Religious Populism, Cyberspace and Digital Authoritarianism in Asia

INDIA, INDONESIA, MALAYSIA, PAKISTAN, AND TURKEY

IHSAN YILMAZ
RAJA M. ALI SALEEM
MAHMOUD PARGOO
SYAZA SHUKRI
IDZNURSHAM ISMAIL
KAINAT SHAKIL

ECPS
EUROPEAN CENTER for POPULISM STUDIES

JANUARY 2022
Table of contents

1. Contents ................................................................. 1
2. Abbreviations and Acronyms ....................................... 4
3. Foreword ............................................................... 5
4. Executive Summary .................................................. 7
5. Democracies in Transition ........................................... 9
  5.1. Cyber Space and Democratic Citizenship .................... 9
  5.2. Changing Democracies ........................................... 10
  5.3. The Digital Authoritarian Toolkit .............................. 11
  5.4. Conceptual Framework .......................................... 12
    5.4.1. Obstacles to Access ....................................... 13
    5.4.2. Limits on Content ......................................... 13
    5.4.3. Violations of User Rights ................................. 14
6. Applying the Toolkit: Case Studies ............................... 15
  6.1. India ............................................................... 15
    6.1.1. Obstacles to Access ....................................... 16
    6.1.2. Limits on Content ......................................... 16
    6.1.3. Violations of User Rights ................................. 17
  6.2. Indonesia ........................................................ 19
    6.2.1. Obstacles to Access ....................................... 19
    6.2.2. Limits on Content ......................................... 20
    6.2.3. Violations of User Rights ................................. 21
6.3. Malaysia ................................................................. 22
   6.3.1. Obstacles to Access .............................................. 22
   6.3.2. Limits on Content ............................................... 23
   6.3.3. Violations of User Rights ..................................... 24
6.4. Pakistan ................................................................. 25
   6.4.1. Obstacles to Access .............................................. 25
   6.4.2. Limits on Content ............................................... 26
   6.4.3. Violations of User Rights ..................................... 27
6.5. Turkey ................................................................. 28
   6.5.1. Obstacles to Access .............................................. 29
   6.5.2. Limits on Content ............................................... 29
   6.5.3. Violations of User Rights ..................................... 30

7 Faith, Cyberspace, and Populist Authoritarianism ...................... 32
   7.1. Religious Justifications of Internet Curbs by the Government ......................... 32
   7.2. The Prominent Role of Religious Leaders in Restricting Digital Freedom ......................... 33
   7.3. Laws to Limit Blasphemy, Heresy, Heterodoxy, and Pornography ......................... 34
   7.4. More Restrictions on Religious Minorities or in Areas Where Religious Minorities Live in Large Numbers ......................... 36

8. Conclusion .................................................................. 37

9. Appendix .................................................................. 39

10. Author Bios ............................................................. 42
2. Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>BJP</td>
<td>Bharatiya Janata Party</td>
</tr>
<tr>
<td>CMA</td>
<td>Communications and Multimedia Act</td>
</tr>
<tr>
<td>CMS</td>
<td>Central Monitoring System</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed denial-of-service</td>
</tr>
<tr>
<td>ECPS</td>
<td>European Center for Populism Studies</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FRT</td>
<td>Facial recognition technology</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IRG</td>
<td>Iranian Revolutionary Guard</td>
</tr>
<tr>
<td>ISIL</td>
<td>Islamic State of Iraq and the Levant</td>
</tr>
<tr>
<td>J-KOM</td>
<td>Department of Community Communication</td>
</tr>
<tr>
<td>MCMC</td>
<td>Malaysian Communications and Multimedia Commission</td>
</tr>
<tr>
<td>RSS</td>
<td>Rashtriya Swayamsevak Sangh</td>
</tr>
<tr>
<td>TLP</td>
<td>Tehreek-e-Labaik Pakistan</td>
</tr>
<tr>
<td>OTT</td>
<td>Over-the-top media</td>
</tr>
<tr>
<td>PH</td>
<td>Pakatan Harapan</td>
</tr>
<tr>
<td>PKK</td>
<td>Kurdistan Worker’s Party</td>
</tr>
<tr>
<td>PTA</td>
<td>Pakistan Telecommunication Authority</td>
</tr>
<tr>
<td>PTI</td>
<td>Pakistan Tehreek-e-Insaf</td>
</tr>
</tbody>
</table>
I am honored to be writing this foreword for the first research report of the European Center for Populism Studies (ECPS). This newly-founded, Brussels-based independent research organization investigates and analyzes the various manifestations of populism and the challenges posed by its increasing spread across the world.

The world has been suffering from the fatal effects of the COVID-19 pandemic over the last two years. This horrible and costly experience has reminded us that we really do live in a global village in every sense. A contagion that emerged in a wet market in one part of the world spread in a matter of months to all four corners of the earth and turned rapidly into a global pandemic. As of January 17, 2022, almost 329 million people have been infected, and over 5.5 million people from every walk of life and continent have died. It is evident that problems emerging in far-flung places have the potential to affect us all in ways we could scarcely imagine.

At the risk of stretching the metaphor, the rise and spread of the most recent wave of global populism carry many of the same characteristics and pose, in the view of many, no less a global threat than COVID-19. Alongside renewed racism, rising authoritarianism, and ongoing oppression, exclusion, mass persecution, extremism and radicalization, bigotry, fanaticism, xenophobia, antisemitism, Islamophobia, and climate change denial, populism has come to reinforce the sense that the world confronts a new age of severe global crisis that threatens to spiral out of control and which no country or region on earth can hope to avoid.

After all, who could possibly argue that the poisonous mixture of populism and religious bigotry we see today on the streets of Lahore does not affect the feelings and security perceptions of the people walking peacefully through the streets of Amsterdam? And who among us can ignore the fact that the anti-Islamic discourses and exclusionary populist narratives expressed from the comfortable rostrums of splendid buildings in European capitals have no impact on the Egyptian youths who watch TV in their lounge rooms and are mobilized by feelings of hate and enmity? Against this backdrop, we can readily see that opposing extremisms fuel each other and create fertile ground for a vicious cycle of worsening extremism that threatens to engulf the planet. If we agree that the physical, offline world is a global village, it is no stretch to argue that the online world is a global town hall. And in this online global town hall, conspiracy theories, extreme emotions, and destructive discourses spread much faster than in the offline global village. So, the ECPS has decided to examine authoritarian religious populists and to research the dangerous nexus between faith and populism in cyberspace and, of course, its fatal effects in the offline world. I am sure that this report, as an impressive product of comprehensive research across five different Asian countries, will help us to understand the role of digital space in Asian
democracies, especially concerning religious populism. Being aware of the fact that the global rise of populism can lead to democratic decay, the spread of authoritarianism worldwide, and threats to global peace, security, and stability, I want to thank the scholars who have poured their efforts into preparing this report. I also sincerely hope that this report will fill a crucial gap in this research field and become a valuable resource for scholars and practitioners alike.

Dr. Bulent Kenes
ECPS Executive Director
Turkey, Pakistan, India, Malaysia, and Indonesia span one of the longest continuously inhabited regions of the world. Centuries of cultural infusion have ensured these societies are highly heterogeneous. As plural polities, they are ripe for the kind of freedoms that liberal democracy can guarantee. However, despite having multi-party electoral systems, these countries have recently moved toward populist authoritarianism. Populism — once considered a distinctively Latin American problem that only seldom reared its head in other parts of the world— has now found a home in almost every corner of the planet. Moreover, it has latched on to religion, which, as history reminds us, has an unparalleled power to mobilize crowds.

This report explores the unique nexus between faith and populism in our era and offers an insight into how cyberspace and offline politics have become highly intertwined to create a hyper-reality in which socio-political events are taking place. The report focuses, in particular, on the role of religious populism in digital space as a catalyst for undemocratic politics in the five Asian countries we have selected as our case studies.

The focus on the West Asian and South Asian cases is an opportunity to examine authoritarian religious populists in power, whereas the East Asian countries showcase powerful authoritarian religious populist forces outside parliament. This report compares internet governance in each of these countries under three categories: obstacles to access, limits on content, and violations of user rights. These are the digital toolkits that authorities use to govern digital space. Our case selection and research focus have allowed us to undertake a comparative analysis of different types of online restrictions in these countries that constrain space for opposition and democratic voices while simultaneously making room for authoritarian religious populist narratives to arise and flourish.

The report finds that surveillance, censorship, disinformation campaigns, internet shutdowns, and cyber-attacks—along with targeted arrests and violence spreading from digital space—are common features of digital authoritarianism. In each case, it is also found that religious populist forces co-opt political actors in their control of cyberspace. The situational analysis from five countries indicates that religion’s role in digital authoritarianism is quite evident, adding to the layer of nationalism. Most of the leaders in power use religious justifications for curbs on the internet. Religious leaders support these laws as a means to restrict “moral ills” such as blasphemy, pornography, and the like. This evident “religious populism” seems to be a major driver of policy changes that are limiting civil liberties in the name of “the people.” In the end, the reasons for restricting digital space are not purely religious but draw on religious themes with populist language in a mixed and hybrid fashion. Some common themes found in all the case studies shed light on the role of digital space in shaping politics and society offline and vice versa.
The key findings of our survey are as follows:

- The future of (especially) fragile democracies is highly intertwined with digital space.

- There is an undeniable nexus between faith and populism which offers an insight into how cyberspace and politics offline have become highly intertwined.

- Religion and politics have merged in these five countries to shape cyber governance.

- The cyber governance policies of populist rulers mirror their undemocratic, repressive, populist, and authoritarian policies offline. As a result, populist authoritarianism in the non-digital world has increasingly come to colonize cyberspace, and events online are more and more playing a role in shaping politics offline.

- “Morality” is a common theme used to justify the need for increasingly draconian digital laws and the active monopolization of cyberspace by government actors.

- Islamist and Hindutva trolls feel an unprecedented sense of cyber empowerment, hurling abuse without physically seeing the consequences or experiencing the emotional and psychological damage inflicted on their victims.
5. DEMOCRACIES IN TRANSITION

5.1 CYBER SPACE AND DEMOCRATIC CITIZENSHIP

Over 60 percent of the world's population has access to the internet, with some 4.66 billion active users in January 2021. While there is a global divide in access to the internet related to income disparities and unequal human development, the overall growth remains staggering. The largest share of the planet's internet users, nearly 52 percent, reside in Asia, with its dense population and steady increasing uptake of digital communication technology.

Moreover, the widespread availability of cell phone technology and the rapid development of the mobile internet has meant that digital platforms are a well-integrated part of daily life. In 2009, less than 1 percent of internet traffic was generated by mobile phones compared to 50 percent in 2020. Internet use is forecast to grow again in 2022 and beyond. It is, thus, not surprising that governments are keen to adopt digital technologies such as high-speed internet, smartphones, social media, and artificial intelligence (AI) as part of their governance strategies. As a result, political processes—including in the region's democracies—are becoming highly intertwined with digital space.

At the dawn of the internet age, the global community shared a sense of optimism about the prospects for a bright digital future. Indeed, the web was often spoken about as an agent for democratization. Cheap and ready access to the internet was hailed by scholars as an inherently democratizing development that would ensure the widest possible dissemination of information to the people. The internet was supposed to facilitate the creation and expression of ideas and political views by ordinary citizens in a media ecosystem dominated by powerful corporate or state-controlled television, radio, and print media. Indeed, many democratic theorists cast the world wide web as a virtual Habermasian “public sphere” promising a global “society engaged in critical public debate.” The online network society was expected to serve as a forum for the formation of public opinions, like the coffee houses of Vienna (in Habermas’ original theory), in which all citizens would have equal access to influence public debate. Several mass protests in the late 2000s and early 2010s that were mostly organized and facilitated by digital social media further boosted this techno-optimism in developing countries. The Arab Spring, in which Twitter featured prominently as a mobilizing tool, saw the fall of dictatorial regimes in Egypt, Libya, Tunisia, and Yemen.
5.2. Changing Democracies

This optimism over the increase in cyber activity and access to the internet came in the wake of the “third wave” of global democratization that began in the 1970s and peaked after the end of the Cold War. However, the first decades of the twenty-first century have witnessed a significant “democratic retrenchment” worldwide and the rise of an unprecedented wave of populist governments on virtually every continent. Unlike in the past, this new wave of populism has affected longstanding democracies once thought immune. For instance, America and India, the world’s two most populous democracies, have seen populist leaders rise within the democratic system. Moreover, despite unprecedented democratization since the mid-2000s, Pakistan and Turkey, countries with a history of military interventions, have chosen populist Islamist leaders.

Over the years, the populist wave has not only expanded but diversified as well. There are at least three broad categories of populism today. The most familiar is anti-establishment, where the “political elite” and other groups are demonized as part of the populist narrative. Socioeconomic populism is a center-left outlook featured in movements such as the Wall Street Protests and the leadership of political leaders such as Bernie Sanders in the US and Jeremy Corbyn in the UK. The last and most widespread category is cultural populism, which pictures elements within society and outside the country as “the enemy” of the “pure people.”

Along the spectrum of cultural pluralism, religious populism is prominent and has been championed by leaders around the world since the early 2000s. While most major religions of the world have been politicized by populist leaders and religious movements, there is distinctiveness in how they manifest. When Islam is politicized and deployed as Islamism by populist leaders, it manifests not only as a way to distinguish “the pious people” from “the corrupt secular elite” but also wields a religious symbolism and style wherein followers are encouraged to adopt explicit religious morals and “traditional” lifestyles in everyday life. These populists are nevertheless adept at leveraging technology and have been at the forefront of political messaging in digital space. As early as the 2000s, political parties in Muslim-majority countries were exhibiting a greater online presence compared to those in non-Muslim countries. Given that democracy is in a precarious state across the Muslim world, introducing draconian measures is not difficult for such governments, even on digital platforms.

In non-Western, non-Muslim-majority countries, identarian populism, another form of religious populism, has arisen. It uses religion to demarcate a civilizational division between “the people” and “the Other.” Arguably the most pernicious example here is India’s Bharatiya Janata Party (BJP). The party, led by Indian Prime Minister Narendra Modi, has long espoused a highly exclusivist and chauvinistic Hindutva politics, which declares Hindus to be “the true people” and non-Hindus by implication as “Other.” Despite its moralistic overtones, the BJP has shown little interest in moral
reform but still champions a Hindutva construction of society as the epitome of “civilization.” Consequently, in a world where democracy appears “in retreat,” the early digital optimism has given way among analysts and intellectuals to a kind of digital pessimism, or at the very least skepticism. While at one end, individual citizens can use social media and digital technology to stay informed and engage in online and offline activism, there is a growing concern that authoritarian (and democratic) governments can use digital tools to assert their control over this space. Extensive digital capabilities—especially AI and Big Data—are increasingly being utilized by governments to exert control over their citizens. Indeed, some observers are talking about the spread of full-blown digital authoritarianism — namely, “the use of digital information technology by authoritarian regimes to survey, repress, and manipulate domestic and foreign populations.” In response to the rise of digital activism, authoritarian regimes—not just populist ones—have been fast to catch up and adapt, launching their own digital countermeasures of repression. Governments have been observed employing advanced digital technologies to undermine democracy in various ways, including surveillance, censorship, disinformation, cyber-attacks and hacking, internet shutdowns, and targeted arrests. Against this backdrop, the present report contributes to our understanding of how emerging digital technologies affect, enable and undermine democracy, human rights, freedom, and the electoral process.

While scholarship on the topic is in its infancy, the focus has generally been on Western democracies. Despite the scale of internet usage in Asia, this part of the world—and the Global South more generally—has been largely excluded from such studies. Thus, studies focusing on non-Western countries that have witnessed democratic backsliding under the rule or influence of authoritarian religious populists are sorely needed. In all the cases analyzed in the present report, digital platforms have been used intensely by governments and dissidents and can reveal much about the contested role of digital technology and the future of democracy.

5.3. The Digital Authoritarian Toolkit

States implement multi-layered and complex measures to manipulate the use of and access to cyberspace by people residing in their territory and to restrict online freedoms. The key measures in the toolkit of digital authoritarianism are:

Censorship includes “restrictions on what information can be publicized or viewed on the Internet.” Examples of internet censorship are blocking undesirable content, apps, and social media, and passing laws that allow the removal of certain forms of content. Some countries have created so-called “sovereign internets,” facilitated by technology. Think of the “Great Firewall” of China and Russia’s Roskomnadzor, which enforces data localization, and Iran’s National Information Network (also called the Halal Internet).

Disinformation campaigns involve
the spread of large volumes of false content by state-owned and regime-friendly media against the opposition. This can include social media manipulation through “cyber warriors” using bots and cyber-trolls. Examples include Iran’s so-called “cyber battalions” linked to the Iranian Revolutionary Guard (IRG). Disinformation campaigns also involve the manipulation of elections, including voter engineering and influencing voter behaviors and outcomes by micro-targeting propaganda and individualized campaigns using AI and Big Data capabilities. The creation of “filter bubbles” and “echo chambers” in elections can also undermine meaningful exchanges of ideas in electoral debates.

Cyber-attacks and hacking. Cyber-attacks include any “attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber-attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.” Such attacks often target opposition groups’ data centers, networks, social media accounts, and computer systems to undermine their public image and spy on their campaigns. There are reports that the Iranian government has been proactively gathering intelligence on Iran’s opposition by hacking applications, even secure ones like Telegram, which uses sophisticated symmetric encryption.

Internet shutdowns. “An Internet shutdown is an intentional disruption of Internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information.” Short of complete shutdowns, governments can disrupt the internet and other electronic communications through rolling blackouts or selected blocking/filtering of the internet and social media.

Targeted arrests and violence occur when “a large group of abusers collectively attacks a target through a barrage of threats, slurs, insults, and other abusive tactics.” There are many reports of influential digital activists and actors being physically assaulted, arrested, and sentenced to jail.

Surveillance. In the digital realm, this usually takes the form of software that is specifically “marketed for or that can be used (with or without the authorization of the business) to detect, monitor, intercept, collect, exploit, interpret, preserve, protect, transmit, and/or retain sensitive data, identifying information, or communications concerning individuals or groups.” Today, this includes facial recognition technology (FRT), video surveillance, and so-called smart policing, monitoring communications and social media, tapping mobile phones, monitoring locations, using spyware, intercepting networks, biometric identification, and text/data mining.

5.4. Conceptual Framework

There are several frameworks for monitoring and measuring restrictions on freedom on the internet. One of the earliest frameworks to investigate and analyze internet filtering and surveillance practices was developed
by The OpenNet Initiative (ONI). Initially, the ONI focused on measuring internet filtering under four main categories: pervasive filtering, substantial filtering, selective filtering, and suspected filtering. Further elaborating the index, ONI distinguished filtering based on its locus—namely, whether blocking is conducted centrally and infrastructurally (at the level of the underlying internet architecture) or decentralized (at the level of ISPs). In their later work, ONI researchers studied how governments “shape, limit, and control the Internet.” Unlike the first-generation controls, which often focused on denial of access, the second generation utilized a repertoire of manipulation techniques to normalize and legalize control. These techniques included “distributed denial-of-service (DDoS) attacks, targeted malware, surveillance at key points of the Internet’s infrastructure, take-down notices, and stringent terms-of-usage policies.”

A more detailed categorization, which is partly based on previous work by ONI, is used by Freedom House in its annual Freedom on the Net reports. Here, three areas are covered: obstacles to access, limits on content, and violations of user rights. The current report follows Freedom House’s framework, which offers a comprehensive conceptual apparatus to investigate modern manipulations of the internet. The table in the Appendix provides a brief explanation of each category of violations of internet freedom based on the Freedom on the Net 2021 report.

5.4.1. Obstacles to Access

Governments can erect several types of obstacles to restrict access to the internet or the speed and quality of internet connections. This includes making the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons. Governments can also exercise technical or legal control over internet infrastructure to restrict connectivity or impose legal, regulatory, or economic obstacles that restrict the diversity of service providers. Finally, national regulatory bodies can impose controls on service providers such that digital technology fails to operate in a free, fair, and independent manner.

5.4.2. Limits on Content

The state can block or filter internet content—or compel service providers to do so. As well, state or non-state actors often employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content. Often, restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process. Limits can also be self-imposed, such as when online journalists, commentators, and ordinary users practice self-censorship. There are also examples where online sources of information are controlled or manipulated by the government or other powerful actors to advance a particular political interest or where economic, regulatory, or other constraints exist that negatively
affect users’ ability to publish content online. Finally, the online information landscape may lack diversity and reliability such that conditions impede users’ ability to mobilize, form communities, and campaign, particularly on political and social issues.

5.4.3. Violations of User Rights

The constitution or other laws of a country may fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and may be enforced by a judiciary that lacks independence. Violations also occur when laws exist that assign criminal penalties or civil liability for online activities, particularly those protected under international human rights standards. In some countries, individuals are penalized for online activities, or the government restricts anonymous communication or encryption. Another concern is state surveillance of internet activities, which infringes on users’ right to privacy, and the monitoring and collection of user data by service providers and other technology companies, which also infringe the right to privacy. In serious cases, individuals are subject to extralegal intimidation or physical violence by state authorities or other actors concerning their online activities. Finally, the websites of government and private entities, service providers, or individual users may be subject to widespread hacking and other forms of cyberattack.
6. Applying the Toolkit:
Case Studies

6.1. India

India’s current prime minister and leader of the BJP, Narendra Damodardas Modi, worked at a tea stall in his childhood and rose to become the leader of one of the world’s largest democracies. His first taste of politics came during his meteoric rise within the Rashtriya Swayamsevak Sangh (RSS), a right-wing Hindutva social movement linked to the BJP. In launching his election campaign in 2013, Modi emphasized social mobility and progress for a “new India.” An end to corruption, dynastic politics, and socioeconomic gulfs seemed tantalizingly close when he was elected as prime minister in 2014. However, after nearly two consecutive terms, Modi’s promised “new India” has yet to materialize, while there has seen a drastic decline in democratic freedoms, mainly due to right-wing policies. According to the Freedom House Index, freedom for Indian citizens declined for a third straight year in 2020–21. With a ranking of 67, India has been downgraded from “Free” to “Partly Free” status. Ripples of deteriorating democracy are also felt in cyberspace. Nearly 58 percent of India’s population has access to the internet, and this is rising fast. The total number of internet users in India rose from 795.18 million at the end of December 2020 to 825.3 million at the end of March 2021. As the following discussion shows, despite widespread internet access and India’s positive track record of democracy, today internet freedom in India is severely compromised.
6.1.1. Obstacles to Access

In 2014, Modi declared, “I dream of a Digital India where access to information knows no barriers,” a far cry from where the country stands today. During its second term (2019—present), the BJP government has increasingly resorted to full internet shutdowns. The most prominent example was the full shutdown in the Jammu and Kashmir state in 2019. The only Muslim-majority state in India before its autonomy was taken away that same year, Jammu and Kashmir’s internet was totally blocked for almost five months. Even when restored, only 2G or 3G service was available in most places, making the opening only partial. The 4G internet service was only available after more than a year. Another service block in 2019 came during the protests against India’s Citizenship Amendment Act (2019), which was widely seen as targeting Muslims. Largely organized by civil society concerned over the discriminatory nature of the law, the protests soon spread all over India. Lasting well into 2020, many parts of the country saw massive internet shutdowns at the peak of the protests. As Figure 1 shows, India has recently had the largest number of internet shutdowns globally. Inspired by the federal government, the state authorities in India have also started using network curbs. In October 2021, in the state of Rajasthan, the districts of Jaipur, Bikaner, and Dhausa closed mobile network services and cell phone access to curb cheating in regional examinations. The country lost $2.8 billion in 2020 due to internet shutdowns.

6.1.2. Limits on Content

The Indian government frequently uses Section 69A of the IT Act 2000 to block websites. The 2009 blocking rules published by the Indian government are themselves vague and allow the government to withhold information on which sites are actually being blocked. There has also been a marked increase in the number of blocked websites. Some 633 websites were banned in 2016, rising to 9,849 in 2020. Investigative journalists have revealed that most blocked websites belong to human rights groups, separatist movements, feminist platforms, NGOs, and even sites linked to United Nations agencies. The government justifies most blocks on the grounds of “national security.” The year 2020 was quite testing for India. In addition to the burden of COVID-19 and the continued economic downturn and massive unemployment, there was the Indo-China border clash, all of which presented the BJP government with a range of social and political issues to
The government responded by cracking down in cyberspace. Between January and October 2020 alone, India blocked 100 websites, 1,364 online domains, and 157 Internet Protocol (IP) addresses. Due to the extensive blockade of content, the use of Virtual Private Network (VPN) has surged. Only 3.28 percent of Indian internet users used a VPN in 2020. In the first two quarters of 2021, 25.27 percent of users used one. In October 2021, the Parliamentary Standing Committee on Home Affairs recommended that the government ban VPNs in India. No action has been taken as yet.

India has one of the largest number of Facebook users globally, the third-largest Twitter population, and is the world’s largest market for WhatsApp. Under the government’s 2021 information technology rules, issued under the IT Act 2000, social media platforms are required to remove content identified as “illegal” by the government within three days, provide access to user information for law enforcement officials. The rules also extend the data retention period to 180 days and increase the penalties for non-compliance for the global platforms, putting end-to-end encryption in India at risk. These rules have been presented as necessary to protect individuals’ privacy, stop terrorism, riots, and breakdowns of law and order. Yet, the regulations give the government greater control over social media.

Since the law came into effect, firms have been obliged to share a monthly report with the government. These briefs showcase the amount of content removed. The first three months of published data revealed that Facebook, Google, WhatsApp, and others removed a staggering 110.88 million posts. While content that is sexual or graphic in nature makes up a hefty chunk of the requested take-downs, there is also the question of what constitutes “terrorism” and “hate speech,” which the government frequently requests be removed from social media sites. Despite the tradition of rule of law in India, mob lynching of minorities triggered by misinformation via social media continues as well.

When India was struck by the Delta variant of COVID-19 in 2021, posts on social media that were critical of Prime Minister Modi’s handling of the virus were removed from these platforms because of the pressure from the government. Deemed “false statements,” these were posts from opposition leaders and concerned citizens over the mishandling of the COVID-19 crisis.

Online streaming services have yet to face legal reproach by the BJP government, yet the government has supported the RSS (and the broader Sangh Parivar Hindu nationalist movement, of which it is a part) in their protests against these services. The group targeted Netflix and Amazon Prime for offending Hindu religious sensibilities. The government has also done little to prevent harassment of producers and movie stars by Sangh Parivar attackers, who have bullied them in person and online.

6.1.3. Violations of User Rights

Digital surveillance measures ranging from targeted to mass surveillance have been normalized in India. Events such as the Mumbai
attacks of 2008 have justified these measures as necessary for “security.” Thus, the Central Monitoring System (CMS), an ambitious surveillance system that monitors text messages, social media engagement, and phone calls on landlines and cell phones, among other communications, was launched after 2008. Under the law, citizens targeted by it are not obliged to be informed whether their data has been intercepted. There are reports that the CMS has become a mass surveillance tool by the state without valid legal and constitutional authority. In addition, Indian police in several states have routinized the use of fingerprinting and FRT to stop and screen people on flimsy pretexts, turning vital public spaces into privacy-violating zones. The CMS and the FRT have frequently been used to profile and target protesters. These tools have been extensively used in the conflict-ridden zone of Jammu and Kashmir and for profiling people based on race, religion, and profession (among other factors) without legal permission.

Under such close monitoring, it is not surprising that journalists and social media activists continue to be arrested under terror or treason charges. Independent right-wing organizations, such as those of the Sangh Parivar, use these laws to file reports regularly against those opposing the government online. Legally speaking, right-wing factions act as “partisan supporters” reporting these incidents. Since 2016, India’s rank on the World Press Freedom Index has slid from 133 to 142 in 2021. Moreover, India is seen as one of the most dangerous countries for journalists trying to do their job.

Along with the CMS, India has been using other ways to snoop and surveil its citizens. In July 2021, India was also caught up in the Pegasus spyware scandal. Pegasus is Israeli software that has purportedly been used to spy on terrorists and marketed exclusively to governments. However, like many other governments worldwide, the Modi government has bought this spyware and secretly used it to spy on anyone considered a political threat. The Supreme Court of India has ordered an inquiry into the matter as of October 2021.
6.2. Indonesia

Indonesia’s recent surge in attacks on minority religions has been instigated mainly by right-wing Islamist movements who have enjoyed much greater freedom after the sudden collapse of the New Order regime in 1998. After a period of democratic flourishing in the 2000s, Indonesia has recently been in a steady state of democratic decline, as highlighted by its 2017–2021 scores by Freedom House. Further complicating the matter, President Joko Widodo (Jokowi) has deliberately side-lined democratic norms in the interests of building a modern economy, which he and his supporters contend is a prerequisite for the future consolidation of democracy. The government’s reduced tolerance of criticism and discriminatory regulations against minorities has been an unfortunate consequence. Combined, both elements have led to increased abuses of religious freedom. Interestingly, Indonesia’s level of discrimination against religious and social minorities has seemingly remained unchanged since 1998. There are also signs of an increased Islamization with a rise in the visibility of Islamic gatherings, modest clothing, Muslim-only residential compounds, and Shariah-compliant banks. Given shrinking public space, minorities have resorted to going online. Social movements such as those supporting LGBTQ+ or women’s rights have sought refuge on cyber platforms. While online communities enable like-minded individuals to interact, there are still limitations as the Indonesian government censored, regulated, and controlled the internet. Though Indonesia’s internet governance laws (see Table 1.0 in the Appendix) have been described to be well-intended, censorship regulations have created controversies. This highlights the presence of a specific moral compass being used by the government imposed on its citizens. Additionally, their loose definitional parameters also facilitate their instrumentalization by the government.

6.2.1. Obstacles to Access

The Indonesian government has resorted to internet shutdowns to
manage riots. In 2019 alone, there were three reported cases: one protesting the 2019 presidential election results, a successionist riot in Papua in reaction to the arrest and racist treatment of Papuan students in East Java, and a second similar riot in Papua triggered by racism toward Papuan students in Wamena. Of the three riots, the internet shutdown was the longest in the second riot spanning a two-week period from August 21 to September 4. While the Jakarta State Administrative Court ruled that the internet shutdowns in Papua and West Papua in 2019 violated the law, the Constitutional Court ruled otherwise on October 27, 2021. In April 2021, internet access in West Papua was disrupted on three separate occasions coinciding with events related to Papuan successionist movements. These coincidental disruptions were blamed on a damaged sea cable in the area.

### 6.2.2. Limits on Content

Indonesia continued its tactic of banning websites deemed inappropriate, including those that purportedly promote religious extremism, pornography, entertainment streaming websites, and websites promoting content piracy. This practice of selective blocking started in 2008 when the government attempted to prevent its citizens from accessing an anti-Islamic film, Fitna. In 2018 alone, nearly 3,000 websites disseminating extremist ideologies were blocked, and about 9,500 other sites were under review. Based on Google’s recent “Content Removal Transparency Report,” Indonesia submitted the largest amount of requests from January to June 2021 on all of Google’s platforms, including YouTube, Google Search, and Blogger. While the Ministry of Communication and Information Technology is responsible for blocking sites found inappropriate, ministry officials do not assess the sites requested for review. Instead, agencies like the National Counter Terrorism Agency (BNPT) are responsible for the assessments. One potential issue is how such assessments are made and what happens when agencies disagree. Additionally, repeated blocking of popular websites has driven Indonesians to become au fait with countermeasures such as VPNs. In 2019, Indonesia had the most extensive VPN usage in the world. In addition to website blocking, the government banned homosexual emojis in 2016, citing its potential for public unrest.

Indonesia recently passed an internet bill that mandates online service providers to remove or block content on their platforms when requested by the government. According to Ministerial Regulation 5/2020, the law is essential to address disinformation and the destabilizing effects of “fake news.” Under the new rules, service providers must also register with the government by the
end of 2022 to obtain the licenses required to operate. This is not the government’s first attempt. Indonesia threatened to ban Blackberry (a handset maker) in 2011 and Telegram (a messaging service) in 2017 on security grounds. These mandatory registrations and the threat that licenses will be withdrawn enable the government to exert control over multinational companies such as Facebook, YouTube, and Netflix. In complying with Ministerial Regulation 5/2020, these companies are required to ensure that their platforms do not contain or facilitate the distribution of prohibited content. Unfortunately, as with other censorship laws, defining what is prohibited is problematic due to its broad definition.

6.2.3. Violations of User Rights

One of Indonesia’s cyber laws, known as UU ITE, severely threatens civil liberties. This law, passed in 2008, has been used more frequently by Jokowi’s administration than previous administrations in response to the growing polarization on social media and to counter accusations against it such as corruption and misconduct. In November 2020, it was reported that since 2016, more than 300 criminal cases had been brought under UU ITE. The key issue with the law is its broad definitions. Though its stated purpose is to safeguard the populace against immorality through its criminalization under Article 27(1) of UU ITE, what is deemed immoral is not clearly defined, leaving it open to manipulation. Similarly, in this article and Article 27(3), “transmission” of immoral content is open to interpretation, thus, enabling even private consensual sharing of “immoral” content to be considered an offense. Not only has the government leveraged UU ITE, but also the police, government officials, and business people who form the three largest cohorts to make use of the legislation to pursue their interests.

In Indonesia, cyber harassment is a common way to target “the Other.” The weak legal framework for combating cyberbullying emboldens trolls such as the Muslim Cyber Army, which has a history of harassment and intimidation of individuals deemed to have insulted Islam. Numerous members of this group who go by a multitude of aliases were arrested for crimes such as spreading false reports and inciting racial and religious discrimination. In such an atmosphere, LGBTQ+, non-Muslims, Ahmadis, and other marginalized groups commonly self-censor.
6.3. Malaysia

For six decades under the UMNO-led Barisan Nasional ruling coalition, Malaysia functioned as a hybrid regime. In 2018, the Pakatan Harapan (PH) coalition defeated Barisan Nasional in the general elections, and for the first time, Malaysia experienced a peaceful transition in government. The contested Anti-Fake News Act in December 2019 was also repealed as part of the reform promised by the new government. Unfortunately, the PH experiment lasted for a mere 22 months before a soft coup by the Malay Muslim establishment. Since then, Malaysia has dropped in the rankings on various measures of democratic freedoms. The overly broad, colonial-era Sedition Act remains in place. The change in government and the COVID-19 pandemic actively prevented private media from covering events. However, Malaysians enjoy greater freedom online than they do offline. It is also worth noting that despite the 2020 soft coup, the Perikatan Nasional government has maintained a relatively open space for dissent online.

Returning to the prime ministership in 2018, Dr. Mahathir Mohamad—introducing his new agenda—promised no internet censorship under Section 3(3) of the Communications and Multimedia Act 1998 (hereafter the CMA). However, over the years, there has been an increase in laws that govern cyberspace (see Table 1.0 in Appendix for detailed laws).

6.3.1. Obstacles to Access

The Malaysian government has yet to completely shut down the internet. The closest the government was accused of affecting the entire network was in 2012 when mobile phone usage was disrupted during a rally. Officially slow internet speed was blamed for the disruption. Another reason given in 2016 was that the government was more focused on providing greater coverage across the country than on increasing the internet speed. In general, Malaysia
suffers from a relatively low mobile internet speed, which was 31.34 Mbps on average in September 2021 (the global average was 63.15 Mbps). Slow internet connections were exacerbated during the lockdown period in 2020 and 2021 as more people went online. The government remains committed to improving this by introducing 5G technology in Malaysia in 2023.

6.3.2. Limits on Content

The Malaysian government has actively blocked thousands of web pages that fit the definition of the “offensive” contained in the CMA Act 1998. As of April 2021, 18 websites were confirmed blocked in the country, whereas many others face anomalies, ranging from pornography to websites that criticized Islam. From 2018 until 2020, 2,921 pornographic websites were blocked, while 4,277 pornographic websites were blocked from 2015 until 2016. Most of the banned websites included terrorist-backed platforms, gambling sites, and the like, which infringe the Muslim ethos of the country. The Malaysian Communications and Multimedia Commission (MCMC) blocks websites when it receives complaints and applications from government ministries and agencies. This means that the MCMC may abuse its power against the opposition. For example, during the general election in 2018, the MCMC ordered 11 internet service providers to block three websites of Malaysiakini, a popular online news portal known for its neutrality (and thus not being a proxy for the government), on live updates of the election results for fear it could affect “national stability, public order and harmony, and economic stability.” Compared to the other case studies, the Malaysian government has been less restrictive toward social media companies. In 2018, 97.3 percent of internet users owned a Facebook account, making it the most popular social networking site, whereas 98.1 percent of users preferred WhatsApp as a communication channel. At the same time, the MCMC had requested social media platforms such as Facebook, Twitter, and YouTube to take down content violating local social and cultural norms. For Twitter, 275 legal demands were made to remove or withhold content from 2012 until 2020. Interestingly, out of the total, 153 requests, or 55.6 percent, were made from July through to December 2020, a huge spike compared to previous years. The same trend is observed with Facebook posts with 376 items of content restricted between January and June 2020, more than double the previous count at 163 from July until December 2019. The pandemic has provided an opportunity for the government to clamp down on critics under the guise of combating fake news. This is done through the Emergency (Essential Powers) (No.2) Ordinance 2021, which was enforced throughout the Emergency Ordinance period from January until July 2021.

The government has also prosecuted online news portals. The latest major case would be the Federal Court’s finding in February 2021 that the online news portal Malaysiakini is liable for contempt of court over five readers’ comments that the court alleged “clearly meant that the judiciary committed wrongdoings,
is involved in corruption, does not uphold justice and compromised its integrity.” This goes beyond proxies to individual users as well. The 2012 amendment to the Evidence Act 1950 enables enforcement of Section 114A against social media organizations, online forums, news webpages, or even public places that provide wifi, all of which may be liable to legal action from an online user’s action. Although Malaysiakini was fined an exorbitant RM500,000—beyond the RM200,000 sought by the prosecution—they were able to crowdsource the fund within a few hours after the judgment.

6.3.3. Violations of User Rights

Prosecution and harassment of users are the most common methods for the Malaysian government to control the internet. In 2020, six journalists from Al Jazeera were investigated for alleged sedition, defamation, and transmitting offensive for airing a critical documentary. Al Jazeera’s staff were faced with abuse and death threats for allegedly sullying Malaysia’s image. Similarly, a Bangladeshi national, Mohamad Rayhan Kabir, was arrested and later deported for criticizing the government’s treatment of undocumented migrants in an interview. Individuals are commonly charged and prosecuted under Section 233 of the CMA 1998 or the Sedition Act 1948. Fahmi Reza, a well-known graphic designer, has been investigated at least nine times by the police for his satirical artworks criticizing the government. Even a 17-year-old, Ain Husniza Saiful Nizam, who exposed a male teacher on TikTok for allegedly making a rape joke in class, was served with a defamation suit and called on by the police to make a statement apologizing for “breaching the peace.” Ain also faced cyberbullying. During the pandemic, civil servants were barred from sharing online comments critical of the government.

In 2020, the Department of Community Communication (J-KOM) was awarded a budget of RM40 million. The opposition accuses J-KOM of being the government’s propaganda machine and of funding “cyber troopers” who are paid to create positive content for the government and ruthlessly criticize the opposition. It is also true that bots flood social media, spread disinformation, and engender further social polarization at the behest of the state. In this environment, self-censorship is common in Malaysia. To make matters worse, the MCMC released a statement in January 2021 reminding internet users not to post anything offensive involving the “3Rs”: royalty, religion, or race.
6.4. Pakistan

The decolonization of British India in 1947 and its subsequent division into two countries, India and Pakistan, was a highly traumatic event that took millions of lives. In the over seven decades since, Pakistan’s politics has been very turbulent, with long periods of military-led dictatorships and hybrid regimes interspersed with a few short periods of democracy. The 2018 general elections brought a new party to power, but the military remains the most potent political force, and while this remains the case, the prospects of true democratization in Pakistan remain thin. After more than three years in power, Imran Khan’s Pakistan Tehreek-e-Insaf (PTI) government has largely failed, and misgovernance and corruption have increased. In a populist fashion, the last three years have seen increased curbs both in and out of cyberspace by the government as it seeks to consolidate its position in office. The digital footprint of Pakistani citizens has drastically increased in the last decade, with cheap cellular and internet packages becoming available. According to the Pakistan Telecommunication Authority (PTA), 98 percent of households own a mobile phone. In addition, there was a 17 percent growth in internet usage in just one year, with 90.1 million users recorded in October 2020. Despite this development, the future of internet freedoms, and freedom overall, is bleak in Pakistan due to the ever-increasing rules that control cyberspace. Unsurprisingly, the military establishment, backing the PTI government, has warned the public about “internal enemies” carrying out “fifth-generation warfare” online to justify the curbs.

6.4.1. Obstacles to Access

Pakistan has a high rate of internet outages. Blackouts on social media and the internet are not uncommon in Pakistan. Since 2005, the state has used blackouts to restrict information from the public. There are three types of shutdowns. First, there are regular internet shutdowns on specific dates, primarily religious and national holidays, as the government argues that there is a greater likelihood of
terrorism on these occasions. Second, there are regional shutdowns in areas where there is insurgency or threat of insurgency, such as border areas close to Afghanistan (merged districts, formally known as the Federally Administered Tribal Areas) and areas in Balochistan. Finally, there are local internet shutdowns, usually for a few hours when the government perceives a threat of terrorism or communal violence. Such shutdowns usually happen at times of protest. In 2012 alone, an estimated 507 million Pakistani rupees ($49 million) were lost due to internet outages during Eid (a religious festival), and another 500 million rupees were lost during curbs designed to discourage Ashura processions, a Shia religious practice. Despite these mammoth losses, such blackouts are justified as necessary for “security.”

Long-term shutdowns are usually disciplinary mechanisms. Areas experiencing extended shutdowns are usually the ones where those that the state treats as “Other” tend to reside. Nevertheless, the latest annual report from the PTA has no information about the internet shutdowns.

6.4.2. Limits on Content

The censorship of websites is one of PTA’s key activities. A hefty chunk of the blocked content is done so based on “indecency” such as pornographic websites and content that threatens Islam or the state. The exact number of websites blocked is unclear as PTA reports give contradictory numbers. They vary between 824,000 URLs to 418,139 URLs. This banning trend has escalated in the last four to five years.

In August 2021, the Ministry of Information and Broadcasting published a report called “Anti-State Trends,” which highlighted websites and trends from June 2019 to August 2021 it considered “anti-state.” The report accused separatist movements, political opposition, critical Tweets, and India of colluding with separatists in waging a “fifth-generation warfare” against Pakistan. In reality, these movements are less “anti-state” and more critical of the present government. There are trends of blocking the websites lending support to these factions.

PTA is armed with legislation to ban the operations and content of intermediaries such as YouTube, Facebook, Twitter, WhatsApp, and many more. It usually forces these companies to remove materials and restrict their content based on local laws and sensibilities. If these requests are denied, then the operations of these companies can be blocked.

One of the most famous episodes of this kind of censorship was when YouTube was banned in Pakistan in September 2012 after refusing to take down a crude anti-Islam inflammatory movie, “Innocence of Muslims.” The ban continued for more than three years. During this time, the National Assembly passed a non-binding but unanimous resolution to lift the ban, and courts also ordered negotiations, but the ban was not lifted till 2016. More recently, TikTok has been a target of repeated bans because of its potential to “corrupt” and “misguide” the youth due to its dance
dub mashes, pro-LGBTQ+ content, etc. In addition, it has become a routine matter to suspend messaging applications on social media during times of protests or huge processions. The big social media intermediaries, such as Facebook and Twitter, are not completely banned nowadays, but they continue to be banned for very short periods as a “security measure.” For instance, in April 2021, a major social media blockage was put in place when the militant religious organization Tehreek-e-Labaik Pakistan (TLP) carried out protests in Punjab.

On the pretext of stopping fake news and criminal activity, the PTI government enforced the Rules for Removal of Unlawful Online Content in 2020. This highly problematic regulation compelled the Asia Internet Coalition to write an open letter to Prime Minister Imran Khan to condemn the measure and its consequences. These regulations demand that big tech firms open a local office in Pakistan, mandate storing Pakistani users’ data within the country and oblige companies to remove content when ordered. The near future will indicate the degree to which this law has been instrumentalized.

6.4.3. Violations of User Rights

Over the years, Pakistan has earned the title of a “surveillance state.” The “war on terror” alliance with the United States allowed Pakistan to enhance its surveillance capabilities with modern standards. As a result, a mass surveillance network has been built in Pakistan since 2005, with the government obtaining technology from both local and foreign surveillance companies, such as Alcatel, Ericsson, Huawei, SS8, and Utimaco, to use against its citizens. Pakistan’s religious and ethnic minorities, journalists, human rights activists, and feminists, among others, now suffer at the hands of this well-designed apparatus. Through content monitoring and interception, social media have led to cases of enforced disappearances and harassment of journalists and human rights activists who have used platforms, such as Twitter or YouTube, to challenge state narratives and criticize the state. In addition to the “establishment” (i.e., the nexus of politicians and the military), the PTI’s online followers are known for harassing anyone from opposition leaders to journalists critical of PTI facing cyberbullying at their hand. These insults are highly derogatory, and chauvinistic sexism is rampantly used to target women victims. In addition, those who oppose the army, take a positive stance vis-à-vis India or show “liberal” tendencies also encounter similar hostility in online space. Despite the explicit abuse, to date, there are no records of actions taken to curb this bullying under cybercrime laws.
A glimmer of hope was visible for democracy in the 2000s when the Justice and Development Party (AKP) defied the odds by defeating the Kemalist hegemony in Turkish politics. With peace-building processes to reconcile with historically marginalized communities, reforms to improve human rights, and a commitment to join the European Union (EU), the odds of democratization seemed promising when the AKP came to power.

However, after 2010, the AKP has taken an increasingly authoritarian path. The narrative of the ruling government instils fear and insecurity to legitimize growing authoritarianism. These changes that increasingly curb dissent, criticism, and muffle debate are present both on and offline. Since 2016, 150,348 individuals have been dismissed from office, with 500,650 being criminally investigated, with 96,885 arrested, while 3,003 educational institutions and facilities closed, 6,021 academics have been driven out of their jobs, 4,463 legal professionals such as judges and prosecutors have been terminated, 319 journalists arrested, and 189 media outlets completely closed. In addition to massive crackdowns, it is common for the state to use military custody, and various people have been arbitrarily arrested and tortured, both inside and outside the country, without reasonable evidence in many cases. By 2020, cyberspace had become an essential space of resistance in Turkey. Between 78 and 82.6 percent of the total population uses the internet. In addition, some 54 million people, 64 percent of the total population, use various forms of social media, with the average time spent on the internet per day averaging 7 hours and 57 minutes in 2021. Turkey’s digital realm is thus a highly contested political space. It is, thus, not surprising that the
digital realm has been meticulously regulated and increasingly surveilled by the AKP government through various measures.

6.5.1. Obstacles to Access

The Gezi protests in 2013 marked the beginning of internet closures to curb the ability of civil society and activists to organize in Turkey.

The aftermath led then Prime Minister (now President) Erdoğan to label Twitter the “worst menace to society.” What followed was a marked increase in internet governance. Internet blackouts are one of the many ways of controlling the space, and the newly formed Telecommunication Technologies Authority (BTK) looks over these procedures. While the government insisted that internet curbs are in place to combat “terrorism,” there was also a political motivation behind some of these. The Turkish government’s internet shutdowns peaked between 2015 and 2017. The eastern regions faced the major brunt of internet and cellular shutdown during this period. During high-risk security incidents, such as the 2015 Suruç suicide bombing and the 2016 Atatürk Airport bombing, localized internet and cell phone blocks were put in place. With the government’s growing authoritarian approach, digital anti-terrorism laws are increasingly used to persecute marginalized groups such as the Kurds. Most shutdowns have occurred in the southeast, where Kurdish resistance is firmly grounded. One example was the 2016 landline and internet closure in 11 cities in the region with 6 million citizens devoid of access following the arrests of the mayor and co-mayor of Diyarbakir, which led to protests. Additionally, these internet shutdowns cost millions of dollars to the Turkish economy. Even though internet shutdowns have decreased from six in 2016 to only one in 2020, the cost is still high, at US$51 million in 2020.

6.5.2. Limits on Content

The political climate in Turkey has given birth to many “threats” manufactured by the AKP government, such as “FETOısts” following 2016, demonizing youth activism during Istanbul’s Bogazici University events of 2021 or the Gezi protests along with pre-existing hostilities toward minorities.

Human rights organisations have reported that the right to privacy online and offline in Turkey has been increasingly under threat. In April 2014, Turkey passed a new law that expanded the surveillance powers of the National Intelligence Agency (MIT) that was given sweeping powers to amass private data, documents, and personal information in all forms without a court order. Working in tandem, the BTK and the National Intelligence Agency (MIT) have targeted pornographic websites, weblinks belonging to armed groups such as the Kurdistan Workers’ Party (PKK) and the Islamic State of Iraq and the Levant (ISIL) and since 2016 have targeted sympathizers of the Gülen movement, and LGBTQ+ and pro-Kurdish voices.

In addition to the lack of transparency, since the website owners do not always receive clear reasons for blocks, they cannot appeal
the decision. Without accountability, mere suspicion and precaution are considered sufficient reasons to block a website. From just four websites being blocked in 2006, the number jumped up to 1,014 in 2008 when Law No. 5651 was initially introduced, a dramatic annual rise was visible in 2013, 2014, and 2015 with respective annual blocks of 19,715, 36,287, 27,812, which coincided with the Gezi protests, the corruption exposés and a wave of terrorism in Turkey. From 113,137 websites blocked in October 2016, the number more than doubled in three years to 288,310 in December 2019. Similarly, 450,000 domains, 140,000 URLs, and 42,000 Tweets have been banned in Turkey during 2020. While this pace of blockage has slowed down, the laws in place still play a key role in regular surveillance of websites that are taken down in thousands on an annual basis. Even information platforms such as Wikipedia faced a ban in Turkey when Ankara’s 1st Criminal Court found that certain articles linked Turkey to “terrorist organizations.” The court demanded that relevant articles be edited before the website could function again in Turkey. The ban was lifted in 2020. Social media intermediaries in Turkey have faced various types of restrictions. It was reported that YouTube, Twitter, and Facebook were all temporarily blocked or throttled in 2016 until they agreed to remove “objectionable” content. Even as early as 2014, the Telecommunications Directorate (TİB) was mobilized to urge Twitter, YouTube, and Facebook to remove critical information that was impacting the AKP’s chances in the future local elections. While Facebook was quick to comply, Twitter and YouTube were blocked nationally for several hours before they eventually complied. Twitter’s 2019 Transparency Report revealed that in the first half of the year, the Turkish government made 350 information requests on 596 accounts as well as 6,073 removal requests on 8,993 accounts with a 5 percent compliance rate. Turkey had the highest number of legal demands for removals. Facebook’s 2019 Transparency Report also reveals that the government made 2,060 legal requests and 2,537 user information requests; Facebook was compliant with 73 percent of requests.

In addition to social media, the search engine Google has since complied with the thousands of content removal requests by the Turkish state, which peaked in 2016. The government has further cemented its hold on these entities by allowing them incentives to open data centers in Turkey that are obliged to follow Turkish laws under Decree-Law No. 678. Moreover, over-the-top media services (OTTs), such as Netflix, PuhuTV, and BluTV, are now regulated by BTK, and the Radio and Television Supreme Council (RTÜK) issues mandatory licenses to OTTs before they can stream content in the country. In October 2020, Law No. 7253 with harsher requirements for social media companies was introduced. The impact of this new law is still to be seen.

6.5.3. Violations of User Rights

While keeping pressure on social media, the Turkish government has also kept the prosecuting individuals for their internet activity open. Particularly after the 2016 coup
attempt, many people faced the government's wrath. Six months after the coup, the Ministry of Interior stated that more than 10,000 individuals were investigated, 3,710 faced some legal action, and 1,656 people were arrested for their online activity. More recently, in the two months between mid-January and mid-March 2018, 6,342 social media accounts were investigated, and 2,177 individuals were subjected to legal action. Another report states that, between 2013 and 2018, there were more than 20,000 cases against citizens because of their social media activity. They are sometimes indicted under “terrorism” under Article 314(2) on association with an armed organization and Article 147(5), which concern crimes associated with terrorist organizations and aims.

Essentially limiting space for AKP opposing voices has left a void for healthy debate, and pro-AKP voices tend to dominate physical and digital space. In a blunt move during May 2020, Turkey’s Directorate of Communications warned Turkish citizens that even liking or sharing a post could lead to trouble. Journalists, scholars, opposition leaders, and civil society leaders who are critical of the government are more likely to face prosecution. A large number of arrests has a chilling effect and has given rise to self-censorship. Law No. 7253 not only asserts control over social media companies, it also makes individuals using social media ever more vulnerable to the legal system as “the legal or natural person who facilitates its users to create, view, and share content such as text, image, sound, or location to enable social interaction” are open to scrutiny.

While the AKP is also blocking users from digital space, there is also a parallel attempt to leave AKP trolls quite ungoverned as they indulge in cyberbullying. Academics, journalists, and artists who have criticized AKP have found themselves attacked under a culture of “digital culture of lynching and censorship” by the AKP army of trolls. A significant number of trolls are graduates of pro-AKP Imam Hatip schools. It has been reported that these individuals receive regular payments, and there are also traces that pro-AKP networks further provide benefits to successful trolls, which include entities such as TRT and Turkcell. In addition, AKP has used bots to boost its presence in the digital space, leading to its narrative overrepresentation on online platforms. It was revealed that on a daily average, some 26.7 percent of the top ten trends of Twitter were made by fake accounts or bot trolls. In the same year, the highest impact of these accounts led them to constitute 47.5 percent of the top five Twitter trends.
7. Faith, Cyberspace, and Populist Authoritarianism

7.1. Religious Justifications of Internet Curbs by the Government

Religious leaders and movements wield influence, leading to pressure on governments in how they govern digital space. These curbs are justified in civilizational terms, drawing on various themes, including morality, religion, nationalism, and the like. Consequently, many rationales are provided on religious–nationalist lines for cyber governance.

In Indonesia, the Indonesian Ulama Council (MUI) has attempted to facilitate self-censorship on two occasions. In 2017, the MUI issued Fatwa No. 24 of 2017 to guide Muslim interactions online, prohibiting the spread of hoaxes. Previously, in 2016, the MUI’s branch in Central Sulawesi prohibited married Muslim women from uploading their photos online. It was believed that such acts could “have negative impacts on the individual and their families.” These groups also drive movements that claim to make one a better Muslim with trending hashtags such as #antiselfie, #indonesianpapacaran (literal meaning: Indonesia without dating)—this movement advocates singles marrying without courting in advance—as well as #hijrah and #akhwatbercadar (meaning, veiled Muslim ladies).

While highly diverse culturally, Malaysia has a Malay Muslim majority. Since Mahathir’s first term as prime minister, Islam has been institutionalized within the state apparatus. Consequently, the administration of cyberspace involves justification that has Islamism logic. The MCMC has been deliberating censoring Netflix shows with themes of nudity, sex scenes, and LGBTQ+ content on the platform. Politicians and the government also condemn fake news and justify internet curbs, especially through self-censorship. The ministry deems “fake news” as “fitna” (slander). A religious term is thus instrumentalized to target opposition and critical groups.

In Pakistan, the narrative has become dense in terms of justifying cyber security. In addition to claims that online spaces promote “fifth-generation warfare” against the country by foreigners, religious justifications are being used for cyber governance. The 2020 law has excessively focused on preserving “decency and morality” and promoting “Islamic culture” as opposed to “Western rock and roll” culture. Thus, around 95 percent of the websites banned in 2019 were because of religious reasons.

The Erdoğan regime has always focused on raising a “pious youth” as part of its ideological program. Typically adopting religious connotations in his language, Erdoğan has repeatedly delegitimized
public demonstrations against the government, from the Gezi protests in 2013 to those at Bogazici University in 2021, arguing these are Western ploys to bring down the country. Using the same rhetoric that Western values are “corrupting” the youth, AKP trolls have targeted LGBTQ+ communities online. While it has never been illegal to be gay in secular Turkey, the AKP has requested that TikTok’s local moderation ban LGBTQ+ content. “Cleaning up social media” platforms of “questionable” advertisements from Twitter, Pinterest, and the Turkish PeriscopeCo are quite common. This prevents LGBTQ+ and other opposition forces from generating advertisement-driven revenue from the platforms that support them. The anti-queer “moral” jihad also saw Netflix pressured to cancel a Turkish series with an LGBTQ+ storyline.

In 2011, the government ran a “Safe Use of the Internet” campaign, which mandates that organizations offering public internet access (e.g., libraries, cafes) use a Turkish-built filter called the “family filter.” Essentially designed to block foreign and domestic sites containing adult content, the law was positioned to safeguard young children from age-inappropriate content. By 2017, the BTK had blocked some 1.5 million websites in areas such as cafes and refuses to share a list of the websites it blocks.

### 7.2. The Prominent Role of Religious Leaders in Restricting Digital Freedom

Interestingly, religious leaders and popular figures that hold power to sway public opinion have a paradoxical stance toward the internet. In countries where they warn against the “evils” of cyberspace, they use the same space to communicate their messages to followers. Of course, each country differs in this regard, yet overall, these religious figures seem to hew close to the line of populist governments and find justifications for the authorities’ authoritarianism. Religious leaders in Malaysia have usually not taken any firm position regarding restricting online freedom. Instead, they encourage self-censorship to avoid invoking the wrath of God. The highest order of muftis via fatwas have permitted social media usage, but it is deemed prohibited when the platforms are used for actions such as calling someone a bad name, insulting and degrading others, betraying and lying, slander, and malicious gossip. In a less centralized manner in 2014, two muftis, in vain, urged the National Fatwa Council, the country’s highest Islamic authority, to release a fatwa prohibiting conversation through social media or messaging apps between unmarried men and women.

In India, beyond religious leaders, Bollywood celebrities have also played a key role in adopting the Hindutva ideology and defending the BJP’s questionable actions. The most prominent of them is Kangana Ranaut. An active Twitter user with millions of followers, she has been suspended on the platform in the past for Islamophobic Tweets. However, since 2014, Ranaut has actively defended the BJP’s politics. Recently she declared that “India got freedom in 2014” (since Modi’s victory) rather than 1947. India’s vast entertainment industry, which influences millions of Indian citizens, has many pro-BJP...
voices both in front of and behind the camera, which give full support to the BJP, whereas those who question them face a massive backlash from RSS-affiliated online trolls.

In Pakistan, the religious political parties have never done well, politically never managing to gain more than 10 percent seats in general elections. However, religious movements such as TLP that advocate for severe blasphemy punishments and right-wing clerics such as Maulana Tariq Jamel, Farhat Hashmi, and late Dr. Israr Ahmed have millions of followers on their social media. Ironically while they use these platforms actively, these individuals have repeatedly warned against the “dangers” of “Western technology” and have expressed concern over “anti-Islamic” sentiments of “misguided” liberal youth and Westerns.

Internet governance is also justified by pro-government religious institutions and scholars in Turkey. During the last two decades, Turkey’s Presidency of Religious Affairs (Diyanet), the centralized religious authority, has provided faith-based explanations to back Erdoğan’s moral crusade against the “external” and “internal” enemies. For example, in 2016, the “Social Media and the Family in the Context of Privacy” forum was held to guide Turks on building strong Muslim families, including the rights and responsibilities of each member to avoid the dangers of social media. The President of Diyanet at the time, Mehmet Gormez, directly targeted social media in his opening speech. More recently, Diyanet has published a booklet, “Social Media Ethics,” which advocates for stronger control of the realm and the use of Islam as a yardstick. Ali Erbas, the current president, often uses his bully pulpit to promote pro-AKP stances. His inflammatory comments on LGBTQ+ youth “spreading HIV” became a polarized Twitter debate. Erbas has also used his Twitter to participate in AKP-led political campaigns highlighting Islamophobia. In 2021, a Twitter post targeting Islam by far-right Dutch lawmaker Geert Wilders led top AKP leaders and Erdoğan himself to criticize the Dutch firebrand, and Ali Erbas was also found following the trend of condemning Wilders.

Beyond Diyanet, a host of pro-AKP Islamic scholars have echoed similar narratives. These figures include a close AKP circle of individuals such as Nihat Hatipoglu, a TV show host, and Hayrettin Karaman, a columnist, both Islamic scholars. They use these mediums to sow the idea that social media is full of misinformation targeting Turkish national interests, and it harbors the ability to mislead youth. Karaman has gone as far as publishing a highly emotive poem in his column that warns readers of the dangerous pull of capitalism and immorality of social media, while Hatipoglu has issued a so-called “tele-fatwa” warning of ethical ways of exchanging messages between unmarried women and men.

7.3. Laws to Limit Blasphemy, Heresy, Heterodoxy, and Pornography

Faith being a highly emotive subject, once instrumentalized, it seems to hold power over millions. Our case studies show that populists have a nuanced approach that creates a moral or religious crisis. Consequently,
they justify their authoritarianism as means to “save” “the people.” These real-life realities are echoed online and, for many, lead to serious consequences such as losing personal safety and possible legal prosecution.

There is no blasphemy law in India, but hate speech is punishable under Section 295A of the Indian Penal Code. However, rather than formal punishment targeting minorities (Dalits, Muslims, Christians, Adivasis, Sikhs), it is common for the BJP and its pundits to encourage or overlook the questionable acts of the pro-Hindutva “cyber volunteers.” In the country, 87.4 percent of fake news spreads via social media, which sometimes results in communal rioting or targeting harassment and killing of individuals accused of consuming beef known as “cow lynching.” Most events of mob killing by BJP representatives have been dismissed or have led to blatant victims blaming who “asked for it” because of their “hurtful” actions.

In other regions, explicit blasphemy laws are in place that permit curbs on freedoms online. In Indonesia, blasphemy is covered by Articles 156 and 156(a) of KUHP (criminal code) and in the 1965 Presidential Decree (No. 1/PNPS/1965) on the Prevention of Blasphemy and Abuse of Religions. As outlined in Article 156(a), those “who purposely express their views or commit an act that principally disseminates hatred, misuse or defame a religion recognized in Indonesia,” face a maximum of five years imprisonment. When an online video of Jakarta’s Governor Basuki Purnama (Ahok), a Chinese Christian, discussing Qur’anic verse surfaced during his election campaign in 2016, Ahok was charged and later sentenced to 20 months in prison for insulting Islam. It led to the end of his political career. In 2021, an Indonesian Christian preacher landed in hot water after uploading a video stating that he was the “26th Prophet,” while in Europe, Interpol’s assistance was sought to extradite and trial him. Unfortunately, this encouraged some clerics to demand the “head” of the accused. Additionally, the pornography law has been used to target the LGBTQ+ community. Due to the loose definition, the law aids in identifying “suspects” and sometimes leads to public humiliation such as being strip-searched, photographed, and forced to march naked into police vehicles.

Malaysia also has strict laws on blasphemy. Under the law, Sunni Islam is recognized, with Shiites, Ahmadis, and those from al-Arqam being “deviant.” There is evidence of groups spreading sectarian hatred. One such example is Gerakan Banteras Syiah, with more than 25,000 followers. The government has also suspended a Tamil-language daily for mistakenly printing an image of Jesus Christ holding a cigarette under the law. More commonly, the laws have been instrumentalized to target the LGBTQ+ community. There has been some discussion steered by the minister of religious affairs to regulate LGBTQ+ activity online, yet nothing has come out of it. There is no law against simply watching porn online in Malaysia, but the MCMC is active in blocking the websites, and in 2013, two persons who were charged for posting pornographic images of themselves on their blog were charged and tried.

Similarly, the colonial-era
blasphemy law enshrined in Pakistan’s constitution is misused by right-wing clerics and movements both off and online. These groups have mainly targeted minorities and democratic voices. It is common for people to face imprisonment and, in the worst cases, be issued death sentences if their internet posts or cell phone messages show “questionable” remarks about Islam. While governments and political parties have stayed away from making anti- or pro-comments, the grassroots clerics and their movements have used cyberspace to pressure the state judiciary to target these individuals by running online campaigns.

While Turkey remains secular via its constitution, blasphemy charges have been made possible under a 2016 amendment to the Turkish Penal Code (TCK). While no specific religion is mentioned in the legislation, it is usually used to “defend” Islam. For example, under the amended article, the pianist Fazil Say was tried and sentenced to a jail term for tweeting his skepticism over Islamic values, while actress Berna Lacin was charged with blasphemy for contesting capital punishment in a Tweet in 2018 (she was acquitted after two years). Also, two journalists were each handed two-year sentences for reprinting the Charlie Hebdo sketches satirizing Islam under the law in 2016. In 2020, Enver Aysever, a journalist, was arrested and charged for mocking clergy and their attitude during the COVID-19 pandemic. Astonishingly, people who shared the video of “Bella Ciao” being played in an Izmir mosque were also warned to take off the posts or otherwise face charges by Izmir’s Chief Public Prosecutor.

7.4 More Restrictions on Religious Minorities or in Areas Where Religious Minorities Live in Large Numbers

The countries that display direct targeting of minorities are mainly confined to India and Turkey. In the former, the hurried abrogation of Articles 35a and 370, in August 2019 from the constitution of India, the region of Kashmir administered by India, has witnessed one of the world’s worst forms of suppression of freedoms, lasting 213 days. The region alone accounts for 90 percent of internet shutdowns in the country. The curbs are justified as means of primitively controlling jihadist activity in Kashmir. Despite the crippling impact on tourism, healthcare, education, and the overall economy, the curbs continue. Between January 2012 and March 2021, there were 518 government-imposed internet shutdowns across India, resulting in the highest number of internet blocks in the world so far. In Turkey, the internet shutdown that explicitly targets a region is based on ethnicity rather than religious conflict. Due to the prolonged conflict with the Kurdish community, the regions with Kurdish resistance pockets, as mentioned above, have faced the largest brunt of internet blackouts. However, like India, these are explained as measures to curb “terrorism,” whereas it is rooted in an ideological conflict between the Turkish state and the right of the Kurdish people to exist freely.
8. Conclusion

Change is a hallmark of the twenty-first century. Once considered a Latin American issue or a rarity, the most recent wave of populism has resulted in a drastic global political transformation so much so that it looms large in two of the world’s largest democracies (the United States and India). Impressively, if worryingly, it has latched on to religion which has the power to mobilize crowds and cloud judgment regarding the capabilities of populists in power. This report has brought to light a unique aspect of this nexus between faith and populism, and it offers an insight into how cyberspace and politics offline have become highly intertwined to create a hyper-reality in which events are taking place.

Religion and politics merge in each country to shape cyber governance. For most countries, the last two decades have been dominated by the introduction and rapid adoption of digital technology. Thus, there is still debate about where laws should and should not intervene. The wading of religion into politics in context, it has to be said, usually begins with the right intentions—to regulate cyberspace in the interest of citizens. However, over the years, both politicians and political movements have used relatively lax legal frameworks to their partisan advantage.

Nevertheless, partisan entities have exploited the law in an instrumentalized fashion to curb opposition, exert control, and use the space for growth in popularity. Most populist governments’ cyber governance politics mirror their offline undemocratic policies. For stakeholders outside the ambit of power, cyberspace allows them a medium of connection to spread their ideology. Ironically there is a love-hate relationship with social media. Most of these leaders organize and communicate with their followers using digital media, yet, at the same time, constantly warn against the “ills” of such platforms. Essentially, morality has been a common theme used by all stakeholders to justify the need for increasingly draconian digital laws. Moral panics about digital space simply juice up widespread anxieties and catalyze populist appeal while simultaneously acting as a curtain for their undemocratic actions.

Mirroring and interconnectedness of cybers and offline spaces in quite evident. Firstly, it is noteworthy that populists understand the value of digital space. Thus, in most cases, we notice an active monopolization of the realm that uses both religious and security-driven justifications to limit space for opposition and civil society and at the same time reclaim that space for themselves and their allies. With total control over an alternative space, populists replicate offline socio-politics there. Essentially, this sees populist authoritarianism migrate to the digital realm and also plays some role in shaping offline events such as the case of cow lynching in India or Tweets leading to trials under blasphemy laws in Turkey, Indonesia, and Pakistan.

The future of democracies is highly intertwined with digital space. The narrative that plays a part in bringing a movement to life or aiding political victory is determined in this realm
to a great degree. While the overall picture of free digital space seems precarious in the near future, on the other hand, the individual differences in each case study offer some hope that a move toward democracy might lead to a reconsideration of digital authoritarianism. However, the degree of social damage they are causing is hard to determine. Today Islamist and Hindutva trolls feel an unprecedented sense of cyber empowerment where they can hurl abuse without even physically seeing any consequences or feeling the victim’s plight.
## 9. APPENDIX

### DIGITAL GOVERNANCE TOOLKIT

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>LAW, LEGAL INSTRUMENT, OR AGENCY</th>
<th>SCOPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>INDIA</td>
<td>Information Technology Act, 2000 [amended in 2008]</td>
<td>The basic statutory ground for digital governance. Since its creation, the act has expanded and been extensively instrumentalized to target political activists.</td>
</tr>
<tr>
<td></td>
<td>Central Monitoring System (CMS)</td>
<td>Originally designed to be a counter-terrorism tool, it has enabled massive digital surveillance and profiling of citizens.</td>
</tr>
<tr>
<td></td>
<td>Section 69A of the IT Act and the 2009 blocking rules</td>
<td>The IT Act was drafted in the name of India’s security interests. Responsible for blocking websites on a mass scale without explicitly stating the sites or the reasons.</td>
</tr>
<tr>
<td></td>
<td>Information technology rules 2021</td>
<td>Demands more accountability from social media companies but makes them more compliant about content removal and profile blocking/flagging requests.</td>
</tr>
<tr>
<td>INDONESIA</td>
<td>Indonesian Broadcasting Commission (KPI)</td>
<td>Establishes censorship boards that tackle hate speech and other questionable content. These have usually been used to persecute minorities.</td>
</tr>
<tr>
<td></td>
<td>Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE).</td>
<td>The law enables ministers and ministerial boards to prosecute individuals and related parties legally.</td>
</tr>
<tr>
<td></td>
<td>Law on Pornography No. 19 of 2014</td>
<td>Used to curb sexual content from websites and other digital spaces. It is sometimes used by the authorities to advance a particular sense of morality by censoring content.</td>
</tr>
<tr>
<td></td>
<td>Law No. 14 of 2015 and No. 26 of 2015 on the Implementation of Closing Down Content and/or Related Rights in an Electronic System.</td>
<td>These two laws aim to manage harmful content online and aid digital rights. Yet the lax definitional parameters mean they are ripe for politicization by governments and clerics who wield influence in Jakarta.</td>
</tr>
<tr>
<td><strong>MALAYSIA</strong></td>
<td><strong>Malaysian Communications and Multimedia Commission (MCMC) Communications and Multimedia Act 1998 (CMA)</strong></td>
<td>A regulator of information providing services. Holds authority to regulate, issue licenses, and censor materials. Using the loose definitional parameters, it has been known for censoring cyberspace to weeding out critical sources on the government.</td>
</tr>
<tr>
<td><strong>Malaysia Cyber Security Strategy 2020-2024 (initially introduced in 2017)</strong></td>
<td>The widened definition of cybersecurity in Malaysia has threatened the role of civil society to be the voice of dissent against the government. Internet regulation in the name of cybersecurity has been used to restrict internet freedom among political and social dissidents</td>
<td></td>
</tr>
<tr>
<td><strong>Department of Community Communication (J-KOM)</strong></td>
<td>The basic statutory ground for digital governance. Since its creation, the act has expanded and been extensively instrumentalized to target political activists.</td>
<td></td>
</tr>
<tr>
<td><strong>PAKISTAN</strong></td>
<td><strong>Pakistan Telecommunication Authority (PTA)</strong></td>
<td>Oversees information transmitting technologies and departments. Since the 2006 amendment, it has been instrumental in surveillance.</td>
</tr>
<tr>
<td><strong>Fair Trial Act, 2013 Prevention of Electronic Crimes Act (PECA), 2016</strong></td>
<td>While created with the good intention of preventing cybercrimes, these laws have legalized extensive recording and surveillance by the state. Committees established under these acts are usually headed or supervised by senior military officers.</td>
<td></td>
</tr>
<tr>
<td><strong>Removal and Blocking of Unlawful Online Content Rules, 2020</strong></td>
<td>Allows for content blockage at the proxy level. However, the broad definitional parameters make it a tool to block any information the state deems</td>
<td></td>
</tr>
<tr>
<td><strong>Pakistan Media Development Authority (PMDA) (nearly approved in parliament)</strong></td>
<td>Likely to pass soon, still a bill, this centralizes all media control (including social media) under a single centralized body. Heavy concentration of power and lack of transparency in decision-making.</td>
<td></td>
</tr>
<tr>
<td>TURKEY</td>
<td>Turkish law on the right to information, 2004 (Turkish Penal Code No. 5237)</td>
<td>First piece of legislation to govern the internet in Turkey. Also criminalized illegal activity in cyberspace.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>Telecommunications Directorate (TİB), later the Telecommunications Authority (BTK)</td>
<td>Established in 2005 but viewed as “pro-Gulenist,” it carried out internet governance activities such as tracking, surveillance, and evaluating communications made through the internet along with determining legal and illegal hardware and software development within the country.</td>
</tr>
<tr>
<td></td>
<td>Internet Law, 2007 (Law No. 5651)</td>
<td>Allows for blocking of websites on the grounds of prorogued terrorism. Its loose definitional parameters are used to target civil and political opposition.</td>
</tr>
<tr>
<td></td>
<td>Telecommunication Technologies Authority (BTK)</td>
<td>Replacing the TİB in 2016, the body has been given to shut down the means of communication at the state’s request. This includes internet services.</td>
</tr>
<tr>
<td></td>
<td>Decree-Law No. 678</td>
<td>While it is not a direct law related to cyberspace, it provides incentives for social media companies to open domestic offices. This ensures local laws apply to the organizations.</td>
</tr>
<tr>
<td></td>
<td>Law No. 7253 or “Amendment Law”</td>
<td>Introduces further means to control social media services provided by detailing a list of requirements and fines if companies fail to comply.</td>
</tr>
</tbody>
</table>
10. Author Bios

**IHSAN YILMAZ** is Research Professor and Chair at the Alfred Deakin Institute for Citizenship and Globalisation (ADI), Deakin University, Melbourne, Australia. He is also a Visiting Research Associate of the Oxford Centre for Religion and Culture, Regent’s Park College, The University of Oxford, and a Non-Resident Senior Scholar at the European Center for Populism Studies (Brussels). He has conducted research on religion and politics; authoritarianism; digital authoritarianism; populism (Turkey, Pakistan, Indonesia, India); securitization; “sharp power”; nation-building; citizenship; Islamism; ethnic-religious-political minorities and their securitization (Middle East, Pakistan, Indonesia); Muslim minorities (Australia, Turkey, the UK, and the USA); Islam-state-society relations in the majority and minority contexts; Turkish politics; Turkish diasporas (the UK, Australia, the USA); transnationalism; and intergroup contact (Australia). Professor Yilmaz was a professor of political science at Istanbul Fatih University (2008–2016). He was a lecturer in law, social sciences, and politics at SOAS, University of London (2001–2008), and was a fellow at the Centre for Islamic Studies, University of Oxford (1999–2001). He is the author of Creating the Desired Citizen: Ideology, State and Islam in Turkey (Cambridge University Press, 2021).

**RAJA M. ALI SALEEM** is an Associate Professor (Public Policy) at the Centre for Public Policy and Governance at Forman Christian College in Lahore, Pakistan. He is a former civil servant and has more than 20 years of diverse experience in government and academia. His research focuses on religious nationalism, the relationship between church and state, the politics of Muslim-majority countries, especially Turkey, Iran, and Saudi Arabia, local governments, public financial management, the role of the military in politics, and democratic consolidation. In 2020, he was a Fellow of Wolfson College, University of Oxford. His first book, State, Nationalism, and Islamization: Historical Analysis of Turkey and Pakistan, was published by Palgrave-Macmillan in 2017.

**MAHMOUD PARGOO** is a research fellow at Deakin University (Melbourne) and a visiting fellow at the AI-enabled Processes (AIP) Research Centre, Macquarie University in Sydney. Mahmoud is the author of Secularization of Islam in Post-Revolutionary Iran (Routledge, 2021) and lead-author of Presidential Elections in Iran: Islamic Idealism since the Revolution (Cambridge University Press, 2021).

**SYAZA SHUKRI** is an assistant professor at the Department of Political Science, Kulliyyah of Islamic Revealed Knowledge and Human Sciences, International Islamic University Malaysia. Her area of specialization is in comparative politics, specifically in democratization and politics in the Middle East and Southeast Asia. Her current research interests include populism, identity politics, inter-ethnic relations, political Islam, geopolitics, and gender studies, specifically in
Muslim-majority contexts. Among her recent works is “Populism and Muslim Democracies,” published in Asian Politics & Policy. She is also currently working on a book chapter on Islamist populism in Malaysia since 2018. She has degrees from the University of Pittsburgh (where she graduated summa cum laude), the London School of Economics and Political Science, and International Islamic University Malaysia. She can be reached at syazashukri@iium.edu.my.

IDZNURSHAM ISMAIL, the founder of stratsea.com, possesses a Master in Strategic Studies and a First Class Honours in Biological Sciences from the S. Rajaratnam School of International Studies (RSIS) Nanyang Technological University (NTU), respectively. After his stint as a Research Analyst at the Centre for Political Violence and Terrorism Research (ICPVTR, RSIS), he resided in Indonesia for numerous years, gaining experience in organizations such as The Jakarta Post, the Wahid Foundation, and PAKAR. He specializes in security-related issues, particularly terrorism and unconventional weapons. His current research includes non-traditional security themes such as public health.

KAINAT SHAKIL is a non-resident Research Associate at the European Center for Populism Studies. Her research explores populism from the perspectives of religion, emotions, and gender. The regional focus of her work is mainly Pakistan and demographically Muslim-majority countries. Previously, she was a researcher at The Shahid Javed Burki Institute of Public Policy at NetSol (BIPP)—a Pakistan-based think-tank—where her work focused on reviewing public policies from a people-centric perspective. A large part of her work was qualitative research mapping to understand the public’s perceptions, feelings, reactions, and engagement with government policies and vice versa. Shakil also develops interactive cultural, historical, and political curricula for middle school pupils with a focus on inclusivity. Before working as a full-time researcher, she was an Erasmus research scholar at Middlesex University London and the recipient of the US State Department’s cultural scholarship, Global UGRAD.
ECPS
EUROPEAN CENTER for POPULISM STUDIES

©ECPS 2022 ALL RIGHTS RESERVED
ECPS REPORTS ARE SUBJECT TO INTERNAL PEER REVIEW,
FACT-CHECKING AND COPY-EDITING.

THIS REPORT IS AVAILABLE FOR FREE DOWNLOADING AT:
HTTPS://WWW.POPULISMSTUDIES.ORG/PUBLICATIONS/REPORTS/

EUROPEAN CENTER FOR POPULISM STUDIES (ECPS) IS AN
INDEPENDENT, NON-PARTISAN, NONPROFIT ORGANIZATION, BASED IN
BRUSSELS, FOR RESEARCH ON AND ANALYSIS OF
CHALLENGES POSED BY THE RESURGENCE OF POLITICAL POPULISM.
ECPS FACILITATES COLLABORATION AMONG NETWORKS OF
ACADEMIC EXPERTS, PRACTITIONERS, POLICYMAKERS, MEDIA, AND
OTHER STAKEHOLDERS. ECPS OFFERS A PLATFORM FOR THE
EXCHANGE OF POLICY SOLUTIONS ON ISSUES RELATING TO RISING
POPULISM AND PROVIDES INSIGHTS FOR POLICY-MAKING AND CRITICAL
ANALYSIS TO RAISE BROADER AWARENESS AND
ENGAGEMENT.

ADDRESS: 155 WETSTRAAT / RUE DE LA LOI 1040 BRUSSELS, BELGIUM
EMAIL: ECPS@POPULISMSTUDIES.ORG
PHONE: +32 24658318
WWW.POPULISMSTUDIES.ORG