SDG Zero? A People-Centered Approach to Universal Connectivity*, April 2021, p3.
- 21** UN Department of Economic and Social Affairs, Decade of Action Policy Brief No 92, *Leveraging digital technologies for social inclusion*, February 2021, p1-2.
- 22** Southern Voice, UNDP, *Emerging Trends on SDG 16 in the Context of COVID-19*, July 2021, summary of online discussions, available at: www.sdg16hub.org/system/files/2021-07/KeyMessages.pdf.
- 23** Pathfinders for Peaceful, Just and Inclusive Societies, *From Rhetoric to Action, Delivering Equality and Inclusion*, September 2021, p45.
- 24** International Telecommunication Union, *Facts and Figures 2022* webpage, p3, available at: www.itu.int/itu-d/reports/statistics/facts-figures-2022/.
- 25** World Bank Group, *World Development Report 2021: Data for Better Lives*, 2021, p164.
- 26** UN Women Executive Director Sima Bahous, *Digital rights are women's rights*, Op-ed: available at: <https://www.unwomen.org/en/news-stories/op-ed/2023/05/op-ed-digital-rights-are-womens-rights>.
- 27** United Nations Commission on the Status of Women, Sixty-seventh session, Agreed Conclusions, *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls*, March 2023.
- 28** Pew Research Centre, *8 charts on internet use around the world as countries grapple with COVID-19*. Available at: https://www.pewresearch.org/short-reads/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/ft_2020-04-02_globalinternet_04/.

- 29** Bringing affordable connectivity to hard-to-reach areas is proposed by the UN Secretary-General in Our Common Agenda Policy Brief #5, *A Global Digital Compact – an Open, Free and Secure Digital Future for All*, May 2023, p13.
- 30** These, and related recommendations, are outlined in Pathways for Prosperity Commission, *The Digital Roadmap, How developing countries can get ahead*.
- 31** United Nations Commission on the Status of Women, Sixty-seventh session, Agreed Conclusions, *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls*, March 2023, p12.
- 32** UN Secretary-General in Our Common Agenda Policy Brief #5, *A Global Digital Compact – an Open, Free and Secure Digital Future for All*, May 2023, p3.
- 33** These and related normative concerns are discussed in Pathfinders for Peaceful, Just and Inclusive Societies (Bailey, Nyabola), *Digital Equity as an Enabling Platform for Equality and Inclusion*, Policy Brief, June 2021, p11.
- 34** United Nations, Report of the Secretary-General, *Our Common Agenda*, 2021, p6.
- 35** United Nations Human Rights, Office of the High Commissioner, *It May be Time to Reinforce Universal Access to the Internet as a Human Right, Not Just a Privilege*, High Commissioner tells Human Rights Council, Press release, March 2023, available at: www.ohchr.org/en/news/2023/03/it-may-be-time-reinforce-universal-access-internet-human-right-not-just-privilege-high.
- 36** Article 6 of the Universal Declaration of Human Rights notes that “Everyone has the right to recognition everywhere as a person before the law.”
- 37** UN Department of Economic and Social Affairs, Decade of Action Policy Brief No 172, *Covid-19 pandemic disruption, implications on the full deployment of the United Nations legal identity agenda*, January 2022.
- 38** World Bank Blogs (Marskell, Eichholtzer, Desai), *Digital ID systems can help vaccination deployment, but should never be a barrier to access*, March 2021, available at: <https://blogs.worldbank.org/digital-development/digital-id-systems-can-help-vaccination-deployment-should-never-be-barrier>.
- 39** World Bank Blogs (Clark, Diofasi, Casher), *850 million people globally don't have ID – why this matters and what we can do about it*, February 2023, available at: <https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about>.
- 40** McKinsey Global Institute, *Digital identification – a key to inclusive growth*, April 2019, p1, p23.
- 41** Devex Blog (Xiu, Lister, UNDP) Opinion, *Ensuring legal ID for all is a step to leaving no one behind*, June 2023, available at: www.devex.com/news/opinion-ensuring-legal-id-for-all-is-a-step-to-leaving-no-one-behind-105678.

- 42** See UNICRI, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*, November 2022.
- 43** For more on definitions and terminology vis-à-vis legal identity, see World Bank Group, *Principles on Identification for Sustainable Development: Toward the Digital Age*, November 2022, p4.
- 44** Devex Blog (Xiu, Lister, UNDP) Opinion, *Ensuring legal ID for all is a step to leaving no one behind*, June 2023, available at: www.devex.com/news/opinion-ensuring-legal-id-for-all-is-a-step-to-leaving-no-one-behind-105678.
- 45** UNDP webpage, *Malawi's foundational legal identity system sets the stage for a more efficient and responsible digital future*, May 2022, available at: www.undp.org/digital/stories/malawi%E2%80%99s-foundational-legal-identity-system-sets-stage-more-efficient-and-responsible-digital-future; Center for Global Development (Malik) *Malawi's Journey Towards Transformation: Lessons from its National ID Project*, August 2020, available at: www.cgdev.org/publication/malawis-journey-towards-transformation-lessons-its-national-id-project.
- 46** See Context (Pensulo), *As Malawi Issues IDs for children, privacy concerns rise*, December 2022, available at: www.context.news/surveillance/as-malawi-issues-ids-for-children-privacy-concerns-rise.
- 47** Terminology and definitions of IFFs are discussed in The Global Initiative Against Organized Crime, (Hunter), *Measures that Miss the Mark, Capturing the proceeds of crime in illicit financial flow models*, June 2018.
- 48** This general definition is adopted by several international organizations. For more information on definitions, see U4 Anti-corruption webpage, www.u4.no/topics/illicit-financial-flows/basics, and Global Financial Integrity webpage, <https://gfintegrity.org/issue/illicit-financial-flows/>. Note that not all definitions characterize IFFs as *cross-border* in nature as significant losses and harms can also result from IFFs occurring within a specific country.
- 49** See Global Financial Integrity Money Laundering webpage, <https://gfintegrity.org/issue/money-laundering/>.
- 50** Ibid.
- 51** Campbell, Lord, *Following the Money: Illicit Financial Flows and SDG 16.4*, p9-10 (in Blaustein et al (eds) *The Emerald Handbook on Crime, Justice and Sustainable Development*, 2020).
- 52** UN Inter-Agency Task Force on Financing for Development, Background Note on Illicit Financial Flows, available at, www.un.org/esa/ffd/wp-content/uploads/2017/02/Background-note-on-illicit-financial-flows.pdf.
- 53** This more comprehensive view is adopted by the UN's High-Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda (FACTI Panel) – the senior most international body on IFFs. Similarly, International Financial Institutions such as the International Monetary Fund refers to *Illicit and tax avoidance related flows* (ITAFF).
- 54** For more information on this statistical measurement framework, see UNODC illicit financial flow webpage, available at: www.un.org/esa/ffd/wp-content/uploads/2017/02/Background-note-on-illicit-financial-flows.pdf.

- 55** Further details on the first official data on illicit financial flows are available on the UNCTAD webpage at: <https://unctad.org/news/first-ever-official-data-illicit-financial-flows-now-available>. Additional IFF commentary is available at UNCTAD's SDG Pulse webpage, at: <https://sdgpulse.unctad.org/illicit-financial-flows/>.
- 56** See UNCTAD webpage: <https://unctad.org/news/first-ever-official-data-illicit-financial-flows-now-available>.
- 57** UN FACTI Panel, Report of the High Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p9.
- 58** Figure available on Global Financial Integrity webpage, at: <https://gfinintegrity.org/issue/illicit-financial-flows/>.
- 59** UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa*, Economic Development in Africa Report 2020, p2, p181. And according to Brookings (Signé, Sow, Madden), between 1980 and 2018, sub-Saharan Africa received nearly \$2 trillion in foreign direct investment (FDI) and official development assistance (ODA), but emitted over \$1 trillion in illicit financial flows, See *Illicit financial flows in Africa*, policy brief March 2020, available at: www.brookings.edu/wp-content/uploads/2020/02/Illicit-financial-flows-in-Africa.pdf.
- 60** UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa*, Economic Development in Africa Report 2020, p152-153.
- 61** Governance-related impacts of IFFs are explored in Report of the High Level Panel on Illicit Financial Flows from Africa (commissioned by the AU/ECA Conference of Ministers of Finance, Planning and Economic Development), *Illicit Financial Flows* p51-52. See also UN FACTI Panel, Report of the High Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p10, 14.
- 62** UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa*, Economic Development in Africa Report 2020, p104-105. See also UN FACTI Panel, Report of the High Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p7, 21.
- 63** Transparency International, COVID-19: Documented corruption and malfeasance cases, September 2020, available at: <https://images.transparencycdn.org/images/COVID-19-Documents-corruption-and-malfeasance-cases.pdf>. For more on IFFs during COVID-19, see UN FACTI Panel, Report of the High Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p3.
- 64** See World Development Report 2016 background paper (Tropina), *Digital Dividends, Do Digital Technologies Facilitate Illicit Financial Flows?* 2016.
- 65** Report of the High Level Panel on Illicit Financial Flows from Africa (commissioned by the AU/ECA Conference of Ministers of Finance, Planning and Economic Development), *Illicit Financial Flows*, p68.
- 66** UNCTAD news webpage, *UNCTAD spells out actions to curb cryptocurrencies in developing countries*, August 2022, available at: <https://unctad.org/news/unctad-spells-out-actions-to-curb-cryptocurrencies-in-developing-countries>.

[tions-curb-cryptocurrencies-developing-countries.](#)

67 It is thought that the share of illicit use of cryptocurrencies has in fact decreased over time while their (illicit) usage in absolute terms remains on the rise. Europol notes how (depending on approaches and methodologies in analysis) estimates of illicit use of cryptocurrencies range widely from 0.34% (private sector) to 23% (academia) of transactions. See Europol, Spotlight, Cryptocurrencies: Tracing the Evolution of Criminal Finances, p3-5.

68 UNCTAD policy brief no 100, *All that glitters is not gold: The high cost of leaving cryptocurrencies unregulated*, June 2022, p2-3.

69 UN FACTI Panel, Report of the High-Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p7, 23.

70 UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa*, Economic Development in Africa Report 2020, p84; Report of the High-Level Panel on Illicit Financial Flows from Africa (commissioned by the AU/ECA Conference of Ministers of Finance, Planning and Economic Development), *Illicit Financial Flows* p28, 37.

71 Report of the High-Level Panel on Illicit Financial Flows from Africa (commissioned by the AU/ECA Conference of Ministers of Finance, Planning and Economic Development), *Illicit Financial Flows* p56, 67.

72 UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa*, Economic Development in Africa Report 2020, p40-51.

73 UN FACTI Panel, Report of the High-Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p24.

74 UNICRI, *Drivers of Illicit Financial Flows*, 2018, p39; U4 Anti-corruption webpage, www.u4.no/topics/illicit-financial-flows/basics.

75 UNICRI is another notable actor in this space, bringing expertise in assisting countries in the recovery of illicitly acquired assets and addressing IFFs. For examples of its work, see UNICRI, *Illicit Financial Flows and Asset Recovery in the Eastern Partnership Region, A Mapping of Needs and Recommendations*, 2022.

76 UN FACTI Panel, Report of the High-Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p2.

77 World Development Report 2016 background paper (Tropina), *Digital Dividends, Do Digital Technologies Facilitate Illicit Financial Flows?* 2016, p17, 20.

78 For a summary of global initiatives since the mid-2000's, see UNICRI, *Drivers of Illicit Financial Flows*, 2018, p1-5.

79 A 2022 Study by Global Financial Integrity found extortion payments in the Northern Triangle to amount to over US\$1billion annually, and notes that cash-intensive businesses and payments are common in extortion practices. See press release, September 2022 at: <https://gfintegrity.org/press-release/extortion-payments-in-northern-triangle-amount-to-over-us1-billion-per-year-study-finds/>.

- 80** Inclusive Framework on Base Erosion and Profit Shifting web page, available at: www.oecd.org/tax/beps/. See also OECD, Tax Challenges Arising from Digitalisation – Economic Impact Assessment, Inclusive Framework on BEPS, 2020, p12-13.
- 81** See UNICRI, *Drivers of Illicit Financial Flows*, 2018, p4-5; UN FACTI Panel, Report of the High Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, February 2021, p23-25; and UNCTAD, *Tackling Illicit Financial Flows for Sustainable Development in Africa*, Economic Development in Africa Report 2020, p97.
- 82** While there's no universally accepted definition of disinformation, Media Manipulation Casebook offers a working definition (and of related terms): https://mediamanipulation.org/definitions?term_name=disinformation.
- 83** See UNICRI, *Stop the Virus of Disinformation*, November 2020.
- 84** There is no universally accepted definition of the term (including as it has numerous disparate applications), but it can in its most rudimentary form be understood as a set of rules that define a sequence of operations. For more on definitional parameters, see: www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/.
- 85** UNDP, Strategic Guidance, *Information Integrity: Forging a pathway to Truth, Resilience and Trust*, February 2022.
- 86** UNDP defines information pollution as disinformation, misinformation and/or mal-information, which is information based on real facts, but manipulated to inflict harm on a person, organization or country. See *ibid*, p4.
- 87** UNDP, Oslo Governance Centre, *Polluting hearts and minds: The lessons learned from mapping information pollution across 8 country contexts*, 2022, p6-7.
- 88** Article 19 of the Universal Declaration of Human Rights and article 19 (2) of the Covenant also protect the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds.
- 89** Harvard Shorenstein Center (Donovan, Dreyfuss, Lim, Friedberg), written testimony to the UN Special Rapporteur's Annual Thematic Report (presented to the Human Rights Council's 47th session), *Disinformation at Scale Threatens Freedom of Expression Worldwide*, 2021, p3-4. See also OHCHR, *Stories, Freedom of expression is key to countering disinformation*, November 2022, available at: www.ohchr.org/en/stories/2022/11/freedom-expression-key-countering-disinformation.
- 90** Edelman Trust Institute, *2023 Edelman Trust Barometer Global Report*, available at: www.edelman.com/trust/2023/trust-barometer.
- 91** National Democratic Institute, *Disinformation and Electoral Integrity, A Guidance Document for NDI Elections Programs*, May 2019.
- 92** UNDP, Strategic Guidance, *Information Integrity: Forging a pathway to Truth, Resilience and Trust*, February 2022, p2, p12.

- 93** National Democratic Institute, *Disinformation and Electoral Integrity, A Guidance Document for NDI Elections Programs*, May 2019.
- 94** Varieties of Democracy institute, Democracy Report 2023, *Defiance in the Face of Autocratization*, p25-26.
- 95** Build Up and Ashoka Tech & Humanity (Puig), *Societal Divides As a Taxable Negative Externality of Digital Platforms*, 2022, p10.
- 96** Puig, Morrison, *Understanding Digital Conflict Drivers* p192-193, (Ch. 9 in Mahmoudi et al. (eds) *Fundamental Challenges to Global Peace and Security*, Springer), 2022.
- 97** Build Up and Ashoka Tech & Humanity (Puig), *Societal Divides As a Taxable Negative Externality of Digital Platforms*, 2022, p10. For more on the role of transparency in social media regulation, see Brookings commentary: *Transparency is essential for effective social media regulation*, November 2022.
- 98** More information on challenges vis-à-vis regulatory effectiveness in the era of digitalization are explored by OECD on its webpage at: www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf.
- 99** Summary report, UNDP/UNESCO 'Future of Governance' consultation, *Forging a Path to a Better Information Ecosystem – Effective Governance, Media, Internet and Peacebuilding Responses to Disinformation*, October 2020.
- 100** This New York Times article illustrates how limits of freedom of expression vis-à-vis pandemic-related online disinformation has become a highly partisan issue in the United States: www.nytimes.com/2023/02/09/business/free-speech-social-media-lawsuit.html.
- 101** OHCHR, Stories, *Freedom of expression is key to countering disinformation*, November 2022, available at: <https://www.ohchr.org/en/stories/2022/11/freedom-expression-key-countering-disinformation>.
- 102** Harvard Shorenstein Center (Donovan, Dreyfuss, Lim, Friedberg), written testimony to the UN Special Rapporteur's Annual Thematic Report (presented to the Human Rights Council's 47th session), *Disinformation at Scale Threatens Freedom of Expression Worldwide*, 2021.
- 103** This proposal is advocated by Donovan, Dreyfuss, Lim, Friedberg (ibid). Similar ideas include digital "lockers" where publicly shared (incriminating, or illegal) content that has been removed can be preserved for future research and investigation by select actors to help address impacts of disinformation. See: Foreign Policy (Donovan, Lim) *The Internet Is a Crime Scene*, January 2021, available at: https://foreignpolicy.com/2021/01/20/internet-crime-scene-capitol-riot-data-information-governance/#cookie_message_anchor.
- 104** Build Up and Ashoka Tech & Humanity (Puig), *Societal Divides As a Taxable Negative Externality of Digital Platforms*, 2022, p12. see also Facebook commentary on the types of content it 'demotes', July 2023, available at: <https://transparency.fb.com/en-gb/features/approach-to-ranking/types-of-content-we-demote/>.
- 105** Puig, Morrison, *Understanding Digital Conflict Drivers* p194, (Ch. 9 in Mahmoudi et al. (eds) *Fundamental Challenges to Global Peace and Security*, Springer), 2022.

- 106** More information on such ‘data minimization’ (including how they are implemented in the European Union) can be found at the Access Now webpage: www.accessnow.org/press-release/data-minimization-guide/.
- 107** Build Up and Ashoka Tech & Humanity (Puig), *Societal Divides As a Taxable Negative Externality of Digital Platforms*, 2022, p12.
- 108** This term implies combined conventional and unconventional measures, e.g., military operations, cyber warfare, disinformation campaigns, and economic pressure. For more, see Global Security Review (Ball), *The Changing Face of Conflict: What is Hybrid Warfare?* July 2023.
- 109** These are all examples of how new technologies and emerging domains can be weaponized and have been highlighted by the UN Secretary-General as key areas of concern: See United Nations, Our Common Agenda Policy Brief #9, *A New Agenda for Peace*, July 2023, p26-29.
- 110** USIP Commentary (Mandaville, Schiwal), *A New Approach for Digital Media, Peace, and Conflict*, February 2023, available at: www.usip.org/publications/2023/02/new-approach-digital-media-peace-and-conflict.
- 111** Puig, Morrison, *Understanding Digital Conflict Drivers* p71-173, (Ch. 9 in Mahmoudi et al. (eds) *Fundamental Challenges to Global Peace and Security*, Springer), 2022. See also USIP Commentary (Mandaville, Schiwal), *A New Approach for Digital Media, Peace, and Conflict*, February 2023, available at: www.usip.org/publications/2023/02/new-approach-digital-media-peace-and-conflict.
- 112** For definitions and further information see OECD page: www.oecd.org/dac/states-of-fragility-fa5a6770-en.htm.
- 113** UNDP, Strategic Guidance, *Information Integrity: Forging a pathway to Truth, Resilience and Trust*, February 2022, p4, 12.
- 114** Conciliation Resources, Accord Issue 29, *Pioneering peace pathways, Making connections to end violent conflict*, August 2020, p79.
- 115** Stimson (Hook, Verdeja), *Social Media Misinformation and the Prevention of Political Instability and Mass Atrocities*, July 2022.
- 116** United Nations, Secretary-General’s opening remarks at press briefing on Policy Brief on Information Integrity on Digital Platforms, June 2023, available at: www.un.org/sg/en/content/sg/speeches/2023-06-12/secretary-generals-opening-remarks-press-briefing-policy-brief-information-integrity-digital-platforms.
- 117** Mercy Corps, *Social Media and Conflict: Understanding Risks and Resilience, An Applied Framework for Analysis*, July 2021, p9. See also United Nations, Our Common Agenda Policy Brief 8, *Information Integrity on Digital Platforms*, June 2023, p11.
- 118** Mercy Corps, *Social Media and Conflict: Understanding Risks and Resilience, An Applied Framework for Analysis*, July 2021, p9-10.
- 119** Amnesty International, *The Social Atrocity – Meta and The Right to Remedy for the Rohingya*, September, 2022.

- 120** UN Human Rights Council, Thirty-ninth session, *Report of the independent international fact-finding mission on Myanmar*, September 2018, p14.
- 121** International Crisis Group, Report, Myanmar's Military Struggles to Control the Virtual Battlefield, May 2021.
- 122** Mercy Corps, Social Media and Conflict: *Understanding Risks and Resilience, An Applied Framework for Analysis*, July 2021, p7, p12-13.
- 123** Ibid, p7.
- 124** USIP Commentary (Mandaville, Schiwal), *A New Approach for Digital Media, Peace, and Conflict*, February 2023, available at: www.usip.org/publications/2023/02/new-approach-digital-media-peace-and-conflict.
- 125** Day, Adam, *Pathways for Peace: Five Years On, Changes in the Global Conflict Landscape since "Pathways for Peace": How the UN system can meet new and emerging prevention challenges*, March 2023, p2.
- 126** UNICRI, Freedom From Fear Magazine, *Extremism – No Victory in Violence*, May 2023, p29.
- 127** United Nations Office of Counter-Terrorism, UN Counter-Terrorism Centre (UNCCT), *Examining the Intersection Between Gaming and Violent Extremism*, October 2022, p4-6.
- 128** USIP Commentary (Mandaville, Schiwal), *A New Approach for Digital Media, Peace, and Conflict*, February 2023, available at: www.usip.org/publications/2023/02/new-approach-digital-media-peace-and-conflict.
- 129** Mercy Corps, Social Media and Conflict: *Understanding Risks and Resilience, An Applied Framework for Analysis*, July 2021, p5.
- 130** Puig, Morrison, *Understanding Digital Conflict Drivers* p187-p191 (Ch. 9 in Mahmoudi et al. (eds) *Fundamental Challenges to Global Peace and Security*, Springer), 2022.
- 131** International Crisis Group Commentary, *What the Facebook Whistleblower Reveals about Social Media and Conflict*, November 2021, available at: www.crisisgroup.org/united-states/united-states-internal/what-facebook-whistleblower-reveals-about-social-media-and-conflict.
- 132** Research findings from Brookings that take stock 20 years after the attacks of September 11, 2001 - point to education as a central (and cost-effective) measure of countering extremism and terrorism. See Brookings (Afzal) *A global effort to counter extremism through education*, January 2021; A notable example of how misinformation is integrated into education curricula can be found in Finland, as explored in this New York Times article: www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html.
- 133** For examples of the Centre for Humanitarian Dialogue's (social media and conflict mediation programme) work, see its Digital Conflict webpage, available at: <https://hdcentre.org/area-work/digital-conflict/>; For more leveraging social media in peacemaking, see, Centre for Humanitarian Dialogue and Build Up, *A Social Media Analysis Toolkit for Mediators and Peacebuilders*, April 2022.

- 134** One such initiative is the annual West Africa Peace and Security Innovation Forum. Findings from consultations to inform this forum, and which reflect how regional peacebuilders use technology their interventions can be found in ECOWAS Commission, *Leveraging Technology for Peacebuilding in the ECOWAS Region, Documentation of a Consultative Process*, October 2021.
- 135** United Nations, Our Common Agenda Policy Brief #9, *A New Agenda for Peace*, July 2023, p13; UNICRI, Freedom From Fear Magazine, *Extremism – No Victory in Violence*, May 2023, p3.
- 136** For perspectives from the UN-Secretary-General on the need for a New Social Contract, see his Nelson Mandela Lecture, *Tackling the Inequality Pandemic: A New Social Contract for a New Era*, July 2020, available at: www.un.org/sg/en/content/sg/statement/2020-07-18/secretary-generals-nelson-mandela-lecture-%E2%80%9Ctackling-the-inequality-pandemic-new-social-contract-for-new-era%E2%80%9D-delivered; Additional perspectives on the social contract and approaches to reconsider its meaning and application can be found in McCandless, *Reconceptualizing the Social Contract*, University of Witwatersrand, May 2018.
- 137** Pathways for Prosperity Commission, *The Digital Roadmap, How developing countries can get ahead*, p25-28. For commentary, see Duncan Greene's From Poverty to Power blog, available at: <https://frompoverty.oxfam.org.uk/for-developing-countries-the-digital-revolution-is-not-just-about-the-tech-its-about-the-politics/>.
- 138** UNDP's Digital Strategy (2022-2025) defines digital transformation as “the integration of digital technologies into all areas of business, fundamentally changing how economic and social activities are enacted. It is also a social change process that is purposeful, rather than unregulated, and should be intentionally planned and executed.”
- 139** See United Nations, Our Common Agenda Policy Brief #5, *A Global Digital Compact – an Open, Free and Secure Digital Future for All*, May 2023.
- 140** Pathways for Prosperity Commission, *The Digital Roadmap, How developing countries can get ahead*, p61-64.
- 141** For more on this topic, see Broadband Commission, *Balancing Act: Countering Disinformation While Respecting Freedom of Expression*, September 2020.
- 142** Recommendations to ensure the protection of human rights are outlined in the UN Secretary-General's *Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation*, May 2020, p10, available at: www.un.org/digital-roadmap.
- 143** Pathways for Prosperity Commission, *The Digital Roadmap, How developing countries can get ahead*, p13, 15.
- 144** See UNICRI, Strategic Programme Framework 2023 – 2026, February 2023.



unicri
United Nations
Interregional Crime and Justice
Research Institute

Viale Maestri del Lavoro, 10
10127 Turin, Italy

Website: www.unicri.org