

## RESEARCH BRIEF

# BEHIND THE LENS: EXPLORING THE PROBLEMATIC INTERSECTION OF SURVEILLANCE, CYBER TARGETING AND DISINFORMATION

*'We recognize that the pace and power of emerging technologies are creating new possibilities but also new risks for humanity, some of which are not yet fully known. We recognize the need to identify and mitigate risks and to ensure human oversight of technology in ways that advance sustainable development and the full enjoyment of human rights.'*

*United Nations, Global Digital Compact<sup>1</sup>*

### EXECUTIVE SUMMARY

By empowering individuals, enabling civic engagement and amplifying marginalized voices, digital technologies have become indispensable to exercising fundamental human rights in today's world. Digital platforms in particular have proven transformative for activism and advocacy, as seen in movements like the Arab Spring and #BlackLivesMatter, where social media played a critical role in mobilization. Yet these same technologies present significant risks, including pervasive surveillance, cyberattacks and the spread of disinformation. Spyware like Pegasus, for example, has been used by state actors to target journalists and dissidents, while around-the-clock monitoring by state and non-state actors has eroded privacy, chilled public discourse and restricted civic spaces. China's social credit system, for instance, starkly illustrates how digital surveillance can be leveraged to control and suppress dissent.

Somewhat counterintuitively, our reliance on digital tools has made them prime targets, with recent ransomware attacks on healthcare systems highlighting the tangible risks to essential services. Internet shutdowns in regions like Kashmir or during protests in Iran further demonstrate how access to digital freedoms can be curtailed instantly. All the while, disinformation campaigns are becoming increasingly sophisticated, as seen with deepfake technologies and targeted misinformation. Such tactics have been used to shift public opinion, exacerbate divisions and undermine trust in democratic institutions.

Underlying these challenges is the central role that technology companies play in shaping the digital landscape, and the responsibility of states to issue adequate regulation and demand accountability. These fissures demand

DECEMBER 2024 | ERICA HARPER, JONATHAN ANDREW, FLORENCE FOSTER, JOSHUA NIYO, BEATRICE MERETTI AND CATHERINE STURGESS

This publication has been externally peer-reviewed

urgent attention, as unchecked misuse risks eroding trust, undermining social cohesion and exacerbating global divides. In response, states have started to craft a roadmap for building a more inclusive, secure and equitable digital environment through the Global Digital Compact. Commitments include closing digital divides, safeguarding human rights in digital spaces, fostering responsible governance in artificial intelligence and promoting international collaboration to counter digital threats.<sup>2</sup>

To contribute to this evolving debate, this report makes a case for balancing the benefits of digital technologies with robust safeguards to ensure their proper use. Section 1 explores how new and emerging technologies facilitate surveillance, enable sophisticated network disruptions and drive the spread of disinformation. Section 2 explains the application of international human rights law vis-à-vis the misapplication of digital technologies in specific areas. The final section offers actionable recommendations to ensure that (i) governments implement rights-based regulations to protect privacy and freedom of expression; (ii) private companies enhance transparency and accountability, including by prioritizing ethical practices in AI and content moderation; and (iii) civil society advocates for inclusive digital policies and holds both states and corporations accountable.

## AN OVERVIEW OF KEY TECHNOLOGIES

### MONITORING AND SURVEILLANCE TECHNOLOGIES

Advances in cyber-surveillance and monitoring technologies have broadened the capacity of state entities to oversee the content of political, human rights and civil society movements, as well as the individuals who organize and participate in them.<sup>3</sup> A parallel development is the leveraging of information shared on social networks and mobile applications (apps).<sup>4</sup> Such platforms constitute a rich bank of open-source information that can be combined with covert surveillance to provide unprecedented insight into persons and areas of interest.<sup>5</sup>

These technologies include software (spyware) designed to infiltrate smartphones, computers and certain ‘wearable’ devices, and enable the tracking of activities, interception of communications and sometimes the remote operation of a device’s functions such as its camera or microphone.<sup>6</sup> Real-time surveillance technologies such as satellites, drones, closed-circuit and networked cameras and digital interception tools enable the real-time surveillance of both













online and offline spaces, with facial recognition systems increasingly embedded.

In civilian contexts, such technologies were originally foreseen as a law enforcement or crime prevention tool and were used principally in criminal investigations in a highly regulated manner. Over time, however, their use and scope of focus have expanded to include the surveillance of journalists, activists, political opponents, international non-government organizations and even general population groups.<sup>7</sup>

### TARGETING OF COMPUTER SYSTEMS AND NETWORKS

The targeting of computer systems and networks can take various forms – from offensive exploitation of systems to ransomware that disrupts systems and networks, including with scope to extract information or inhibit use.

## THE TYPES OF SURVEILLANCE TECHNOLOGY

 <b>ANALYSIS</b> <p>Use data to map relationships, recognise patterns, and analyse words’ meaning <i>Example: Relationship mapping software</i></p>	 <b>AUDIO SURVEILLANCE</b> <p>Record and transmit audio <i>Example: Speaker identification software which compares recordings against target voice samples</i></p>	 <b>VIDEO SURVEILLANCE</b> <p>Use video cameras <i>Example: Wide Area Persistent Surveillance systems</i></p>
 <b>PHONE MONITORING</b> <p>Gather data communicated across mobile, fixed or next generation networks <i>Example: IMSI catchers</i></p>	 <b>LOCATION MONITORING</b> <p>Monitor the location of a target using phone identifiers or tracking devices <i>Example: GPS tracking devices</i></p>	 <b>INTERNET MONITORING</b> <p>Technologies that gather information communicated across the internet <i>Example: Optical Fiber Cable taps</i></p>
 <b>MONITORING CENTRE</b> <p>Combine different surveillance technologies (internet, phone etc) into one suite <i>Example: Monitoring Centres offered by surveillance companies</i></p>	 <b>INTRUSION</b> <p>Remotely installed on communication devices to extract data &amp; control functions <i>Example: Commercial “spyware”</i></p>	 <b>BIOMETRICS</b> <p>Identify individuals on distinctive physiological or behavioral characteristics <i>Example: Facial recognition software</i></p>
 <b>COUNTER-SURVEILLANCE</b> <p>Detect and counter surveillance <i>Bug detection tools</i></p>	 <b>EQUIPMENT</b> <p>Aids the operation of surveillance and counter surveillance capabilities <i>Example: Vans or vehicles in which surveillance technology can be installed</i></p>	 <b>FORENSICS</b> <p>When attached to a device, extract and visualise data from it <i>Example: Commercial software packages offered by surveillance companies</i></p>

## CYBERATTACKS INCREASINGLY LEVERAGE THE VALUE ATTACHED TO DATA

In April 2022, the Costa Rican Ministry of Finance (specifically its tax collection and export systems) was targeted in a cyberattack. Russian hackers demanded USD 20 million in exchange for it not leaking the stolen data, prompting the president to declare a national emergency.<sup>8</sup> In February 2023, hackers of Technion University in Israel took control of the University's files and demanded USD 1.7 million in Bitcoin to decrypt them.<sup>9</sup>

Disruption can also take the form of maliciously interrupting the normal functioning of a computer network or website by overwhelming it with a flood of traffic from multiple sources (formally known as Distributed Denial of Service, DDoS). The goal is to make the targeted system or website inaccessible to its intended users. Instead of a single attacker, DDoS attacks involve a network of compromised computers, often referred to as a 'botnet', working together to generate the massive traffic needed to overload the target.<sup>10</sup> DDoS attacks should be distinguished from deliberate disconnections of the internet, known as 'network shutdowns', that interrupt internet-based communications (or throttle bandwidth), rendering them non-functional for a specific demographic, geographical region or mode of access.<sup>11</sup> Such blackouts are often orchestrated by governmental authorities aiming to regulate or censor digital speech, or as part of a conflict strategy.

## DISINFORMATION AND MANIPULATIVE TECHNOLOGIES

Misinformation and disinformation, while colloquially referred to as 'fake news', may not always comprise false content. *Misinformation* is the sharing of incorrect information whereas *disinformation* is the sharing of incorrect information either with malicious intent<sup>17</sup> or to discredit accurate reporting. While there is no clear definition of disinformation,<sup>18</sup> campaigns generally rely on digital techniques such as deep and shallow fakes, 'trolling' and dissemination tools such as botnets. Importantly, these are often a single component of a wider playbook of so-called information warfare – the continuation of politics by other means.

The shift to digital spaces dominated by algorithm- and ad-based platforms has led to reduced quality news, 'click-bait' journalism and peer-to-peer self-curated news sharing. These new news ecosystems tend to have fewer checks and balances and create a flourishing landscape for dis- and misinformation. Indeed, such models amplify sensational, hateful or false content to keep users engaged, thus perpetuating an environment that is conducive to being exploited by various technologies that curate manipulative content.

Deepfakes are a type of synthetic media created using artificial intelligence (AI) and machine learning techniques to create highly convincing but fabricated content, for example by creating people who do not exist, or depicting real people saying or doing things that did not take place. Shallow fakes – which are generated manually as opposed to using AI – have the same aim as deepfakes. Originating as 'revenge porn', they have since been used for fraudulent purposes, to intimidate or exploit or to spread disinformation. Deepfakes are alarmingly on the rise, from 14,000 appearing online in 2019 to around 500,000 in 2023.<sup>19</sup>

## INTERNET DISRUPTIONS ARE A KEY TOOL IN THE RUSSIA-UKRAINE CONFLICT

DDoS attacks have seen a steep increase since Russia's invasion of Ukraine in February 2022. Targets have included the Finnish ministries of defence and foreign affairs in April 2022,<sup>12</sup> Lithuania's state-energy provider in July 2022<sup>13</sup> and the Czech stock exchange in August 2023.<sup>14</sup> In each case, hackers were Russia-aligned groups stating that their actions were a response to European governments' support to Ukraine. Russia, however, has also been subjected to attack, most recently in April 2024 when Ukrainian military intelligence targeted the United Russia party's servers, websites and domains, making them inaccessible.<sup>15</sup> Importantly, DDoS attacks are not always politically motivated; in August 2023, hackers disabled the access of over 20,000 X-users in the US and UK, demanding that Elon Musk open Starlink (a group of internet-enabling satellites) in Sudan.<sup>16</sup>

Trolling – the act of deliberately provoking an argument or emotional reaction at scale – is facilitated by so-called ‘troll factories’ dedicated to disseminating disinformation on the internet, usually of a political or economic nature. Factory employees hold multiple different social media accounts that appear authentic and credible, including by showcasing content of a personal nature over a sustained period of time. These factories are often supported by

‘bots’ – computer programs that automatically distribute messaging in response to the appearance of a keyword. When networked, bots form ‘botnets’ that are controlled by a single entity to amplify the reach of false information or facilitate coordinated attacks on digital platforms or websites.<sup>22</sup> Such practices are improving rapidly over time; the use of Big Data, for example, is allowing messages to be adjusted automatically to target specific audiences.

### DEEPPAKES FOR POLITICAL GAIN

In February 2024, hackers aligned with the Iranian state interrupted streaming services in the UAE and broadcast a fabricated report generated by artificial intelligence on the Israel– Hamas conflict. The broadcast featured a synthetically generated news anchor and displayed images depicting Palestinians who had been injured and killed by Israeli attacks. The action formed part of a larger campaign to influence public opinion around the conflict, weaken the Israeli narrative and strengthen Arab support for Hamas.<sup>20</sup>

In 2019, doctored videos of Nancy Pelosi, Speaker of the US House of Representatives, were generated to make her appear intoxicated and stammering. YouTube deleted the videos, however not before they were shared and tweeted, including by then President Donald Trump. The video was viewed 2.5 million times on Facebook alone.<sup>21</sup>

### THE EVOLUTION OF TROLL FACTORIES

One of the first troll factories was set up following Russia’s annexation of Crimea in 2014. The entity, registered as an internet research agency in St Petersburg, employed 300 people and was managed by Yevgeny Prigozhin. It operated mainly in the domain of social media by generating and circulating posts praising President Vladimir Putin, and criticizing countries deemed non-supportive of Russia.<sup>23</sup> Since then, the use of trolling has expanded profusely. A study by the Oxford Internet Institute found that at least 80 countries have harnessed the capabilities of social media platforms, messaging applications and state-aligned media to deploy ‘cyber troops’.<sup>24</sup>

### THE BUDDING TREND OF ‘HACKTIVISM’

A relatively new form of type of cyberattack can be likened to a form of social or political activism. In October 2023, so-called ‘hacktivists’ stole 3,000 documents from NATO, allegedly as a response to member-state human rights abuses. In another incident in June 2022, hackers leaked files and photos known as ‘The Xinjiang Police Files’, which captured human rights abuses committed against the Uyghur population. In February 2023, Iranian hacktivists disrupted the state-run television broadcast of a speech by Iranian President Ebrahim Raisi during Revolution Day ceremonies. Hackers aired the slogan ‘Death to Khamenei’ and encouraged citizens to join anti-government protests.<sup>25</sup> Another form of hacktivism occurs between states to protest issues of foreign policy. While the groups taking responsibility for such hacking are generally private, they are often state-aligned or proxy entities. In September 2022, for example, Iranian hackers targeted Albanian computer systems, forcing officials to temporarily shut down the Total Information Management System, a service used to track individuals entering and exiting the country. This attack closely followed Albania’s decision to sever diplomatic ties with Iran and NATO’s condemnation of an Iranian cyberattack against Albania in July.<sup>26</sup> Another example is Russia’s DDoS attacks against countries offering support and/or assistance to Ukraine, including New Zealand’s parliament,<sup>27</sup> Bulgaria’s defence, interior and justice ministries,<sup>28</sup> France’s National Assembly<sup>29</sup> and the European Investment Bank.<sup>30</sup>

## HOW THE MISUSE OF NEW TECHNOLOGIES CAN VIOLATE HUMAN RIGHTS

Upholding fundamental rights and freedoms in the context of emerging digital and information technologies is a rapidly developing area of international law. The Global Digital Compact – an intergovernmental framework for the global governance of digital technology and artificial intelligence – recently acknowledged the need ‘to identify and mitigate risks and to ensure human oversight of technology in ways that advance sustainable development and the full enjoyment of human rights’.<sup>31</sup> Moreover, while access to the internet is not a formally recognized human right, pressure is mounting, as underscored in Our Common Agenda.<sup>32</sup>

Importantly, the diversity of digital tools and their ubiquity – computers, networks and particularly the internet – are enablers of other rights that need to be protected from technology misuse under current international law. Chief among these are the right to freedom of opinion and expression (which includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers<sup>33</sup>) and the right to privacy (which encompasses the free development and expression of an individual’s personality, identity and beliefs, and their ability to participate in political, economic, social and cultural life). Moreover, as the remit of digitalization expands, so does society’s reliance on digital tools for the realization of other rights including social and cultural rights (such as the right to education, to participate in social, cultural and political life, to health, to an adequate standard of living, to work and to social and economic development) as well as civil and political rights (such as the right to freedom of association and assembly).

### MONITORING AND SURVEILLANCE TECHNOLOGIES

When states misuse surveillance technologies to monitor not only the content of civil society activity, but also those who organize and participate in it, the result can be to hinder civic participation and/or quash political dissent.<sup>36</sup> It can also repress emergent civil society groups, leading to a contraction of the democratic space. Monitoring people’s communications in particular can create a chilling effect on debate and the interchange of ideas, both of which are critical to enabling a plurality of opinions. When such monitoring categorizes behaviours and preferences into pre-existing frameworks, the result can be to promote social conformity

### TOWARDS GLOBAL REGULATION

Concern about the potential negative impacts on human rights has been central to the negotiations of a global cybercrime treaty.<sup>34</sup> This process began in UNGA’s Third Committee, which is responsible for the protection of human rights. In 2021, an Ad-hoc Committee was established by resolution and tasked with developing a ‘comprehensive international convention on countering the use of ICTs for criminal purposes’. The Global Digital Compact is another positive development: states have committed to set up ‘appropriate safeguards to prevent and address any adverse impact on human rights’ and establish ‘effective oversight and remedy mechanisms’ for violations arising from the use of digital and emerging technologies.<sup>35</sup>

and control. This marginalizes those who deviate from the norm, creating particular risks for minorities and other groups.<sup>37</sup>

Trends in monitoring also have implications for privacy. Indeed, in modern society, the groups that form to associate or assemble extend far beyond the political realm to include, for example, sexual identity groups, groups advocating for gender equality, environmental human rights defenders, etc. Especially for younger generations, online platforms (such as social media and messaging apps) are widely used as a means to build community and mobilize, both online and offline.<sup>38</sup> The upshot is that as individuals become more connected, their lives are intermeshed with fora that can be surveilled. Even for those not engaged in civil society movements, the massive ‘dragnets’ (widespread, indiscriminate data collection) used in many surveillance systems have widened the scope for unwarranted mass surveillance.

A further area of risk concerns the pooling and cross-analysis of surveillance data with other open-source information (observed behaviours, financial and commercial transactions, installed applications in a smartphone, social network profiles, etc.) using methods such as social graph analysis. This can deliver a complex and informative profile of an individual,<sup>39</sup> including their political beliefs, religion or sexual orientation.<sup>40</sup> Such data can be leveraged for constructive ends, for example detecting and solving crime,<sup>41</sup> or to forecast risks around violence or

public safety that may extend from civic activism.<sup>42</sup> Indeed, it is under such aims that most surveillance is authorized from a legal standpoint. However, malign uses also exist, such as the monitoring of protest movements and political opposition groups, and the identification of minorities such as LGBTQI+ or human rights defenders. Such data can also be used to undertake profiling, i.e. classifying attributes of an individual's behaviour and/or their associations to draw conclusions on likely future behaviour. This is a particular concern insofar as it compromises autonomy and agency. Moreover, when profiling draws linkages based on gender, race, religion, etc., existing biases can be exacerbated and individual rights to equality and protection against discrimination infringed.<sup>43</sup>

Finally, the risks associated with technical errors need to be acknowledged. For example, while advances have been made in the accuracy of facial recognition technology, false positives remain a concern. Such problems are rooted in biases and non-representativeness in the datasets underpinning the technologies, making them less accurate in identifying individuals with darker skin tones and women.<sup>44</sup> This creates scope not only for discriminatory outcomes but also to amplify existing racial and gender biases. Such risks carry over to other technologies, such as crowd management software and the use of social network analysis by law enforcement. Here the issue is that individuals whose lifestyles are less 'datafied' vis-à-vis the general population (due to poverty, geography or because they live on the margins of society) are not included in the data that feed the technology.<sup>45</sup> As such, the Big Data sets collected contain 'dark zones' where certain citizens or communities are overlooked or underrepresented, creating scope for discrimination.<sup>46</sup>

In terms of states' responsibilities under international law, information gathering, whether by public or private entities, including through surveillance or the interception of communications, must be consistent with standalone rights, including the right to privacy and protection from discrimination, as well as interdependent human rights, such as freedom of assembly and freedom of movement. The principle of proportionality requires that the effects of monitoring should not be excessive and that authorities should minimize the resulting interference caused by the surveillance activity. Monitoring, whether conducted covertly or overtly, should never be aimed at intimidation, harassment or limiting people's freedom of expression. Surveillance practices must be regulated by appropriate and publicly accessible domestic legal frameworks and allow

for sufficient transparency and scrutiny by courts.<sup>47</sup>

Only in exceptional circumstances are more invasive forms of surveillance permitted, for example to protect national security or safeguard rights and liberties (such as the right to life) in situations where public order is at risk.<sup>48</sup> Such limits must be set out in law and be sufficiently accessible to the public, clear and precise so that any individual may without difficulty review the legislation and determine who is authorized to conduct surveillance activities, and under what circumstances. Limitations must not breach core rights protections and must be both necessary and proportionate to serving a legitimate purpose, and the least intrusive option available.<sup>49</sup> Moreover, the limitation must be shown to be plausible and to have a reasonable chance of achieving its objective. The onus is on the state authority seeking to limit the right to show that the limitation is clearly connected to achieving a legitimate aim.<sup>50</sup>

## TARGETING COMPUTER SYSTEMS AND NETWORKS

The increased targeting of computer systems and networks and the diversification of ways in which this is being done, has created myriad consequences across a range of actors – state, corporate and individual. Attacks of a financial nature (generally orchestrated by private or citizen hacker groups) are the most frequent. The impacts of such acts are broad-reaching; one study has suggested that shutdowns in 46 countries between 2019 and 2021 led to losses amounting to \$20.54 billion.<sup>51</sup> The sharpest escalation in attacks, however, has been disruptive events *between* states. This is usually geared towards obtaining information of intelligence value, but other aims include to disrupt, interfere in electoral processes or problematize access to essential services.

The most serious forms of rights violations occur when states use system interference against their own citizens, for example action that compromises the ability of individuals to coordinate collective action.<sup>52</sup> Particularly in Asia and Africa, there has been a marked increase in the use of blackouts during periods of heightened civic engagement, public dialogue or protest on issues of societal concern.<sup>53</sup> Where this prevents popular mobilization and communication between groups, the right of peaceful assembly can be compromised. Another trend is the use of shutdowns and interruptions in the lead-up to elections, impeding electoral competition and political debate, and in their aftermath to prevent protest or contestation over results.<sup>54</sup> This is especially destructive in settings where the conventional media landscape is under government control,

making the internet the only venue for the unhindered expression of diverse viewpoints.

Internet interruptions and shutdowns can also be used as a tool for orchestrating violence and human rights abuses, for example during domestic military operations. Moreover, blackouts tend to foster impunity, emboldening state actors to perpetrate violations.<sup>55</sup> Indeed, connections have been established in certain jurisdictions between internet blackouts and heightened instances of violence.<sup>56</sup>

The spillover consequences of internet disruptions also need to be considered. Shutdowns can endanger safety and well-being, for example, when they compromise essential services<sup>57</sup> such as the running of hospitals or banks,<sup>58</sup> prevent the dissemination of public messaging, interrupt transportation services<sup>59</sup> or prevent businesses from operating. Another form of spillover can take place in the context of deliberate data leaks. While the primary target is generally a company or the state, individual rights to privacy can be affected. Likewise, campaigns of electoral interference can violate individuals' right to participate in public affairs.<sup>60</sup>

Shutdowns ordered covertly or without an obvious legal basis violate the requirement of Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR). Indeed, Article 19(3) provides that states may limit freedom of expression – which includes the freedom to hold opinions and to receive and impart information and ideas without

### ATTACKS ON ESSENTIAL GOVERNMENT FUNCTIONS AIM TO UNDERMINE TRUST

In the last five years, several countries have experienced attacks on their online voting system: Bahrain in November 2022, Estonia in March 2023 and Ecuador in August 2023.<sup>61</sup> Ahead of the 2024 European elections, the websites of specific political parties suffered DDoS attacks in the Netherlands<sup>62</sup> and Germany,<sup>63</sup> allegedly by Russia-aligned hacker groups. In June 2022, public alert systems in Jerusalem and Eilat were hacked, triggering air raid sirens.<sup>64</sup> In July 2022, hackers disabled the e-Albania portal used to access public services, 95 percent of which are provided online.<sup>65</sup> In December 2022, hackers obtained and attempted to sell the contact information of more than 80,000 members of an FBI threat information-sharing program, InfraGard.<sup>66</sup>

### CASE STUDY: INDIA'S DIGITAL TIGHTENING: INTERNET SHUTDOWNS IN JAMMU AND KASHMIR

Internet shutdowns are part of the Indian Government's toolbox for managing dissent, protests and security threats, with 771 documented shutdowns between 2016 and 2023<sup>69</sup> (58 percent of instances globally).<sup>70</sup> The justifications range from restoring law and order to controlling hate speech, misinformation and harmful content, and policing.<sup>71</sup> Such explanations sit uncomfortably, however, given the sheer number of shutdowns and geographic locations affected. A striking example concerns Jammu and Kashmir (J&K) – a Muslim-majority region at the heart of a longstanding conflict involving India, Pakistan and China.<sup>72</sup> Between August 2019 and February 2021, J&K experienced what has been described by human rights groups as the 'longest shutdown ever in a democracy'<sup>73</sup> and a manifestation of a 'digital apartheid'.<sup>74</sup> The 552-day-long ban saw the suspension of social media,<sup>75</sup> mobile internet, WiFi hotspots and virtual private networks (VPNs).<sup>76</sup> Initially, the government explained the shutdowns as a preventive measure against the 'spread of misinformation and [to] maintain public order'<sup>77</sup> ahead of its decision to abrogate Articles 370 and 35A of the Indian Constitution,<sup>78</sup> de facto stripping J&K of its special autonomous status and rights.<sup>79</sup> The communication blockade was accompanied by severe movement restrictions, including a public curfew. The consequences were broad-reaching; schools and universities were unable to conduct exams or release results, businesses struggled<sup>80</sup> and the healthcare system was further strained.<sup>81</sup> The restrictions also crippled people's ability to exercise freedom of speech and expression. Journalists in particular were unable to reach their sources or editors, move around freely<sup>82</sup> and, due to bandwidth throttling, could not release real-time information, thus fuelling the impacts of disinformation and misinformation.

interference by public authority and regardless of frontiers – only where this is provided by law and is necessary for the respect of the rights or reputations of others, or for the protection of national security, public order (ordre public) or public health or morals.<sup>67</sup> While states can exceptionally



place limitations on the freedom of expression, these must adhere to the principles of necessity, legitimacy, legality and proportionality. Generalized or blanket internet shutdowns – given their indiscriminate and broad-reaching effects – are unlikely to meet such criteria.<sup>68</sup>

As well as refraining from obstructing rights, states are obligated to take positive steps to work towards protecting rights from being violated. In particular, states have a prerogative to make the internet universally available and accessible, free from unjustified restrictions. Under Sustainable Development Goal Target 9.c states have also committed to ‘significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020’.

## DISINFORMATION AND MANIPULATIVE TECHNOLOGIES

The right to freedom of opinion and expression includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.<sup>83</sup> It is well established that non-consensual actions designed to coerce or manipulate the thinking process would violate a state’s obligations. Traditionally, such actions have concerned the administration of psychoactive drugs or punishing an individual holding a particular opinion.<sup>84</sup> Technological advances, however, have expanded the scope for influencing opinion, including by narrowing, curating and controlling the volume of content an individual is exposed to (also known as micro-targeting). Indeed, this is how much disinformation is channelled.

The spread of disinformation can also undermine specific human rights. Disinformation about health interventions, such as vaccines or the causes and evolution of a pandemic, for example, can cause physical harm and loss of life, while disinformation pertaining to the integrity of an election process or a particular candidate can undermine the right to participate in public affairs. Disinformation that involves hate speech, incitement to discrimination, hostility or violence can also spill over from the digital into the physical sphere.

When disinformation threatens human rights, states have a duty to take appropriate steps to address these harmful impacts. Identifying thresholds for illegality, however, is complex. In reality, our opinions are the end-product of influence, including from other individuals, the media, state authorities, events and personal experiences.

Moreover, being able to access diverse sources of information is fundamental to forming opinions and thus to exercising the right to freedom of expression and opinion. Such access may also prove to be a key tool for countering disinformation. A further complicating factor is that the information influencing an individual’s opinion may be the product of another individual’s exercising of their right to freedom of expression. Indeed, freedom of expression applies to a broad range of information, including that which may shock or offend,<sup>85</sup> irrespective of its veracity.<sup>86</sup> In other words, international human rights law protects the expression of ill-founded opinions and inaccurate statements.

Moreover, while it is not an absolute right, the threshold for limiting the freedom of expression is set very high, due to the role that freedom of expression plays in realizing other fundamental rights. General Comment No. 34 (2011), for example, concluded that a state denying access to specific internet sites and systems *would* constitute a violation of article 19(3) of the ICCPR. Indeed, the freedom of expression and access to information can only be restricted under certain specific conditions – and to be lawful, in accordance with Article 19(3), such restrictions must be ‘provided by law, and be necessary for the respect of the rights or reputations of others or for the protection of national security or of public order (ordre public) or of public health or morals’. However, Article 20(2) of the ICCPR does require that propaganda for war *or* advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, be prohibited by law<sup>87</sup> (see further the Rabat Plan of Action).<sup>88</sup>

States also have positive obligations to ensure the availability of plural and diverse sources of information, including media freedom. This problematizes the development of regulation that limits exposure to content that may manipulate or coerce, but that is also consistent with the freedom of expression. In this context, the main point of leverage for protection against disinformation will likely be ensuring that users have knowledge of how digital platforms can purposefully channel information, and requiring user consent. Importantly, states have pledged, through the Pact for the Future, to better address the risks posed by disinformation, misinformation, hate speech and content inciting harm, including content disseminated through digital platforms, while respecting the right to freedom of expression and to privacy, and ensuring unhindered access to the internet in accordance with international law, domestic legislation and national policies.<sup>89</sup>

## CASE STUDY: AMPLIFICATION OF ANTI-LGBTQI+ SENTIMENT IN UGANDA

In recent years, Uganda has leveraged legislative provisions, generally around national security, to conduct mass digital surveillance and communication interception. These measures not only affect individuals' right to privacy and freedom of expression but also, when combined with punitive laws and disinformation, disproportionately impact LGBTQI+ people. Disinformation campaigns, generally instigated by political or religious leaders, have accused LGBTQI+ people of being influenced by Western imperial agendas, and portray such lifestyles as un-African and incompatible with Christianity and Islam. These 'harmful stereotypes ... are repeatedly circulated' on social media platforms,<sup>90</sup> with information 'manipulated and amplified with some degree of coordination to reaffirm gender stereotypes, [and] inflame existing bias and prejudices'.<sup>91</sup> This context has fuelled an increase in blackmailing against LGBTQI+ people, including by setting up fake online 'trap' profiles and then threatening victims with doxing.<sup>92</sup>

## THE CASE OF PRIVATE ACTORS

The dependence of modern society on digital tools and, by extension, on the private sector entities that facilitate access to these technologies, highlights the complicated nature of protecting human rights in the digital age. Indeed, states have obligations to take steps to protect individuals from undue interference with human rights when committed by private actors.<sup>93</sup> Human rights law also protects individuals against violations and abuses committed by private persons or entities, such as internet platforms or companies engaged in surveillance and monitoring, and/or their collection, processing and retention of personal data.<sup>94</sup> The Guiding Principles on Business and Human Rights (UNGPs), endorsed by the Human Rights Council in 2011, stipulate that states are required to take appropriate steps to *prevent, investigate, punish and redress* private actors' abuse.<sup>95</sup> Such steps include the adoption and implementation of legislative, judicial, administrative, educative and other appropriate measures that require or enable businesses' respect for fundamental freedoms, and, in the case of abuses, access to an effective remedy.<sup>96</sup>

Further, the UNGPs set out companies' responsibilities with respect to both preventing human rights infringements and addressing adverse human rights impacts that they may have caused 'independently of States' abilities and/or willingness to fulfil their own human rights obligations'.<sup>97</sup> For example, businesses must put measures in place to prevent personal information they hold from being leaked or misused, and for transparency with respect to what information is collected and retained. In practice this may mean, for example, pushing back against unjustified internet shutdowns or demands for private data to be handed over to state authorities, insisting on a legal basis for any such orders and interpreting requests in a manner that causes the least intrusion. Such scenarios are increasingly non-hypothetical. Although only a few governments have openly defended their ability to shut down the internet, several have passed legislation that grants them an increased authority to regulate it. India, Indonesia, Russia, Thailand, Turkey, Vietnam and Uganda, for example, have enacted laws aimed at overseeing platform content, mandating local data storage and facilitating centralized state supervision of internet infrastructure. In such cases, companies will need to determine how they leverage their influence to address the adverse impact of over-reach or direct orders on human rights.<sup>98</sup>

When it comes to restricting the flow of disinformation, what tech companies can and might be compelled to do is a topic of heated debate among regulators. While US courts have made clear that platforms cannot be prosecuted for their exercise/non-exercise of editorial functions, the individual states where large social media companies operate employ various strategies to mitigate the risks posed. Some have laws criminalizing false content that, for example, encourages violence or facilitates terrorism. They may also require platform operators to remove such content within a certain time period or face fines. Such regulation, however, is difficult to enforce, rarely has extraterritorial application and 'workarounds' such as VPNs are increasingly commonplace. Finally, it must be acknowledged that media platforms craft and apply their own rules. Google, for example, prohibits and can ban individuals/groups that impersonate or post manipulated media, or that share content that exploits children. Companies like Meta have been proactive in taking down false accounts run by troll factories. Twitter (now known as 'X') also intervened by removing accounts implicated in disinformation campaigns.<sup>99</sup>

## **CASE STUDY: NETWORK SHUTDOWNS IN MYANMAR AND THE ROLE OF THE PRIVATE SECTOR**

In February 2021, Myanmar's military seized power in a coup, ousting the democratically elected government led by Aung San Suu Kyi and detaining prominent leaders of her party, the National League for Democracy. Against widespread protests and civil disobedience, authorities imposed extensive internet shutdowns, blocking social media and mobile networks. The disruptions started on 31 January 2021, with national connectivity falling to 75 percent and then to 50 percent of ordinary levels by Monday 8:00 a.m. local time. Although connectivity was partially restored on 8 February, authorities engaged in regular shutdowns during the evenings between 14–22 February 2021. These disruptions aimed to hinder the organization of protesters and their communication with the international community, while at the same time minimizing interference with daytime business operations and government activities<sup>100</sup> and allowing security forces to carry out arrests and violent crackdowns with impunity during the night.<sup>101</sup> Internet shutdowns continued into 2024, with at least 37 shutdowns verified over a 12-month period, and the predominantly Rohingya-populated states of Rakhine and Chin being disproportionately targeted.<sup>102</sup>

The private sector played a significant, if complex, role in facilitating these internet shutdowns. The Myanmar military pressured telecom and internet companies, both local and foreign, to restrict internet access and block social media platforms such as Facebook, Twitter and Instagram, as well as specific VPNs that were being used to bypass restrictions. On 2 April 2021, it was reported that the military instructed telecommunication companies and internet service providers to cease all wireless broadband services 'until further notice' or face stiff legal penalties. While some companies complied, citing concerns for staff safety and adherence to local laws, their actions drew international criticism for indirectly supporting the military's repression. Norwegian telecommunications operator, the Telenor Group, ultimately decided to exit the Myanmar market due to ethical and

operational challenges posed by these government pressures, selling its Myanmar operations to the M1 Group, a known military-linked entity. The company was forthright in explaining its decision-making: 'We did however arrive at the sad conclusion that it is no longer possible to adhere to these [business and human rights] principles, keep our employees safe, and at the same time remain as an operator in Myanmar. This makes our continued presence in Myanmar untenable'.<sup>103</sup>

## RECOMMENDATIONS

### SURVEILLANCE AND MONITORING

#### States should:

- Develop and effectively enforce – through independent, impartial and well-resourced authorities – robust privacy and data protection legislation that regulates surveillance technology, including facial recognition technology. These laws should clearly define the parameters for data collection, ensure transparent consent mechanisms and strict limits on data retention and include pathways to remedies.
- Adopt strong technical solutions to safeguard the confidentiality of digital communications, including measures for encryption and anonymity. Such safeguards should apply to the end-to-end collection, processing and retention (i.e. storage) of data.
- Require that any exemption to rules around the confidentiality of digital communication and use of targeted surveillance adheres to the principles of legality, necessity, proportionality and legitimacy (of purpose), and be executed under judicial supervision
- Limit public surveillance to strictly necessary and proportionate measures, specific locations and times, and constrain the grounds for and duration of data storage. The use of surveillance for indiscriminate monitoring and discriminatory profiling should be prohibited.
- Increase the *transparency* of the use of surveillance technologies including by:
  - Appropriately informing the public and affected individuals and communities, and regularly providing data relevant for the public to assess their efficacy and impact on human rights
  - Disclosing current and future contracts with private surveillance companies by responding to requests for information, or through proactive disclosure
- Ensure robust, independent, transparent and timely investigations into all reports of unlawful targeted surveillance and use of spyware alongside adequate access to effective remedies for victims, notably against journalists and human rights defenders
- Develop human rights-compliant rules for the issuing of export and import licences for digital surveillance and monitoring technology including by:
  - Conducting human rights due diligence systematically, including regular comprehensive human rights impact assessments, when designing, developing, purchasing, deploying and operating surveillance systems
  - Joining and abiding by the Wassenaar Arrangement and its rules and standards to the extent that these are consistent with international human rights law
  - Implementing moratoriums on the domestic and transnational sale and use of surveillance systems, such as hacking tools and biometric systems that can be used for the identification or classification of individuals in public places, until adequate safeguards to protect human rights are in place. Such safeguards should include domestic and export control measures.

#### International organizations and multilateral bodies should:

- Encourage the development of international guidelines and standards on digital surveillance in accordance with international human rights laws. This could include co-regulatory initiatives that develop rights-based standards of conduct for the private surveillance industry.
- Facilitate information sharing on the use and regulation of surveillance technology, fostering cooperation among states, to ensure the responsible development, export and use of surveillance technologies
- Promote public debate on the use of surveillance technologies and ensure the meaningful participation of all stakeholders in decisions on the acquisition, transfer, sale, development, deployment and use of surveillance technologies, including the elaboration of public policies and their implementation

- Engage in partnerships with technology companies and human rights organizations to develop solutions that promote the right to freedom of expression, facilitate peaceful assembly etc. online and safeguard the ability of civil society groups to connect and collaborate securely online

**Private sector actors, including but not limited to tech developers, business and media platforms, should:**

- Integrate human rights due diligence processes from the earliest stages of product development and throughout the operations lifecycle. These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights.
- Set in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. Such safeguards should include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law; technical design features to flag, prevent or mitigate misuse; and human rights audits and verification processes.
- Establish effective grievance and remedial mechanisms that enable victims of surveillance-related human rights abuses to submit complaints and seek redress
- Adopt robust security measures to safeguard data, conduct regular audits, and ensure transparency in data handling practices
- Provide opportunities for individuals to exercise rights over their data, including the right to access, correct, or delete their information

**DISINFORMATION**

**States should:**

- Develop clear and robust legal frameworks designed to:
  - Identify and impose appropriate and proportionate sanctions on those responsible for the creation and dissemination of disinformation
  - Prevent false information from being used as a tool against human rights activists, political opposition, etc.
  - Strike a balance between ensuring open online access and placing necessary and fair restrictions on the circulation of harmful content
- Strengthen the legal frameworks governing personal data protection by introducing comprehensive measures aimed at preventing misuse, and strict regulations governing the collection, processing and storage of personal data
- Ensure that legal frameworks are adaptable to evolving technologies and provide for the offline impacts of online behaviours
- Prioritize non-legal measures of countering disinformation and propaganda, starting with their own obligation to proactively disclose official data, encourage trustworthy fact-checking, promote access to diverse and reliable sources of information, ensure media, digital and information literacy and foster an enabling and inclusive environment for civil society to take initiatives to counter information manipulation
- Allocate financial resources to bolster initiatives aimed at
  - Enhancing media and critical digital literacy (including in schools), such as how to assess the credibility of online sources or identify disinformation
  - Supporting projects aimed at protecting vulnerable communities from the harmful effects of disinformation
  - Supporting diverse media outlets and independent journalism to ensure a plurality of voices and viewpoints in the digital space
- Prohibit advocacy of hatred in line with the guidance provided in the Rabat Plan of Action.
- Respect and protect the right of individuals to receive foreign news and propaganda (unless such information has been restricted in line with international human rights standards)

- Regulate social media in a manner that encourages companies to ensure meaningful transparency, engage in human rights due diligence and uphold the due process rights of users
- Refrain from asking platforms to enforce measures in relation to content that does not conform with international human rights standards
- Involve civil society in the design of policies and other efforts aimed at countering disinformation

**International organizations and multilateral bodies should:**

- Promote international cooperation and standards for countering disinformation and its impacts on fundamental rights such as freedom of speech and access to information
- Revisit the issue of extraterritorial application of human rights to take account of the digital threats to human rights, notably the right to freedom of expression and information from across borders
- Advocate for the recognition of digital literacy as an essential component of human rights and good governance. Digital literacy should be included as part of human rights education and awareness campaigns. Reciprocally, training and resources should be provided to empower activists with digital literacy skills.
- Work to diminish the digital divide and ensure affordable internet access globally, with a particular focus on marginalized and rural communities
- Engage in partnerships with human rights organizations to develop technological solutions that promote the right to freedom of expression, facilitate peaceful assembly etc. online and safeguard the ability of civil society groups to connect and collaborate securely online
- Focus attention on enhancing digital literacy skills in fragile and conflict-affected contexts, particularly for young people, women and other marginalized groups

**Private sector actors – including but not limited to tech developers, business and media platforms – should:**

- Avoid causing or contributing to adverse human rights impacts through their services and activities, including by engaging in robust human rights due diligence processes
- Develop, implement and disclose rules around content moderation and oversight in line with established guidelines and principles that balance freedom of expression and curbing harmful or illegal content
- Take proactive measures, including implementing policies and dedicating resources to combat disinformation through technological solutions. For example, algorithms can be designed to ensure that users see posts and updates not only from mainstream news outlets but also from citizen journalists, advocacy groups and individuals on the ground, fostering a more comprehensive and inclusive understanding of events.
- Enable real-time fact-checking tools to counter the spread of false information and maintain accuracy in information dissemination; incorporate functionalities into digital platforms that improve users' ability to assess the credibility of information. Browser extensions and plugins can flag potentially false or misleading content and direct users to verified sources for additional information.
- Design algorithms that prioritize content from reputable sources in users' news feeds, reducing the visibility of dubious or unreliable information
- Collaborate with educators and digital literacy experts to create user-friendly tools and platforms that promote responsible internet usage
- Carry out heightened human rights due diligence in fragile or conflict-affected contexts, that trigger enhanced risk management strategies. Due diligence processes should incorporate robust analyses of the impact of the companies' operations, products and services, including the business model itself, on conflict dynamics as well as on human rights.

## TARGETING OF COMPUTER SYSTEMS AND NETWORKS

### States should:

- Refrain from imposing internet shutdowns, in particular blanket shutdowns
- Refrain from conducting or knowingly supporting information and communication technology (ICT) activity that is contrary to its obligations under international law or that damages critical infrastructure (particularly infrastructure that provides services to the public)
- Develop legislation that prohibits the deliberate disruption or disconnection of internet or telecommunications services, particularly during public gatherings, electoral events or times of unrest, unless absolutely necessary. Oversight mechanisms should be established to monitor and regulate the implementation of internet shutdown policies.
- Evaluate the development of legal frameworks, policies and programmes to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution as a means to protect against misuse
- Ensure that where access to online platforms is limited (for example, with a view to upholding copyright or other intellectual property rights), such action is narrow in scope, serves only valid objectives and is subject to judicial oversight
- Provide publicly available information, in a timely manner, regarding any internet shutdowns, including bandwidth throttling, or limiting access to certain communication services, platforms or VPNs
- Not ban, block or criminalize the use of encryption or circumvention tools or particular communications channels, such as VPNs
- Protect (including legislatively) the availability of and access to the internet as a primary channel for individuals to exercise their rights to express opinions, access information and participate in discourse on political subjects and topics of communal significance
- Develop regulation that compels companies to ensure the openness and accessibility of online platforms, with a view to bolstering public debate, the dissemination of information and participation in governance
- Allocate funding to initiatives aimed at expanding internet accessibility. Projects might include the development of resilient, localized internet infrastructure, supporting digital literacy and skill-building programmes, providing subsidies for affordable internet and collaborating with local stakeholders to establish alternative communication channels in the event of a shutdown (e.g. through satellite-based internet solutions).

### International organizations and multilateral bodies should:

- Recognize the pivotal role of internet-based technologies in upholding human rights and facilitating development
- Further discuss the recognition of internet access as a human right and the importance of maintaining open online platforms for free expression and civic engagement
- Initiate discussions within the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (established pursuant to UNGA Res 75/240, 4 January 2021) geared towards addressing human rights concerns arising from the involvement of actors in developing and using offensive cyber capabilities, and to include those in their report to the General Assembly in 2025
- Engage in partnerships with tech companies and human rights organizations to develop technological solutions that promote the right to freedom of expression, facilitate peaceful assembly etc. online and safeguard the ability of civil society groups to connect and collaborate securely online
- Advocate for global standards that discourage unjustified internet shutdowns and prioritize the principles of necessity and proportionality, recognizing that such disruptions can have far-reaching consequences on the enjoyment of other fundamental rights
- Increase transparency, for instance by establishing a comprehensive and publicly accessible database of orders that limit access to the internet or digital communications platforms, their underlying reasons and their scope.

- Specifically, development agencies, regional organizations and international organizations should:
  - Ensure that the risks of internet shutdowns are considered when designing and implementing cooperation programmes relating to internet connectivity
  - Include reference to human rights standards when supporting the development of legal and institutional frameworks and seek commitments to limit interferences with digital communications consistent with those obligations
  - Consider including initiatives to provide access to encryption and other circumvention tools, and to promote digital literacy in efforts to expand connectivity
  - Review existing systems of data collection relating to internet access, including by monitoring target 9.c of the Sustainable Development Goals, to ensure that they reflect occurrences of state-ordered disruptions and their impact on the achievement of meaningful connectivity

**Private sector actors – including but not limited to tech developers, business and media platforms – should:**

- Carry out adequate human rights due diligence to identify, prevent, mitigate and account for how they address adverse human rights impacts, including in relation to (ordered) internet shutdowns, when they enter and leave markets
- Take all possible lawful measures to prevent an ordered shutdown and, if the shutdown proceeds, prevent or mitigate to the extent possible adverse human rights impacts; implement shutdown requests narrowly, in the most human rights-preserving way, and with the goal of keeping communications channels as open as possible; and take all lawful measures to enable the full disclosure of information about the interference
- Include in their public human rights policy statement their commitment to preventing and mitigating adverse human rights impacts in the context of internet shutdowns, and establish operational policies and procedures in order to be adequately prepared for responding to shutdown requests even in high-pressure situations
- Reinforce engagement and collaboration with all stakeholders working to prevent and reverse communications disruptions, in particular affected communities and civil society, including by systematically sharing relevant information about communications anomalies and mandated disruptions in a timely manner



## GLOSSARY: A SELECTED TYPOLOGY OF TECHNOLOGIES AND HOW THEY WORK

Monitoring and Surveillance Technologies	
<b>Commercial spyware</b>	Sophisticated software tools designed to infiltrate smartphones, computers and certain 'wearable' devices. Once installed, spyware enables the tracking of activities, interception of communication and sometimes the remote operation of a device's functions such as its camera or microphone.
<b>Pegasus spyware</b>	Unlike most hacking utilities that require a level of engagement from the intended victim – such as activating a hyperlink or opening an email attachment – Pegasus uses 'zero-click' infiltration, preventing the victim from obstructing the software's installation. Once installed, the software gains unmitigated access to all of the target device's sensory and data components including photographs, geolocation markers, electronic correspondence, text messages, visual and audio files and installed applications. Comparable software, for example Predator, is developing rapidly.
<b>Real-time surveillance</b>	Satellites, drones, closed-circuit and networked cameras and digital interception tools enable the real-time surveillance of both online and offline spaces.
<b>Signals intelligence</b>	SIGINT is electronic surveillance that involves the interception, decoding and analysis of (often encrypted) communications, radar and other electronic systems, the combination of which is used for deep intelligence analyses.
<b>Foreign instrumentation signals intelligence</b>	FISINT is gleaned from the interception of electromagnetic data emissions that follow the testing or deployment of aerospace, surface and subsurface systems. Such data can be transmitted by both military assets (e.g. unmanned aerial vehicles or missile systems) and civilian assets (e.g. satellites or traffic control systems), and can give insight into a range of activities such as weapons production.
<b>Social media intelligence</b>	SOCMINT refers to the harvesting and monitoring of large pools of open-source data, including social media, to generate profiles and predictions about the future behaviour of specific users.
<b>Facial recognition systems</b>	Rely on advanced machine learning algorithms that scan, recognize and match facial features against existing data. 'Live facial recognition technology' is the systematic visual documentation of individuals in real time by comparing a digitally captured facial image, or 'template', against stored data based on criteria set by the system's operators.
<b>Stingrays and IMSI catchers</b>	International Mobile Subscriber Identity catchers are electronic surveillance tools that simulate a cell phone tower or mobile phone traffic base station, thereby forcing smartphones, watches, tablets, etc. to connect to them. Once connected, information specific to a phone and SIM card can be identified and linked to an individual user. The primary function is to pinpoint an individual's location and/or movements. Modern IMSI catchers can also block communications, intercept data transmitted and received (including the content of calls, text messages and websites visited) and communicate with devices, for example by sending messages directing a user to a website enabled with malware.
<b>WiFi sniffers</b>	WiFi sniffers are hardware installations that enable monitoring even when a user sets their phone to aeroplane mode or turns it off completely.
<b>Location trackers</b>	Global Navigation Satellite Systems (GNSS), Bluetooth and WiFi are increasingly embedded into wearable personal devices such as smartwatches, fitness trackers, neuro-monitoring headsets and medical devices. These technologies facilitate the detection of an individual's location and proximity to others in real time with a high degree of accuracy. Meta's platforms such as Facebook and Instagram, along with TikTok, Snapchat and X, also collect location data and profile user patterns of mobility.
Malware	
<b>Offensive malware</b>	'Zero-day exploits' take advantage of vulnerabilities in a computer or network for which there are no security measures to defend against it. The term 'zero-day' refers to the fact that, at the time of exploitation, the vulnerability is unknown to the vendor or developer, giving them no time to prepare a fix or patch. 'Vulnerabilities' refer to tools that leverage already disclosed weaknesses. These attacks target systems that have not been updated by an organization or individual, but for which patches or updates may have been developed by software or system developers.
<b>Advanced persistent threats (APTs)</b>	APTs employ zero-day exploits and/or known vulnerabilities to gain initial access to a target's systems and then maintain long-term persistent control. The goal is often espionage or data theft, and they are known for their ability to stay undetected for extended periods.
<b>Viruses</b>	Function by embedding themselves within legitimate software or files. Their primary goal is to infect and compromise the host system or software. Once activated, viruses can perform a variety of tasks, such as data corruption, theft or unauthorized access. One distinctive feature of viruses is their ability to spread from one host to another, often through infected files or email attachments.
<b>Trojan horses</b>	Pose as legitimate software but carry out malicious tasks once installed. They do not replicate themselves but instead rely on social engineering to trick users into installing them, following which they can steal data, create backdoors for attackers or damage the host system.
<b>Ransomware</b>	Encrypts a user's files or locks them out of their computer or system until a 'ransom' is paid. <i>Crypto ransomware</i> encrypts the user's files using a strong algorithm, making them inaccessible. The attacker then demands a ransom, usually in cryptocurrency, in exchange for a decryption key. <i>Locker ransomware</i> locks a user out of their system and then issues a ransom note demanding payment to regain access to their computer or files.
<b>Worms</b>	Independent software that replicate to spread to other computers or networks independently, i.e. without the need for a host file or propagation software. They exploit vulnerabilities in computer systems or network protocols to infect other computers.
<b>Rootkits</b>	An advanced and invasive form of malware. They are designed to maintain persistent and stealthy access to a compromised system. <i>Kernel rootkits</i> operate at the deepest level of the operating system and can manipulate system functions and evade security mechanisms. <i>User-level rootkits</i> operate at the application layer, making them less powerful but still capable of concealing malicious activities and granting unauthorized access.
System Disruptions	
<b>Distributed Denial of Service</b>	DDoS attacks disrupt the normal functioning of a computer network or website by overwhelming it with a flood of traffic from multiple sources, rendering it inaccessible. DDoS attacks involve a network of compromised computers, using more than one unique IP address or machines, often from thousands of hosts infected with malware. They are often referred to as a 'botnet', working together to generate the massive traffic needed to overload the target.
<b>Amplification attack</b>	A type of DDoS attack whereby an attacker leverages network vulnerabilities to send small requests that trigger much larger responses from other devices on the network. These responses are directed to the target in a massive flood, overwhelming the system.
<b>Smurf attacks</b>	A type of DDoS attack whereby an attacker forges or 'spoofs' the IP address of the target and sends out a large number of ICMP (Internet Control Message Protocol) echo request packets to a network's broadcast address. This broadcast causes the packets to be sent to multiple computers within the network, all of which then respond to the forged IP address (the target). The victim or target's network is then flooded with responses from these multiple computers, causing congestion and potentially rendering the system or network inaccessible.
<b>Network shutdowns</b>	Deliberate disconnections that interrupt internet-based communications, rendering them unattainable or nonfunctional for a specific demographic, geographical region or mode of access. Methods include termination of connectivity, selective restrictions on principal communication channels, reduction of data transfer rates (bandwidth throttling) and reducing mobile services to suboptimal speeds (such as 2G).

<b>Disinformation and Manipulative Technologies</b>	
<b>Deepfakes</b>	Involve manipulating audio-visual content, such as videos or audio recordings, to create convincing but fabricated content. The technology works by training machine learning models on actual footage and images of an individual, which is then manipulated using advanced computer graphic tools. Footage can be accessed through compromised devices, but increasingly sufficient information is available online, for example through an individual's social media.
<b>Shallow fakes</b>	Have the same aim as deepfakes (i.e. to alter an image, audio feed or video to misrepresent its actual meaning for malicious intent), but are generated manually as opposed to using AI. While of a lower quality, shallow fakes are easier to achieve using free downloadable software. Shallow fakes originated as 'revenge porn' but have since extended to become a disinformation tool.
<b>Troll factory</b>	A business entity dedicated to disseminating disinformation on the internet, usually of a political or economic nature. Employees (often hundreds) hold multiple social media accounts that appear authentic, including by showcasing content of a personal nature over a sustained period of time. The aim is to promote a 'company narrative' by circulating both positive media associated with a political figure or product, coupled with disinformation around rival figures or companies. Factories are often supported by 'bots', i.e. computer programs that automatically distribute messaging in response to the appearance of a keyword.
<b>Botnets</b>	A network of computers that have been compromised and are controlled by a single entity, often a cybercriminal or hacker. These compromised computers, also known as 'bots' or 'zombies', are then used to disseminate propaganda or disinformation. Botnets are typically used to amplify the reach of false information; text prediction tools (like Open AI's GPT-2) generate disinformation at scale, which is then repeatedly (in a circular feedback loop) channelled through algorithms to individuals who seek particular content on social media.
<b>Foreign information manipulation and interference</b>	Coordinated activity by a state or non-state actor group using both traditional and digital media (e.g. the falsification of user accounts in social media or the artificial amplification of reach) to intentionally threaten or negatively impact the target.

## END NOTES

- 1 United Nations, Summit of the Future Outcome Documents: Pact for the Future, Global Digital Compact and Declaration on Future Generations, September 2024, p 37, [https://www.un.org/sites/un2.un.org/files/sof-pact\\_for\\_the\\_future\\_adopted.pdf](https://www.un.org/sites/un2.un.org/files/sof-pact_for_the_future_adopted.pdf) (last accessed 18 January 2025).
- 2 Ibid, pp 39–49.
- 3 M. Land, and J. Aronson, 'Human Rights and Technology: New Challenges for Justice and Accountability', 16 Annual Review of Law and Social Science (2020) 223–226.
- 4 See generally, M. Brunati, M. Conti and A. Tezza, 'SNIFFO: Security of Networks and Intelligence for Field Operations', in 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2017.
- 5 See generally, L. Vomfell, W. K. Härdle and S. Lessmann, 'Improving Crime Count Forecasts Using Twitter and Taxi Data', 113 Decision Support Systems (2018).
- 6 T. Kaldani and Z. Prokopets, 'Pegasus Spyware and Its Impacts on Human Rights', DGI (2022) 04, Council of Europe, 2022, p 7, <https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8> (last accessed 18 January 2025); Amnesty International, 'German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed', 25 September 2020, <https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/> (last accessed 18 January 2025).
- 7 Kaldani and Prokopets, 'Pegasus Spyware', supra fn 6, p 18.
- 8 P. M. Datta and T. Acton, 'Ransomware and Costa Rica's National Emergency: A Defense Framework and Teaching Case', 14 Journal of Information Technology Teaching Cases 4 (2022).
- 9 Y. J. Bob, 'Technion University Hacked; Cyber Authority Trying to Assist', The Jerusalem Post, 12 February 2023, <https://www.jpost.com/breaking-news/article-731327>.
- 10 See, M. K. Hasan, A. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah and B. Pandey, 'DDoS: Distributed Denial of Service Attack in Communication Standard Vulnerabilities in Smart Grid Applications and Cyber Security with Recent Developments', 9 Energy Reports (2023) 1321.
- 11 See D. Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc A/HRC/35/22, 30 March 2017, §8.
- 12 'Finnish Government Websites Hit by Cyber Attack During Zelenskyy Speech', Euronews, 8 April 2022, <https://www.euronews.com/2022/04/08/finnish-government-websites-hit-by-cyberattack-during-zelenskyy-speech>.
- 13 'Russian Hackers Claim Responsibility for Cyberattack on Lithuania', Al Jazeera, 27 June 2022, <https://www.aljazeera.com/news/2022/6/27/russia-hackers-claim-responsibility-for-cyber-attack-on-lithuania>.
- 14 D. Campbell, 'Russia's DDoS Attack on Czech Banks to Cut-Off Ukraine', RIT Cyber Security Policy and Law Class Blog, 28 November 2023, <https://ritcyberselfdefense.wordpress.com/2023/11/28/russias-ddos-attack-on-czech-banks-to-cut-off-ukraine/> (last accessed 18 January 2025).
- 15 'Ukrainian Intelligence Targets Ruling United Russia Party in Large-Scale Cyber Attack', The New Voice of Ukraine, 26 April 2024, <https://english.nv.ua/nation/ukrainian-military-intelligence-officers-launch-cyberattack-on-united-russia-party-services-50413618.html>.
- 16 J. Tidy, 'Anonymous Sudan Hacks X to Put Pressure on Elon Musk Over Starlink', BBC News, 31 August 2023, <https://www.bbc.co.uk/news/technology-66668053>.
- 17 "'Misinformation" vs. "Disinformation": Get Informed on the Difference', Dictionary.com, 15 August 2022, <https://www.dictionary.com/e/misinformation-vs-disinformation-get-informed-on-the-difference/> (last accessed 18 January 2025). Note: malinformation is a controversial term for information that is based on fact, but removed from its original context in order to mislead, harm or manipulate.
- 18 Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms: Report of the Secretary-General, UN doc A/77/287, 12 August 2022, §3.
- 19 K. Somoray and D. J. Miller, 'Providing Detection Strategies to Improve Human Detection of Deepfakes: An Experimental Study' (2023) 149 Computers in Human Behavior, <https://doi.org/10.1016/j.chb.2023.107917>; N. Jacobson 'Deepfakes and Their Impact on Society' (2024) <https://www.openfox.com/deepfakes-and-their-impact-on-society/>
- 20 'Iranian Hackers Interrupt UAE Broadcasts With Deepfake News', VOA, 8 February 2024, <https://www.voanews.com/a/iranian-hackers-interrupt-uae-broadcasts-with-deepfake-news-/7480126.html>.
- 21 'Doctored Nancy Pelosi Video Highlights Threat of "Deepfake" Tech', CBS News, 26 May 2019, <https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/>.
- 22 See generally, O. Habibi, M. Chemmakha and M. Lazaar, 'Imbalanced Tabular Data Modelization Using CTGAN and Machine Learning to Improve IoT Botnet Attacks Detection', 118 Engineering Applications of Artificial Intelligence (2023).
- 23 NATO Defence Education Enhancement Programme, Troll Factories, [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/5/pdf/2005-deeportal2-troll-factories.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deeportal2-troll-factories.pdf) (last accessed 18 January 2025).
- 24 See S. Bradshaw, H. Bailey and P. N. Howard, Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, Oxford Internet Institute, 2021, <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf> (last accessed 18 January 2025).
- 25 Centre for Strategic and International Studies, Significant Cyber Incidents dataset, <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents#main-content> (last accessed 27 October 2024).
- 26 S. Lyngaas, 'Albania Blames Iran for Second Cyberattack Since July', CNN, 12 September 2022, <https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html>.
- 27 T. Pullar-Strecker, 'Russian Hackers May Be Behind "DDoS" Attack on NZ Parliament Website', The Post, 19 July 2023, <https://www.thepost.co.nz/business/350038942/russian-hackers-may-be-behind-ddos-attack-nz-parliament-website>.
- 28 Center for Strategic & International Studies (CSIS), 'Significant Cyber Incidents', <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> (last accessed 18 January 2025).
- 29 'France's Assemblée Nationale Website Temporarily Blocked by a Group of Pro-Russian Hackers', Le Monde, 27 March 2023, [https://www.lemonde.fr/en/pixels/article/2023/03/27/france-s-assemblee-nationale-website-temporarily-blocked-by-a-group-of-pro-russian-hackers\\_6020872\\_13.html](https://www.lemonde.fr/en/pixels/article/2023/03/27/france-s-assemblee-nationale-website-temporarily-blocked-by-a-group-of-pro-russian-hackers_6020872_13.html).
- 30 European Investment Bank (@EIB), X, 19 June 2023, <https://x.com/EIB/status/1670783791600656384?lang=en> (last accessed 18 January 2025).
- 31 UN, Summit of the Future Outcome Documents, supra fn 1, p 37.
- 32 Ibid, Objective 1, p 39.
- 33 See Art 19, Universal Declaration of Human Rights (UDHR); Art 19, International Covenant on Civil and Political Rights (ICCPR).
- 34 R. Celorio, 'The Cyber World and Human Rights: Perspectives on International Accountability', Stimson, 13 September 2024, <https://www.stimson.org/2024/the-cyber-world-and-human-rights-perspectives-on-international-accountability/> (last accessed 18 January 2025).

- 35 UN, Summit of the Future Outcome Documents, *supra* fn 1, p 43.
- 36 Land and Aronson, 'Human Rights and Technology', *supra* fn 3, 226.
- 37 See B. E. Harcourt, *Against Prediction: Sentencing, Policing, and Punishing in an Actuarial Age*, Chicago Public Law and Legal Theory Working Paper No. 94, 2005, p 36, [https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1021&context=public\\_law\\_and\\_legal\\_theory](https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1021&context=public_law_and_legal_theory) (last accessed 18 January 2025).
- 38 See further UN Human Rights Committee (HR Committee), General Comment No. 37 (2020) on the Right of Peaceful Assembly (Article 21), UN doc CCPR/C/GC/37, 17 September 2020, §2.
- 39 N. Jiang, J. Wen, J. Li, X. Liu and D. Jin, 'GATrust: A Multi-Aspect Graph Attention Network Model for Trust Assessment in OSNs', 35 *IEEE Transactions on Knowledge and Data Engineering* 6 (2023). See further K. J. Strandburg, 'Surveillance of Emergent Associations: Freedom of Association in a Network Society', in A. Acquisti, S. Gritzalis, C. Lambrinouidakis and S. di Vimercati (eds), *Digital Privacy: Theory, Technology, and Practices*, Auerbach Publications, 2007, p 437; see also Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests: Report of the United Nations High Commissioner for Human Rights, UN doc A/HRC/44/24, 24 June 2020.
- 40 See Strandburg, 'Surveillance of Emergent Associations', *supra* fn 39, pp 435, 438.
- 41 See Appendix to the Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics, 19 September 2001.
- 42 See further C. McCue, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*, Elsevier, 2007; T. Scassa, 'Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges', 14 *SCRIPTEd* (2017); R. Montasari, 'The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights', in R. Montasari, *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*, Springer, 2023.
- 43 See Arts 2(1) and 26, ICCPR .
- 44 V. L. Raposo, 'When Facial Recognition Does Not "Recognise": Erroneous Identifications and Resulting Liabilities', 39 *AI & SOCIETY* 4 (2024).
- 45 See generally, J. Lerman, 'Big Data and its Exclusions' 66 *Stanford Law Review Online* (2013) 55.
- 46 See K. Crawford, 'Think Again: Big Data', *Foreign Policy*, 10 May 2013, <https://foreignpolicy.com/2013/05/10/think-again-big-data/>.
- 47 See further HR Committee, General Comment No. 37, *supra* fn 38, §61. See also Joint Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the Proper Management of Assemblies, UN doc A/HRC/31/66, 4 February 2016, §73; HR Committee, Concluding Observations on the Fourth Periodic Report of the Republic of Korea, UN doc CCPR/C/KOR/CO/4, 3 December 2015, §§42-43.
- 48 HR Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, §7; HR Committee, General Comment No. 37, *supra* fn 38, §§41-47; Art 22(2), ICCPR.
- 49 Where authorities place a constraint on citizens' enjoyment of a particular right, such a limitation must be sufficiently narrow and, crucially, prove to be a necessity in protecting the permissible purposes of applying the restriction. The principle of proportionality maintains that the law in place effectively enables the least intrusive instrument amongst those that might achieve the desired result. The principle of proportionality is discussed further in General Comments Adopted by the Human Rights Committee Under Article 40, Paragraph 4, of the International Covenant on Civil and Political Rights, UN doc CCPR/C/21/Rev.1/Add.9, 1 November 1999, §§11-16.
- 50 For further guidance see UNGA Res 68/1670, 21 January 2014, §23.
- 51 See S. Migliano, 'Government Internet Shutdowns Cost \$7.69 Billion in 2024', *Top10VPN*, 2 January 2025, <https://top10vpn.com/research/cost-of-Internet-shutdowns/> (last accessed 18 January 2025).
- 52 C. N. Voule, *Ending Internet Shutdowns: A Path Forward: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, UN doc A/HRC/47/24/Add.2, 15 June 2021, §§12-20, 31.
- 53 See Impact of New Technologies, *supra* fn 39, §18.
- 54 For example, Belarus – 'Belarus: UN Rights Chief Condemns Violence Against Protestors, Calls for Grievances to be Heard', UN News, 12 August 2020, <https://news.un.org/en/story/2020/08/1070112> (last accessed 18 January 2025); and Niger – Amnesty International, 'Niger: Post-Election Period Marred by Violence, Mass Arrests and Internet Disruption', 4 March 2021, [www.amnesty.org/en/latest/news/2021/03/niger-post-election-period-marred-by-violence/](https://www.amnesty.org/en/latest/news/2021/03/niger-post-election-period-marred-by-violence/) (last accessed 18 January 2025).
- 55 Voule, *Ending Internet Shutdowns*, *supra* fn 51, §33.
- 56 Impact of New Technologies, *supra* fn 38, §20.
- 57 *Ibid.*
- 58 In February 2016 the Central Bank of Bangladesh was hacked via vulnerabilities in its electronic payment messaging system, resulting in losses of more than USD 100 million. See T. Maurer and A. Nelson, 'The Growing Global Cyber Threat', *International Monetary Fund*, Spring 2021, <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm> (last accessed 18 January 2025).
- 59 Swedish air traffic control was interrupted by a cyberattack in November 2015. See 'Russia Blamed for Swedish Air Traffic Hack', *Cyber Security Intelligence*, 27 April 2016, <https://www.cybersecurityintelligence.com/blog/russia-blamed-for-swedish-air-traffic-hack-1254.html>.
- 60 The right to participate in public affairs is codified in international law in Art 2, UDHR, Art 25, ICCPR, as well as in articles of other international treaties such as the Convention on the Elimination of all forms of Discrimination Against Women, the International Convention on the Elimination of all forms of Racial Discrimination and the Convention on the Rights of Persons with Disabilities.
- 61 CSIS, 'Significant Cyber Incidents', *supra* fn 25.
- 62 J.Schickler, 'DutchCyberAttacksLatestinEUElectionCampaignMarredbyDisruption and Violence', *Euronews*, <https://www.euronews.com/my-europe/2024/06/07/dutch-cyberattacks-latest-in-eu-election-campaign-marred-by-disruption-violence>.
- 63 A. Ford, 'Germany's CDU Hit by Major Cyberattack', *Politico*, 2 June 2024, <https://www.politico.eu/article/germany-cdu-politically-motivated-cyberattack-russia-military-intelligence/>.
- 64 CSIS, 'Significant Cyber Incidents', *supra* fn 25.
- 65 *Cyber Law Toolkit*, 'Homeland Justice Operations Against Albania (2022)', [https://cyberlaw.ccdcoe.org/wiki/Homeland\\_Justice\\_operations\\_against\\_Albania\\_\(2022\)](https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022)) (last accessed 18 January 2025).
- 66 F. Bajak and The Associated Press, 'Hacker Says They Broke Into FBI's 80,000-Member InfraGard Database by Posing as Financial Firm CEO', *Fortune*, 15 December 2022, <https://fortune.com/2022/12/15/hacker-says-they-broke-into-fbi-80000-member-infragard-database-posing-financial-firm-ceo/>.
- 67 See HR Committee, General Comment No. 34: Article 19: Freedoms of Opinion and Expression, UN doc CCPR/C/GC/34, 12 September 2011; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and

expression, UN doc A/71/373, 6 September 2016; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN doc A/HRC/29/32, 22 May 2015.

68 It is noteworthy that blanket internet shutdowns are likely to constitute a form of collective punishment, and thus be prohibited by treaty in both international and non-international armed conflicts, more specifically Common Art 33 of the Fourth Geneva Convention and Art 4 of Additional Protocol II.

69 A. Bhattacharya, 'India Shuts Down the Internet Far More than Any Other Country', *Rest of World*, 27 September 2024, <https://restofworld.org/2024/india-internet-shutdown-record/>.

70 Z. Rosson, F. Antonio and C. Tackett, *Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022*, Access Now, February 2023, 2022-KIO-Report-final.pdf (last accessed 18 January 2025), p 4. See also Access Now, #KeptOn STOP [Shutdown Tracker Optimization Project] Data 2016–2023, <https://www.accessnow.org/keepiton-2016-2022-data/> (last accessed 18 January 2025).

71 'Internet Shutdowns in India: Explained, Pointwise', ForumIAS, 22 July 2023, <https://forumias.com/blog/internet-shutdowns-in-india-explained-pointwise/> (last accessed 18 January 2025); K. Ruijgrok, 'Understanding India's Internet Shutdowns', *Internet Society Pulse*, 23 June 2021, <https://pulse.internetsociety.org/blog/understanding-indias-internet-shutdowns> (last accessed 18 January 2025).

72 D. Mukhopadhyay and A. Gupta, 'Jammu & Kashmir Internet Restrictions Cases: A Missed Opportunity to Redefine Fundamental Rights in the Digital Age', 9 *Indian Journal of Constitutional Law* 207 (2020). For instance, out of the total number of shutdowns that occurred in the country in 2022, 49 were enforced in Kashmir. See 'Internet Freedom in India – Statistics & Facts', Statista, 24 May 2024, <https://www.statista.com/topics/6071/internet-freedom-in-india/#topicOverview> (last accessed 18 January 2025).

73 Mukhopadhyay and Gupta, 'Jammu & Kashmir Internet Restrictions Cases', supra fn 72, 210.

74 'Jammu and Kashmir: Rights Group Calls Communications Blockade "digital apartheid"', *Scroll*, 26 August 2020, <https://scroll.in/latest/971432/jammu-and-kashmir-ngo-calls-communications-blockade-digital-apartheid-collectivepunishment>.

75 See A. Rajvanshi, 'How Internet Shutdowns Wreak Havoc in India', *Time*, 15 August 2023, <https://time.com/6304719/india-internet-shutdowns-manipur/>: 'In addition to cutting off the internet, the government also routinely blocks specific websites or successfully pushes social media platforms to block content in India'.

76 'India Restores 4G Mobile Internet in Kashmir After 550 Days', *The Independent*, 6 February 2021, <https://www.independent.co.uk/news/india-restores-4g-mobile-internet-in-kashmir-after-550-days-kashmir-india-ban-internet-activists-b1798530.html>; Rajvanshi, 'How Internet Shutdowns Wreak Havoc in India', supra fn 75.

77 M. Krishnan, 'Kashmir at Epicentre of India's Spate of Internet Shutdowns', *RFI*, 4 March 2023, <https://www.rfi.fr/en/international/20230304-kashmir-at-epicentre-of-india-s-spate-of-internet-shutdowns>.

78 Art 370, introduced in 1949, granted Jammu and Kashmir special autonomy, enabling it to have its own constitution, flag and official language. Art 35A, often referred to as the 'Permanent Residents Law', granted Kashmir's residents certain rights and privileges related to property, public aid, welfare programmes and public sector employment, thereby safeguarding the rights of the region's minority communities. See G. Howard, 'India's Removal of Kashmir's Special Protection Status: An Internationally Wrongful Act?', 28 *University of Miami International and Comparative Law Review* 2 (2021) 501.

79 See A. Kalra, S. Miglani and D. Ismail, 'India Scraps Special Status for Kashmir in Step Pakistan Calls Illegal', *Reuters*, 5 August 2019, <https://www.reuters.com/article/world/india-scraps-special-status-for-kashmir-in-step-pakistan-calls-illegal-idUSKCN1UV0E8/>.

80 Estimates suggest that this shutdown had an economic cost of over £1.9 billion and resulted in nearly 500,000 jobs lost. V. Shastry, 'Asia's Internet Shutdowns Threaten the Right to Digital Access', *Chatham House*, 18 February 2020, <https://www.chathamhouse.org/2020/02/>

[asia-internet-shutdowns-threaten-right-digital-access](#) (last accessed 18 January 2025).

81 'India Restores 4G Mobile Internet in Kashmir After 550 Days', supra fn 74. See also S. Gupta, 'Internet Shutdowns in Asia: Locating the Right to the Internet a Human Right Under International Human Rights Law', *Cambridge Core Blog*, 15 March 2023, <https://www.cambridge.org/core/blog/2023/03/15/internet-shutdowns-in-asia-locating-the-right-to-the-internet-a-human-right-under-international-human-rights-law/> (last accessed 18 January 2025); R. Hassan, 'Digital Exclusion and its Impact on Journalism in Kashmir', 19 *E-Learning and Digital Media* 5 (2022) 489–490.

82 A. Rai, 'Modi Government's Internet Blackouts Hurt the Poor and Curbed Job Opportunities, HRW Says', *The Independent*, 14 June 2023, <https://www.independent.co.uk/asia/india/internet-blackouts-modi-kashmir-hrw-report-b2356573.html>. See also Mukhopadhyay and Gupta, 'Jammu & Kashmir Internet Restrictions Cases', supra fn 70, 209. See also International Federation of Journalists, 'India: A Grim Milestone, 365 Days of Internet Shutdown in Kashmir', 5 August 2020, <https://www.ifj.org/media-centre/news/detail/category/press-releases/article/india-a-grim-milestone-365-days-of-internet-shutdown-in-kashmir> (last accessed 18 January 2025).

83 Art 19, UDHR, and Art 19, ICCPR, guarantee the right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media.

84 See generally, M. Novak, *UN Covenant on Civil and Political Rights: CCPR Commentary*, 2nd edn, Engel, 2005.

85 HR Committee, General Comment No. 34, supra fn 67, §11. See also ECtHR, *Handyside v the United Kingdom*, Judgment, App no 5493/72, 7 December 1976, §49.

86 HR Committee, General Comment No. 34, supra fn 67, §§47 and 49. See also ECtHR, *Salov v Ukraine*, Judgment, App no 65518/01, 6 September 2005, §113: 'Article 10 of the [European] Convention [on Human Rights, on freedom of expression] does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful.'

87 See further *Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms*, supra fn 18.

88 Annual Report of the United Nations High Commissioner for Human Rights, Addendum: Report of the High Commissioner for Human Rights on the Expert Workshops on the Prohibition of Incitement to National, Racial or Religious Hatred, UN doc A/HRC/22/17/Add.4. The Rabat Plan of Action provides guidance on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, through the lens of six factors. These factors include the context of the statement, the status of the speaker, the intent to incite the audience against a target group, the content and form of the expression, the extent of its dissemination and the likelihood of harm.

89 UN, *Summit of the Future Outcome Documents*, supra fn 1, p 15.

90 Amnesty International, 'Everybody Here is Having Two Lives or Phones': The Devastating Impact of Criminalization on Digital Spaces for LGBTQ People in Uganda, p 11, <https://www.amnesty.org/en/documents/afr59/8571/2024/en/> (last accessed 18 January 2025).

91 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, UN doc A/78/288, 7 August 2023, §16.

92 Amnesty International, 'Everybody Here is Having Two Lives or Phones', supra fn 90, p 11.

93 See Art 2(2), ICCPR, and HR Committee, General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN doc CCPR/C/21/Rev.1/Add.13, 26 May 2004.

94 See HR Committee, General Comment No. 31, supra fn 93, §8.

---

95 See Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, UN doc A/HRC/17/31, 21 March 2011, Annex, Principle 1.

---

96 HR Committee, General Comment No. 31, supra fn 93, §7; Report of the Special Representative of the Secretary-General, supra fn 93, Annex, Principles 3 and 25.

---

97 Report of the Special Representative of the Secretary-General, supra fn 95, Annex, Principle 11.

---

98 United Nations Office of the High Commissioner for Human Rights, Business and Human Rights in Challenging Contexts: Considerations for Remaining and Exiting, August 2023, <https://www.ohchr.org/sites/default/files/documents/issues/business/bhr-in-challenging-contexts.pdf> (last accessed 18 January 2025).

---

99 See generally, S. Bradshaw, H. Bailey and P. N. Howard, Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, Oxford Internet Institute, 2021, <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf> (last accessed 18 January 2025).

---

100 Voule, Ending Internet Shutdowns, supra fn 52.

---

101 Report of the Special Rapporteur on the situation of human rights in Myanmar, Thomas H. Andrews, UN doc A/HRC/46/56, §74.

---

102 Z. Rosson, F. Anthonio and C. Tackett, Shrinking Democracy, Growing Violence: Internet Shutdowns in 2023, Access Now, May 2024, <https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf> (last accessed 18 January 2025).

---

103 Statement issued 17 September 2021 via <https://www.webwire.com/ViewPressRel.asp?ald=279200>

## THE GENEVA ACADEMY

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and protection of human rights.

## DISCLAIMER

The Geneva Academy of International Humanitarian Law and Human Rights is an independent academic centre. Our publications seek to provide insights, analysis and recommendations, based on open and primary sources, to policymakers, researchers, media, the private sector and the interested public. The designations and presentation of materials used, including their respective citations, do not imply the expression of any opinion on the part of the Geneva Academy concerning the legal status of any country, territory, or area or of its authorities, or concerning the delimitation of its boundaries. The views expressed in this publication represent those of the authors and not necessarily those of the Geneva Academy, its donors, parent institutions, the board or those who have provided input or participated in peer review. The Geneva Academy welcomes the consideration of a wide range of perspectives in pursuing a well-informed debate on critical policies, issues and developments in international human rights and humanitarian law.

**The Geneva Academy  
of International Humanitarian Law  
and Human Rights**

Villa Moynier  
Rue de Lausanne 120B  
CP 1063 - 1211 Geneva 1 - Switzerland  
Phone: +41 (22) 908 44 83  
Email: [info@geneva-academy.ch](mailto:info@geneva-academy.ch)  
[www.geneva-academy.ch](http://www.geneva-academy.ch)

**© The Geneva Academy  
of International Humanitarian Law  
and Human Rights**

This work is licensed for use under a Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International License (CC BY-NC-ND 4.0).