Dystopia is now: Digital authoritarianism and human rights in Asia

Mark Anthony V Ambay III,* Neha Gauchan,** Mahesti Hasanah*** and Numfon K Jaiwong****

Abstract: The advent of new information and communication technologies has opened up new economic opportunities, heightened the availability of information, and expanded access to education and health knowledge and services. These technologies have also provided new avenues for political, economic, social participation, and have presented new opportunities and methods for the advancement of human rights. At the same time, these same technologies can be used to violate human rights. This article queries as to how exactly states and other actors use digital authoritarianism to limit human rights. The study aims to understand what threats to human rights are presented by using new information and communication technologies. The article critically examines available literature on authoritarian practices using information and communication technologies, reports of government and intergovernmental bodies, non-governmental organisations, and various media agencies as well as by gathering first-hand data of samples of digital authoritarianism. The article argues that states and other actors practise digital authoritarianism by invading privacy, denying access to information and spreading misinformation, and limiting expression and participation, all of which violate the rights to freedom of expression, information and participation. Case studies of digital authoritarian practices are presented in the study, drawing on experiences and circumstances in several Asian countries.

Key words: digital authoritarianism; authoritarian practices; human rights; Asia; information and communication technology

1 Introduction

Every move you make is watched by millions of cameras, recorders and applications around you, even inside your own home. You wish to contact your family and friends but the network is down. You go online to read the news on what is happening, but your screen says 'HTTP 404'. You post #WhatIsHappening on your social media account but the post does not go through. A few hours later, security officers knock on your door to take you away. You are never heard again.

This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. MA (Human Rights and Democratisation); Programme Manager, Global Campus of Human Rights Asia Pacific; ihrpmhrd@mahidol.edu MA (Human Rights and Democratisation); Researcher, ChildSafeNet Nepal,

^{**} neha.gauchan.96@gmail.com

^{***} MA (Human Rights and Democratisation); Researcher, Research Centre for Politics and Government, Universitas Gadjah Mada; mahesti.hasanah@mail.ugm.ac.id

^{****} MA (Human Rights and Democratisation); fonjaiwong@gmail.com

While the situation sounds like it is straight out of a dystopian, futuristic science fiction film, it is not. It is happening, today, in nearly all countries. New information and communication technologies (ICTs) can help bridge social and economic inequalities by opening up new economic opportunities and helping to uplift countless millions from poverty, heightening the availability of information necessary for better policy and decision making, and expanding access to education and health services. These new ways of obtaining and exchanging information and communication with other people have also provided new avenues for political, economic and social participation. Advocacy groups, in particular, are successfully making use of these ICTs, especially the internet, in working for human rights, democracy and peace in even the most closed-off, authoritarian countries.

Yet, these same ICTs must also be viewed as a double-edged sword. Political actors, particularly governments, recognise the potential of ICTs, and many repressive regimes have subsequently developed new ways of limiting human rights and democracy using ICTs in a phenomenon that the advocacy group Freedom House has dubbed the 'rise of digital authoritarianism' (Freedom House 2018). Hence, this study explores how exactly states and other actors use digital authoritarianism to limit human rights.

This article aims to better understand the threats to human rights by using new ICTs. It seeks to identify the various ways in which states and other vested actors are using ICTs to limit access to and the exchange of information and communications to stifle opposition and dissent. The article critically examines relevant literature, reports of governments and intergovernmental bodies, non-governmental organisations (NGOs) and various media agencies as well as by gathering first-hand data of samples of digital authoritarianism, the article argues that states and other actors practise digital authoritarianism by invading privacy, denying access to information and spreading misinformation, and limiting expression and participation, all of which violate the rights to freedom of expression, information and participation. After reviewing research on the current status of digital authoritarianism. The article illustrates how digital authoritarianism is practised specifically in the Asian Pacific.

2 Authoritarianism in the digital sphere

The world is currently experiencing a 'global turn to authoritarianism' (Murakami Wood 2017: 358). This trend threatens to reverse the gains made by human rights movements in the last several decades. It is important to study how authoritarianism, in all its forms, affects human rights in order to better defend human rights against it. Political studies at one point or another invariably refer to Spanish political scientist Juan Linz in defining authoritarianism. Linz (2000: 159) saw authoritarianism as a political system that has limited political pluralism, lacks a guiding ideology but with a distinctive mentality, with the limited or minimal political mobilization of and participation by the populace, and ill-defined powers of the leaders.

It is not surprising to hear that under the presidency of Xi Jinping, 'China appears more authoritarian, not less' (Ang 2018) or that there is 'a

deepening of authoritarian rule' in Thailand (Mérieau 2018). However, in supposedly democratic countries in Asia, where elections are regularly held and civil and political liberties are supposedly guaranteed by law, commentators consider that 'an authoritarian India has emerged' (Nilsen 2018) and that 'the Philippines just became more authoritarian' (Santos 2019). It seems that, currently, Linz's definition of authoritarianism no longer is as clear-cut as before.

International relations scholar Glasius (2018) suggests that instead of focusing on authoritarian regimes or leaders, the study should be one of the authoritarian practices, thus allowing an analysis of the actions of political actors once they are in power. This goes beyond state-centric or single-state analyses of authoritarianism to explore settings that transcend state boundaries, and identify and interrogate the involvement of both state and non-state actors involved in authoritarianism.

This suggestion also means that authoritarian practices can be analysed in even so-called democratic countries, where the classic definitions of authoritarianism do not apply. The study of authoritarian practices can also be utilised in analysing how ICT is being used to suppress rights and freedoms through arbitrary surveillance, secrecy and disinformation, and the violation of freedom of expression (Glasius & Michaelsen 2018).

Japanese sociologist Yoneji Masuda (1980) argues that the advent of new information and communication technologies, most especially the internet, and the post-industrial 'information age' will usher in a new era of participatory democracy and democratisation, the emergence of 'information communities', and a spirit of globalism. Indeed, at least to a certain extent and for those who can avail of these new ICTs, the storage, access, and exchange of information and communication are faster and more reliable. New economic opportunities and modes of working have opened up, learning and training has become easier, and work processes are becoming more digitised and automated.

ICT has also presented new opportunities for the advancement of human rights. Social media and messaging applications such as WhatsApp have been utilised to mobilise people in defending their rights and interests (Breuer 2012; Ruijgrok 2016; Smidi & Shahin 2017). The internet plays an important role in assisting human rights organisations to gather and disseminate information about human rights to the general populace (Halpin & Hick 2000). New information storage systems make it easier to store and transport information. Even the ordinary smartphone can be a powerful tool to record and document human rights violations.

This technology, however, is a double-edged sword. Authoritarian practices in the digital sphere using ICTs are also used to restrict and violate human rights (Michaelsen & Glasius 2018). Privacy is invaded when a person's actions are continuously monitored by state-of-the-art surveillance systems, with all the data stored in a database accessible to state security forces at any given time (Lucas & Feng 2018). Internet access is restricted – or even suspended – to limit access to information that may have a bearing on social and political issues (OpenNet Initiative 2013). Shutdowns of telecommunication services are also used to prevent communications between political dissenters and to stop political mobilisation, whether spontaneous or organised (Wagner 2018).

Contrary to popular belief, these situations occur in both repressive and democratic countries, as evidenced by Hintz and Milan's study on the use of ICT for the surveillance and monitoring of citizens by governments in the 'liberal West' (Hintz & Milan 2018). Another example would be the use of social media in manipulating public opinion through employing fake social media accounts to support the candidacy of Donald Trump when he was running for President of the United States (Mayer 2018). In this regard, Freedom House (2018) refers in its report to the 'rise of digital authoritarianism'.¹

3 Defining digital authoritarianism

Before attempting to define digital authoritarianism as a concept, it is important to acknowledge that this article builds on the definition of authoritarian practices by Michaelsen and Glasius (2018). In their essay they introduce the twin concepts of illiberal and authoritarian practices. The former, they argue, infringes on the 'autonomy and dignity of a person' (Michaelsen & Glasius 2018: 3797). As such, it is a human rights issue. The latter, on the other hand, sabotages accountability, thereby threatening democratic processes and therefore is a democracy problem (Michaelsen & Glasius 2018: 3797).

Michaelsen and Glasius (2018: 3796) argue that threats to people in the digital sphere can be arranged into three categories: arbitrary surveillance; secrecy and disinformation; and violations of freedom of expression or disabling voice. While arbitrary surveillance is an illiberal practice and, therefore, a human rights violation, secrecy and information are authoritarian practices as it sabotages the accountability of leaders to their constituents. Violations of freedom of expression, they argue, are both illiberal and authoritarian practices (Michaelsen & Glasius 2018: 3804). This is where this article diverges from Michaelsen and Glasius. All three above-mentioned categories are human rights issues and lead to human rights abuses in the digital sphere. Each of these three categories violates specific human rights, as laid out in the major Covenants. Arbitrary surveillance violates one's right to privacy while secrecy and disinformation go against the right to information. The third category is stated as a violation of freedom of expression, but it is also a violation of the right to participation, and the right to be involved in political and public affairs. Thus, with regard to this article, it matters little whether the three categories mentioned by Michaelsen and Glasius affect the individual or sabotage accountability. What is clear is that they violate universally-recognised human rights. They are, therefore, human rights issues.

With this in mind, we define digital authoritarianism as practices using information and communication technology designed to either invade privacy, deny access to information, spread misinformation, limit expression, and limit political participation.

1 The report lacks a precise definition of what exactly digital authoritarianism constitutes. Despite this weakness, the report is useful in assessing current trends on the use of new ICTs in suppressing freedoms and rights.

4 (Digital authoritarian) practice makes perfect

In an effort to control information and communications, several Asian governments engage in digital authoritarianism, often in cooperation with government-controlled or private companies that provide information and communication technology and services. These efforts are usually backed up by draconian laws and policies that allow governments to control the ingress and outflow of information and communications where they deem fit. There are at least 29 laws and policies in 15 countries in the region that give governments the authority to access personal data, shut down communications, and limit or block information exchange, with no mechanisms available to appeal. Other countries, while not having specific policies governing information and communication, have established regulatory bodies with sweeping powers that often have little oversight and accountability. In many countries there are both regulatory bodies and the laws that empower them. National security or public safety is frequently used as a justification. However, in many instances, curbing public discontent is the underlying reason, as the examples in this part will show.

5 Invasion of privacy: Surveillance and censorship

In the past two decades Asian governments have been using technical and legal strategies to regulate online content. A confluence of technology, behavioural science and market power has been used to increase internet surveillance and censorship in many countries (Clark et al 2017). The best example is China where authorities restrict access of citizens to information, searches and applications available on the internet. Since 2018, all the internet and application providers, such as Alibaba, Baidu, Byte Dance and Tencent, are required to keep a log with information such as activities of users posting on blogs, chat rooms, short video platforms and webcasts, which the authorities can monitor or access at any time. This ruling is aimed at preventing online users from engaging in activities that would potentially influence public opinion. In April 2018, Chinese authorities ordered Byte Dance to shut down a popular social media platform where users often shared jokes, videos and GIFs, which the governments regarded as displaying improper public opinion. Later, in December 2018, Reuters reported that China has closed 1 100 social media accounts and 31 websites that it accused of unlawful activities such as trolling or blackmail (Meyer 2018).

All internet or application providers in China are Chinese companies as foreign internet sites and applications are censored and blocked. Chinese companies are required to log information for authorities to monitor at any time, giving the government absolute power to monitor its digital space. China recently developed a new high-technology surveillance system scoring its citizens, called 'social credit'. This ranking of social credit will monitor the behaviour of China's enormous population. The social credit system, which was first announced in 2014 and is due to be fully operational nationwide by 2020, is currently being piloted for millions of people across the country. A person's social score can move up and down depending on their behaviour, such as bad driving, smoking in non-smoking zones, purchasing too many video games, and posting fake

news online (Ma 2018). A high social score means that they will receive a variety of privileges, such as discounted energy bills and the ability to forgo deposits on car and rental properties. In addition, they might get better treatment at Chinese hospitals (Marr 2019). However, as far as those with low scores are concerned, China has already started punishing people by restricting their travel. Channel News Asia (cited by Ma 2018) reported in March that over nine million people with low scores have been blocked from buying tickets for domestic flights. Furthermore, the government can ban them or their children from enrolling in the best schools. Beijing News reported that 17 people who had refused to do military service were barred from enrolling for higher education, applying for high school, or continuing their studies (Xueying 2018). Individuals would also be banned from managerial employment in state-owned firms and large banks, as well as being publicly named bad citizens. The scores are to be monitored by high-technology surveillance cameras. Across China more than 200 million cameras will be equipped with facilities for facial recognition, body scanning, and geo-tracking in order to keep a constant vigil over every citizen.

China is not the only country that aims to use this high-technology surveillance system. Chinese surveillance and security start-up technology has made its foray into Malaysia, by the supply of wearable cameras with artificial intelligence-powered facial recognition technology to local law enforcement agencies (Tan 2018). In January 2018 the Chinese company Yitu opened its first overseas office in Singapore to serve Southeast Asia, Hong Kong, Macau and Oceania. The Yitu technology can identify a person from its database of 1.8 billion people within three seconds with an accuracy of 95 per cent. This technology is being used in public spaces such as airports, banks and hospitals in China (Tan 2018). Investment in AI in the Asia-Pacific region has grown in prominence as governments seek to adopt technologies for urban management. This has raised concerns over the privacy of an individual and their basic fundamental rights.

6 Misinformation and the right to information

6.1 Fake news and misinformation

States have jumped into cyberspace to create and present their information, but in many cases this is not representing factual information. For example, India, where Facebook users exceed 300 million, experienced violence incited by falsities about child abductions spread mostly via social media. WhatsApp and other social networks led to 24 deaths from mob violence (Fernandez 2019). Scores of people across the country were lynched by mobs that suspected them of being child kidnappers (Jain 2018). Unfortunately the incidence of child kidnapping is increasing, so the fake news and disinformation in this case has allowed the actual child traffickers to continue as they are not spotted by mobs.

In Thailand the military junta filed charges against Thanathorn Juangroongruangkit, the leader of the Future Forward Party (FFP), for spreading fake information under the Computer Crimes Act. Thanathorn argued that the law was used to silence and threaten opposition (Fernandez 2019). The FFP was one of the main opposition parties to the

National Council for Peace and Order (NCPO) to the Thai junta during the general election in the early of 2019. The NCPO filed a complaint with the Technology Crime Suppression Division (TCSD) against Thanathorn and two other members of FFP for feeding false information into a computer system. The NCPO claimed that Thanathorn had used his personal Facebook and Party Facebook pages to accuse the NCPO of luring former members of parliament to back the regime by using existing lawsuits against them as a bargaining chip. Thanathorn told reporters that 'the Computer Crimes Act is used to silence and threaten us and to create politics of fear in this country' (*Bangkok Post* 2018). These allegations have raised concerns that the new regulations are enabling the corrupt government to stifle political rivals and free speech in Thailand.

6.2 Hate speech, racism, discrimination

In 2014 the Minorities Rights Group International published State of the world's minorities and indigenous peoples, presenting case studies of 70 countries across the globe, ranking these based on the dangers of hate speech and discrimination faced by minorities. Three Asian countries, Myanmar, Afghanistan and Pakistan, are ranked in the top ten. Hate crime by definition is any crime committed as a result of hostility towards someone because of their race, ethnicity, religious beliefs, disability or sexual orientation (Anwar 2014). In Myanmar, the government continues to circulate misinformation about the Rohingya Muslims. Facebook was used by the Myanmar government to spread disinformation about tensions between its citizens to incite violence against the Rohingya people (Brown 2019). Violence has spread to other parts of the country, where the killing of Muslims has been carried out by local mobs or Buddhist groups (Seiff 2014). Discriminatory violence in Myanmar has displaced approximately one million people (ÓCHA 2018), and the Myanmar government has been accused of ethnic cleansing.

Similarly, in Pakistan the concept of freedom of religion and belief is sensitive and complicated. The minority faith groups in Pakistan not only suffer institutionalised discrimination but also prejudice spread through cyberspace. In April 2018, Pakistan's persecuted Ahmadi minority released an annual report that illustrated how members of the religious sect are consistently targeted by the state. Ahmadis are forbidden from calling themselves Muslims or using Islamic symbols in their religious practices. The report reveals that 77 Ahmadis were booked under discriminatory religious laws in 2017, nine of them remaining in prison, while four Ahmadis were murdered in hate crime across the country. Also, research has shown that Pakistan's media circulated 3 936 news reports and 532 editorial pieces that contained hate propaganda against Ahmadis (Ahmad 2018).

6.3 Digital authoritarianism and human rights in Asia: Freedom of expression and the right to participation

6.3.1 Troll armies on controlling freedom of expression and shaping public opinion

Cyber troops of troll armies are the new strategies for governments to control people's expression by shaping public opinion and its opponents. Moreover, the Philippines under the Duterte administration is known as one of the countries that employ a 'keyboard army' (Palatino 2017; Titcomb 2017; Riley & Pradhan 2018; Coca 2019). There are three methods applied by troll armies under Duterte. First, the troll armies support him during the election process. Many news platforms state that Duterte uses Facebook as a weapon to build support for him and harass his opponents (Stevenson 2019; Riley & Pradhan 2018). Palatino (2017) notes that Duterte's 'keyboard army' consisted of 400 to 500 individuals during the presidential campaign in 2016. The troll army created and distributed messages for the campaign by using both real and fake Facebook accounts. As a result, Duterte dominated the political conversation a month before the vote (Etter 2017).

Second, the drug war that has killed over 20 000 people since 2016 has its policies supported by the troll armies, and criticisms countered. News were shared thousands of times on Facebook by pro-Duterte accounts that claim that Pope Francis blessed the drug war policy at a conference held in the Vatican City (ABS.CBN.com 2018). Since the majority of the population of the Philippines is Catholic, Pope Francis is widely respected. However, the Pope never mentioned the war on drugs.



Source: The New York Times 2019 (left) and The Manila Times 2016 (right).

Finally, troll armies produce hateful news to support Duterte. One example is the arrest of the journalist Maria Ressa who criticised Duterte's administration (Riley & Pradhan 2018). As of March 2019, Maria Ressa has been arrested three times (Buan 2019). Ressa acknowledged that the attacks on her increased after *Rappler* published how Duterte supporters manipulated Facebook (Stevenson 2019). The government publicly stated that *Rappler* is foreign media that wants to abolish the accountability of its government (*The Manila Times* 2016), and Maria Ressa is a foreign actor.

The Myanmar government also has a keyboard army attached to the military regime, campaigning on Facebook for ethnic cleansing against the country's Rohingya Muslim minority group (Stewart 2019). Since roughly 40 per cent of the population uses Facebook, hateful news spread rapidly.

6.3.2 Communications shutdowns

Shutdowns of communications disrupt human rights advocacy by restricting freedom of expression and participation. In December 2018, the

Bangladesh government blocked Facebook and other social media as well as 4G and 3G mobile data service during its unusual parliament elections (Taye 2019). Moreover, at the same time the government ensured slow internet connections during student protests, and also blocked Skype and shut down several essential news sites (Taye 2019). On 5 August 2018, NetBlock.org tweeted that 'internet disruptions intensif[ied] across #Bangladesh today, particularly in and around #Dhaka. Data suggests targeted, localised just-in-time blocking in response to the protest, threatening #PressFreedom and safety' (NetBlock 2018). Slow connections indirectly reduce people's participation in the democratisation process.

Nevertheless, internet shutdowns also prevent misinformation and hoaxes. In Sri Lanka, the government shut down the internet, including Facebook, Twitter, along with YouTube and Viber, a few hours after bombings on Easter Sunday when 300 people died and many others were injured. The next day, the government extended the shutdown by blocking the website of a VPN service (Vox.com 2019). There is no doubt that the serial bombing created panic, and Facebook could not filter out the false information. Furthermore, families who were looking for their members faced difficulties. However, some people supported this strategy. One senior said that 'what the Sri Lanka government did was authoritarian, but it is also probably what needed to be done to prevent social media from really throwing fuel onto this fire afterward' (Vox.com 2019).

In May 2019, the Indonesian government slowed down the internet and social media network, and restricted the sending of pictures and videos to prevent hoax misinformation as a consequence of a violent demonstration wherein eight people died. Supporters of Prabowo, a presidential candidate who lost the election, staged a demonstration. The National Electoral Commission declared the candidate Jokowi, the winner, leading to protests by opposition groups. There was a dispute over who killed the protestors, resulting in a lack of clarity as to who should be held responsible. To halt tensions, the government shut down the internet (*The Jakarta Post* 2019). This may be interpreted as useful in terms of restricting misinformation or it could be problematic. Furthermore, the government provided neither a report on human rights violations in respect of the demonstration, nor to justify the shutdown (Amnesty International Indonesia 2019).



Blocking and content removal: Government Cyber-Control Centres

Left: One of the headlines of *People's Daily*, a newspaper in Mainland China (inksstonews.com 2019)



Right: Fake news about Hong Kong protest from *China Daily* newspaper (2019)

Another practice is the blocking and removal of content, used by the Chinese government. The picture in People's Daily shows a Hong Kong protest in June 2019. This was never a headline on the China mainland where the media blocked the information, while the left picture shows the mainland newspaper's attempt to prejudice the protest. The two pictures above demonstrate how the China government controls information. Ziccardi (2013: 249-250) explains that China is the only country that applies a complex filtering system based on a list of several forbidden keywords, such as democracy, freedom (and all compounds and derivatives, such as Free-China and Free-Net), corruption, children of party leaders, empty chair, and all words related to hatred 'Three T's' (Tibet, Tiananmen and Taiwan) (see also King 2014: 1-10; Perry & Roda 2017: 95-129). The government also has 'The 50 cent party' which produces and manipulates content for blogs and popular media websites, and ensures censorship consistency by trolling the websites in order to find and remove any unacceptable content. They prefer to remove those questionable materials that allow dubious content to circulate freely (Ziccardi 2013: 250).

The authoritarianism in Asian governments seems increasingly to converge. In China, the government established the system decades ago by integrating its system, policy, and troll. Meanwhile, ASEAN countries and Japan started their cyber security not merely as a training programme, but also as the first step towards developing a regional system. In Thailand, the programme could help them control and block information, possibly leading to restrictions on human rights defenders.

7 Arrests, detention, gagging, killings/assassinations

This part explains the restrictions put on human rights defenders in the digital space. The previous parts outline the indirect impact on human rights defenders's rights to participation through content removal and the

misuse of information. This part discusses the direct impact caused by state and non-state actors on the lives of human rights defenders, journalists and media critics, through arrests, detentions, gagging or assassination, looking at examples from countries such as Pakistan, Laos, Vietnam and Cambodia.

Pakistan is the fourth most dangerous country in the world for journalists, with 115 having been killed since 1990, as of May 2019. (Baloch & Qammar nd). Pakistan's extremely limited digital space has led many activists and journalists to be kept in detention, arrested and even assassinated. In January 2017, the Office of High Commissioner for Human Rights (OHCHR) reported that four social media and human rights activists (Waqas Goraya, Asim Saeed, Salman Haider and Ahmed Raza Naseer) had been accused of blasphemy, a criminal offence in Pakistan (Kaye 2017). These social media activists were arrested because they were critical of the state of Pakistan.



Salman Haider delivering his poem 'Kafir', Source: YouTube

Salman Haider, a social media activist, poet and lecturer, was abducted on 6 January 2017 (Zaman 2017). Along with the other activists, he was accused of spreading blasphemous content on social media because of his poem 'Kafir', a controversial term in Islam, which in Urdu literally means 'someone who knows the truth but rejects it' (Qudosi 2017). Conservative groups in Pakistan challenged his criticism of Islam and the military rule. Haider was released after almost three weeks. However, the whereabouts of the other men arrested with him are unknown (*BBC* 2017). These arrests demonstrate Pakistan's use of digital authoritarianism on its citizens to censor contents relating to issues concerning Pakistan's state affairs, religion and civil-military relationships.

Following the disappearance of these activists and other cases of blasphemous content on online media, the Pakistan Telecommunications Authority (PTA), which is the main communication channel in Pakistan, started sending out warnings to its mobile subscribers. The PTA sent out texts to millions of users which read 'Uploading and sharing of blasphemous content on internet is a punishable offence under the law. Such content should be reported ... for legal action' (Human Rights Watch 2018). The PTA also exacerbates restraints on political participation by launching media campaigns about penalties for individuals who dare express any political or religious opinions (Digital Rights Foundation 2018). This relates to freedom of expression in the digital space where individuals are not able to freely express their views and opinions on matters the state believes are criminal offences, such as blasphemy.

Activists and critics have also been arrested and detained in Laos, a oneparty state that exercises absolute control over media and ranks guite low (171) in the 2019 World Press Freedom Index (Reporters Without Borders) 2019). In June 2016, three Laotians were arrested for criticising the Communist State on their social media accounts through anti-Facebook comments and posts (Jha 2016). The 2014 decree on internet freedom mentions that anyone who negatively comments against the government can be arrested or jailed. In Cambodia, a young social media user, Heng Leakhena, was arrested in July 2017 for sharing a video on her Facebook account. The video suggested that the Prime Minister, Hun Sen, and his family had been involved in the killing of a prominent political analyst and scholar, Kem Ley, the previous year (Radio Free Asia 2017). Kem Ley often discussed the extent of the wealth of the family of Hun Sen, who had ruled Cambodia for more than 32 years, in Radio Free Asia (RFA) Khmer Service (RFA 2017). Heng faced arrest for speaking out against the government and criticising the Cambodian People's Party (CPP).

Vietnam is another example where digital authoritarianism practices are prevalent. According to the database of The88project.org (2019), a nongovernmental organisation (NGO) that supports and encourages freedom of expression in Vietnam, reported that since 2003 at least 13 activists have been arrested. Most of these activists were the supporters of democratisation in Vietnam. One arrested activist, Nguyen Dinh Khue, often posted articles on current national issues and criticised the government on Facebook. He was arrested on 30 April 2019 during the crackdown on the occasion of Vietnam's Reunification Day along with two other activists who also actively posted on the same issues on their Facebook accounts (The88project.org 2019). Nguyen and other activists in Vietnam, who have actively spoken out against Vietnam's government through social media, were arrested and detained (The88project.org 2019).

8 Conclusion

Many Asian governments have used information and communication technologies to invade privacy, deny access to information and spread misinformation, and limit expression and political participation. States that are democratic or repressive are practising digital authoritarianism. Troll armies are used, as in the case of in the Philippines under Duterte, to create content supporting the government and to lambast critics, while communication shutdowns in Bangladesh, are more common. Internet shutdowns in Sri Lanka and in Indonesia to prevent misinformation regarding the election impacted adversely on human rights advocacy. Content blocking and removal act as barriers to human rights defenders. India and Thailand have cases of fake news and misinformation. Myanmar and Pakistan rank high in terms of the proliferation of hate speech, racism and discrimination. Critics, including human rights activists and journalists, face arrest, detention, or even extra-judicial killings for their opinions in countries hit by terrorism, such as Pakistan.

When George Orwell wrote 1984, few people imagined that the events he described – horrifying, threatening, distasteful – would ever materialise. Today, 70 years later, the situation has changed radically. New technologies, in the hands of well-meaning people, are useful tools in advancing human rights. In the wrong hands, however, those rights may be threatened using the very same technologies. The dystopian society Orwell imagined is here and now. The world must ensure that this is not also our future.

References

- Agences France-Presse 'Fact check: No, Pope Francis did not bless Duterte's administration' ABS.CBN News, 13 December 2018 [online], available at https://news.abs-cbn.com/news/12/13/18/fact-check-no-pope-francis-did-not-bless-dutertes-administration (last visited 27 June 2019)
- Ahmad I Pakistan's 'Ahmadi community faces persecution, hate crime: Report' Hindustan Times 28 April 2018, available at https://www.hindustantimes.com/ world-news/pakistan-s-ahmadi-community-faces-persecution-hate-crime-report/ story-AuTwmNKaYA63pQwHqrX7oK.html (last visited 24 April 2019)
- Amnesty International Indonesia 'Penjelasan polri terkait kekerasan 21-23 Mei 2019 mengecewakan keluarga korban tewas' (Explanation from national police is disappointing the families' victims of protest on 21-23 May), https://www. amnestyindonesia.org/penjelasan-polri-terkait-kekerasan-21-23-mei-mengece wakan-keluarga-korban-tewas (last visited 27 June 2019)
- Ang YY 'Autocracy with Chinese characteristics' *Foreign Affairs* May/June 2018, available at https://www.foreignaffairs.com/articles/asia/2018-04-16/autocracychinese-characteristics (last visited 15 June 2019)
- Anwar R 'Challenges of hate crimes in Pakistan' Intersections Blog 14 July 2014, available at http://www.intersections.org/challenges-hate-crimes-pakistan (last visited 24 April 2019)
- Baloch H & Qammar 'A danger of digital surveillance. Bytes for all publications' (nd), available at https://content.bytesforall.pk/publication/dangers-digital-surveillance> (last visited 10 February 2019)
- Bangkok Post 'Future Forward leaders fight computer crime charge' Bangkok Post Online 17 September 2018, available at https://www.bangkokpost.com/thailand/ politics/1541550/future-forward-leaders-fight-computer-crime-charge (last visited 27 June 2019)
- BBC News 'China: The world's biggest camera surveillance network' BBC News 2017 (video online), available at https://www.youtube.com/watch?v=pNf4-d6fDoY&t=140s (last visited 27 June 2019)
- Bingcun L '800,000 say "yes" to rendition Bill' *ChinaDaily.com* 10 June 2019, available at http://www.chinadaily.com.cn/hkedition/2019-06/10/content_37478727.htm (last visited 27 June 2019)
- Breuer A 'The role of social media in mobilising political protest: Evidence from the Tunisian revolution' 2012 Bonn: German Development Institute, available at

https://www.die-gdi.de/uploads/media/DP_10.2012.pdf (last visited 14 June 2019)

- Brown N 'Liar, liar, platforms on fire: The rise of misinformation and what to do about it' The SpinOff. InternetNZ, 4 February 2019, available at https://the spinoff.co.nz/partner/internetnz/04-02-2019/liar-liar-platforms-on-fire-the-riseof-misinformation-and-what-to-do-about-it/ (last visited 23 April 2019)
- Buan L 'Maria Ressa arrested at NAIA over anti-dummy law' Rappler.com 29 March 2019, available at https://www.rappler.com/nation/226880-maria-ressa-arrestednaia-anti-dummy-law-case-march-29-2019 (last visited 23 April 2019)
- Clark J et al 'An uptake in communications encryption is tempered by increasing pressure on major platform providers; governments expand content restriction tactics' *The Shifting Landscape of Global Internet Censorship. Internet Monitor* 29 June 2017, available at https://thenetmonitor.org/research/2017-globalinternet-censorship (last visited 23 April 2019)
- Coca N 'The rise of disinformation and censorship in South-East Asia' Equaltimes.org 1 February 2019, available at https://www.equaltimes.org/therise-of-disinformation-and#.XL7rjqeB3MI (last visited 23 April 2019)
- Digital Rights Foundation 'Content regulation in Pakistan's digital spaces' June 2018 Human Rights Council Report, Digital Rights Foundation, available at https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/DigitalRights FoundationSubmissionSpecialRapporteurFreedomofExpression.pdf (last visited 10 February 2019)
- DW.com 'Indonesia blocking social media to '"maintain democracy" DW.Com 25 May 2019, available at https://www.dw.com/en/indonesia-blocking-socialmedia-to-maintain-democracy/a-48858283 (last visited 27 June 2019)
- Etter L 'What happens when the government uses Facebook as a weapon?' Bloomberg.com 7 December 2017, available at https://www.bloomberg.com/ news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weaponwith-a-little-help-from-facebook (last visited 23 April 2019)
- Fernandez B 'Fake news in Asian politics' Global Risk Insights 1 April 2019, available at https://globalriskinsights.com/2019/04/fake-news-in-asian-politics/ (last visited 24 April 2019)
- Freedom House 'The rise of digital authoritarianism' Freedom House 2018, available at https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20 Booklet_11_1_2018.pdf (last visited 25 February 2019)
- Glasius M 'What authoritarianism is ... and is not: A practice perspective' (2018) 94 International Affairs 515, available at https://academic.oup.com/ia/article/94/3/ 515/4992409 (last visited 10 March 2019)
- Glasius M & Michaelsen M 'Illiberal and authoritarian practices in the digital sphere' (2018) 12 International Journal of Communication 3795
- Halpin EF & Hick S 'Information: An essential tool for human rights work' in S Hick, EF Halpin & E Hoskins (eds) (2000) *Human rights and the internet* London: Macmillan Press 238
- Hintz A & Milan S 'Through a glass, darkly: Everyday acts of authoritarianism in the liberal West' 2018 12 International Journal of Communication 3939
- Human Rights Watch 'Pakistan Events of 2017' 2018, available at https://www. hrw.org/world-report/2018/country-chapters/pakistan (last visited 10 February 2019)
- Jain D 'The rising trend of child abductions in India' Live Mint Online 11 July 2018, available at https://www.livemint.com/Politics/Bv4TbeToCpVS9j4IX3 hJjN/The-rising-trend-of-child-abductions-in-India.htm (last visited 27 June 2019)

- Jha P 'Laos cracks down on social media critics' *Al Jazeera* 6 June 2016, available at https://www.aljazeera.com/news/2016/06/laos-cracks-social-media-critics-160606092251543.html (last visited 17 April 2019)
- Kaye D 'UN expert urges Pakistan to locate and return home four disappeared rights and social media activists' OHCHR News 11 January 2017, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?News ID=21074 (last visited 9 February 2019)
- King G, Pan J & Roberts ME 'Reverse-engineering censorship in China: Randomised experimentation and participant observation' (2014) 345 *Science* 1
- Linz JJ (2000) Totalitarianism and authoritarianism Boulder: Lynne Rienner Publishers Inc
- Lucas L & Feng E 'Inside China's surveillance state' *Financial Times* 20 July 2018, available at https://www.ft.com/content/2182eebe-8a17-11e8-bf9e-8771d540 4543 (last visited 29 March 2019)
- Ma A 'China has started ranking citizens with a creepy "social credit" system: Here's what you can do wrong, and the embarrassing, demeaning ways they can punish you' *Business Insider* 29 October 2018, available at https://www. businessinsider.com/china-social-credit-system-punishments-and-rewardsexplained-2018-4 (last visited 27 June 2019)
- Marr B 'Chinese social credit score: Utopian big data bliss or black mirror on steroids?' *Forbes Online* 21 January 2019, available at https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#741c3a2a48b8 (last visited 27 June 2019)
- Matsuzawa M 'Duterte camp spent \$200 000 for troll army, Oxford study finds' Philstar.com 24 July 2017, available at https://www.philstar.com/headlines/ 2017/07/24/1721044/duterte-camp-spent-200000-troll-army-oxford-study-finds (last visited 27 June 2019)
- Mayer J 'How Russia helped swing the election for Trump' *The New Yorker* 24 September 2018, available at https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump (last visited 15 June 2019)
- Mayer S 'China steps up internet surveillance by recording user activities' *CPO Magazine Online News* 19 December 2018, available at https://www.cpomaga zine.com/data-privacy/china-steps-up-internet-surveillance-by-recording-useractivities/ (last visited 23 April 2019)
- Masuda Y (1980) The information society as post-industrial society Tokyo: Institute for the Information Society
- Mérieau E 'Thailand's deepening authoritarian rule' East Asia Forum 30 January 2018, available at https://www.eastasiaforum.org/2018/01/30/thailands-deepen ing-authoritarian-rule/ (last visited 17 June 2019)
- Michaelsen M & Glasius M 'Authoritarian practices in the digital age' (2018) 12 International Journal of Communication 3788
- Murakami Wood D 'Editorial: The global turn to authoritarianism and after' (2017) 15 Surveillance and Society 357
- Netblocks 'Mobile internet speeds restricted in Bangladesh amid student protest' Netblocks.org 4 August 2018, available at https://netblocks.org/reports/bangla desh-internet-shutdown-student-protests-jDA37KAW (last visited 23 April 2019)
- Nilsen AG 'An authoritarian India is beginning to emerge' *The Wire* 31 August 2018, available at https://thewire.in/politics/an-authoritarian-india-is-beginning-to-emerge (last visited 19 June 2019)

- Office for the Coordination of Humanitarian Affairs *Rohingya refugee crisis* United Nations Office for the Coordination of Humanitarian Affairs 29 August 2018, available at https://www.unocha.org/rohingya-refugee-crisis (last visited 27 June 2019)
- Open Net Initiative 'After the Green Movement: Internet controls in Iran, 2009-2012' 2013 Open Net Initiative, available at https://opennet.net/sites/opennet. net/files/iranreport.pdf (last visited 15 March 2019)
- Palatino R 'Beware Duterte's troll army in the Philippines' Thediplomt.com 18 November 2017, available at https://thediplomat.com/2017/11/beware-dute rtes-troll-army-in-the-philippines/ (last visited 23 April 2019)
- Perry S & Roda C (2017) Human rights and digital technology: Digital tightrope London: Palgrave Macmillan
- Qudosi S '"Kafir" poem by Salman Haider' 2017, available at http://muslimre formers.com/2017/03/21/kafir-poem-by-salman-haider-translated/ (last visited 10 May 2019)
- Radio Free Asia 'Young Cambodian arrested for derogatory comments about Hun Sen on social media' Radio Free Asia 13 July 2017, available at https:// www.refworld.org/topic,50ffbce582,50ffbce58e,5a0f01d64,0,,,KHM.html (last visited 28 June 2019)
- Reporters Without Borders 'Laos: No light under the tunnel' Reporters Without Borders for Freedom of Information 2019, available at https://rsf.org/en/laos (last visited 10 February 2019)
- Riley M & Pradhan B 'A global guide to state-sponsored trolling' Bloomberg.com 19 July 2018, available at https://www.bloomberg.com/features/2018government-sponsored-cyber-militia-cookbook/ (last visited 23 April 2019)
- Ruijgrok K 'From the web to the streets: Internet and protests under authoritarian regimes' (2016) 24 *Democratization* 498
- Santos VO 'The Philippines just became more authoritarian, thanks to the people' *The New York Times* 24 May 2018, available at https://www.nytimes.com/2019/ 05/24/opinion/philippines-duterte-election-senate.html (last visited 18 June 2019)
- Seiff A 'Hate crime, racism on the rise in Southeast Asia' UCA News.com 3 July 2014, available at https://www.ucanews.com/news/hate-crime-racism-on-the-rise-in-southeast-asia/71321 (last visited 24 April 2019)
- Smidi A & Shahin S 'Social media and social mobilization in the Middle East: A survey of research on the Arab Spring' (2017) 73 India Quarterly 196
- Stevenson A 'Maria Ressa, journalist critical of Duterte, is arrested again in Philippines' *The New York Times* 28 March 2019, available at https:// www.nytimes.com/2019/03/28/business/media/maria-ressa-arrested-philippinesrappler.html (last visited 23 April 2019)
- Stewart E 'Can Facebook be trusted to combat misinformation? Sri Lanka's shutdown suggests no' Vox.co, 23 April 2019, available at https://www.vox.com/ 2019/4/23/18511640/facebook-sri-lanka-bombing-social-media-attack (last visited 27 June 2019)
- Sullivan B 'Thailand to host ASEAN-Japan cybersecurity centre to be launched in June 2018' *Thailand Business News* 2 April 2018, available at https:// www.thailand-business-news.com/asean/68592-thailand-to-host-asean-japancybersecurity-centre-to-be-launched-in-june-2018.html (last visited 27 June 2018)
- Tan C 'Malaysian police adopt Chinese AI surveillance technology' Nikkei Asian Review 18 April 2018, available at https://asia.nikkei.com/Business/Companies/

Chinas-startup-supplies-AI-backed-wearable-cameras-to-Malaysian-police (last visited 27 June 2019)

- Taye B 'Sudan, Bangladesh, DRC, Gabon start 2019 with major digital rights violations' Accesnow.org 10 January 2019, available at https://www.access now.org/sudan-bangladesh-drc-gabon-start-2019-with-major-digital-rights-violations/ (last visited 23 April 2019)
- Tehusijarana KM & Valentina J 'Jakarta riot: Government temporarily limit access to social media, messaging apps' *The Jakarta Post* 22 May 2019, available at https://www.thejakartapost.com/life/2019/05/22/jakarta-riot-government-tem porarily-limits-access-to-social-media-messaging-apps.html (last visited 27 June 2019)
- The 88 Project 'Database of persecuted activist in Vietnam' 2009, available at https://the88project.org/database/ (last visited 28 June 2019)
- The 88 Project 'Nguyen Dinh Khue' 2018, available at https://the88project.org/ profile/373/nguyen-dinh-khue/ (last visited 28 June 2019)
- Tiglao RD 'Media firm Rappler scorns constitution by getting foreign money' *The Manila Times* 28 October 2016, available at https://www.manilatimes.net/mediafirm-rappler-scorns-constitution-getting-foreign-money/293543/ (last visited 27 June 2019)
- Titcomb J 'Governments in 30 countries are paying "keyboard armies" to spread propaganda, report says' *Telegraph* 14 November 2017, available at https:// www.telegraph.co.uk/technology/2017/11/14/governments-30-countries-paykeyboard-armies-spread-propaganda/ (last visited 23 April 2019)
- Tortermvasana K 'Cybersecurity ASEAN course set for June" *Bangkok Post* 30 March 2018, available at https://www.bangkokpost.com/world/1437530/ cybersecurity-asean-course-set-for-june (last visited 27 June 2019)
- Xueying N 'Many people refused to accept military service into the blacklist of credit information' *Beijing News* 19 March 2018, available at http://www.bjnews.com.cn/news/2018/03/19/479533.html (last visited 27 June 2019)
- United Nations Report of the independent international fact-finding mission on Myanmar United Nations Human Rights Council (2018)
- Wagner B 'Understanding internet shutdowns: A case study of Pakistan' (2018) 12 International Journal of Communication 3917
- Zaman A 'Digital activists are disappearing in Pakistan' Global Voices 2017, available at https://advox.globalvoices.org/2017/01/12/digital-activists-aredisappearing-in-pakistan/ (last visited 27 June 2019)
- Zhou V 'Mainland Chinese evade censors to support Hong Kong protest' Inkstonenews.com 13 June 2019, available at https://www.inkstonenews.com/ politics/chinese-internet-users-evade-censors-support-hong-kong-protests/ article/3014352 (last visited 27 June 2019)
- Ziccardi G (2013) Resistance, liberation technology and human rights in the digital age Netherlands: Springer