Manipulating Social Media
to Undermine Democracy

November 2017

Freedom House

FREEDOM ON THE NET 2017

Freedom on the Net 2017

Table of Contents

This report was made possible by the generous support of the U.S. State Department's Bureau of Democracy, Human Rights and Labor (DRL), Google, the German Federal Foreign Office, the Internet Society, Yahoo, and Golden Frog. The content of this publication is the sole responsibility of Freedom House and does not necessarily represent the views of its donors.

This booklet is a summary of findings for the 2017 edition of *Freedom on the Net*. A full volume with 65 country reports assessed in this year's study can be found on our website at **www.freedomonthenet.org.**

THE AUTHORS

The authors of this report are Sanja Kelly, Mai Truong, Adrian Shahbaz, Madeline Earp, and Jessica White, of the Freedom of the Net project.

ON THE COVER

Protester at demonstration in Moscow, August 2017, against rise in government surveillance and restrictions on the internet.

Photo credit: Getty Images / Maxim Zmeyev

Freedom
House

Manipulating Social Media to Undermine Democracy

Governments around the world have dramatically increased their efforts to manipulate information on social media over the past year. The Chinese and Russian regimes pioneered the use of surreptitious methods to distort online discussions and suppress dissent more than a decade ago, but the practice has since gone global. Such state-led interventions present a major threat to the notion of the internet as a liberating technology.

Online content manipulation contributed to a seventh consecutive year of overall decline in internet freedom, along with a rise in disruptions to mobile internet service and increases in physical and technical attacks on human rights defenders and independent media.

Nearly half of the 65 countries assessed in *Freedom on the Net 2017* experienced declines during the coverage period, while just 13 made gains, most of them minor. Less than one-quarter of users reside in countries where the internet is designated Free, meaning there are no major obstacles to access, onerous restrictions on content, or serious violations of user rights in the form of unchecked surveillance or unjust repercussions for legitimate speech.

The use of "fake news," automated "bot" accounts, and other manipulation methods gained particular attention in the United States. While the country's online environment remained generally free, it was troubled by a proliferation of fabricated news articles, divisive partisan vitriol, and aggressive harassment of many journalists, both during and after the presidential election campaign.

Russia's online efforts to influence the American election have been well documented, but the United States was hardly alone in this respect. Manipulation and disinformation tactics played an important role in elections in at least 17 other countries over the past year, damaging citizens' ability to choose their leaders based on factual news and authentic debate. Although some governments sought to support their interests and expand their influence abroad—as with Russia's disinformation campaigns in the United States and Europe—in most cases they used these methods inside their own borders to maintain their hold on power.

Venezuela, the Philippines, and Turkey were among 30 countries where governments were found to employ armies of "opinion shapers" to spread government views, drive particular agendas, and counter government critics on social media. The number of governments attempting to control online discussions in this manner has risen each year since Freedom House began systematically tracking the phenomenon in 2009. But over the last few years, the practice has become significantly more widespread and technically sophisticated, with bots, propaganda producers, and fake news outlets exploiting social media and search algorithms to ensure high visibility and seamless integration with trusted content.

Half of all internet shutdowns in the past year were specific to mobile connectivity.

Unlike more direct methods of censorship, such as website blocking or arrests for internet activity, online content manipulation is difficult to detect. It is also more difficult to combat, given its dispersed nature and the sheer number of people and bots employed for this purpose.

The effects of these rapidly spreading techniques on democracy and civic activism are potentially devastating. The fabrication of grassroots support for government policies on social media creates a closed loop in which the regime essentially endorses itself, leaving independent groups and ordinary citizens on the outside. And by bolstering the false perception that most citizens stand with them, authorities are able to justify crackdowns on the political opposition and advance antidemocratic changes to laws and institutions without a proper debate. Worryingly, state-sponsored manipulation on social media is often coupled with broader restrictions on the news media that prevent access to objective reporting and render societies more susceptible to disinformation.

Successfully countering content manipulation and restoring trust in social media—without undermining internet and media freedom—will take time, resources, and creativity. The first steps in this effort should include public education aimed at teaching citizens how to detect fake or misleading news and commentary. In addition, democratic societies must strengthen regulations to ensure that political advertising is at least as transparent online as it is offline. And tech companies should do their part by reexamining the algorithms behind news curation and by disabling fake accounts that are used for antidemocratic ends.

In the absence of a comprehensive campaign to deal with this threat, manipulation and disinformation techniques could enable modern authoritarian regimes to expand their power and influence while permanently eroding user confidence in online media and the internet as a whole.

Other key trends

Freedom on the Net 2017 identified five other trends that significantly contributed to the global decline in internet freedom over the past year:

State censors target mobile connectivity. An increasing number of governments have shut down mobile internet service for political or security reasons. Half of all internet shutdowns in the past year were specific to mobile connectivity, with most others affecting mobile and fixed-line service simultaneously. Many of the mobile shutdowns occurred in areas populated by minority ethnic or religious groups that have challenged the authority of the central government or sought greater rights, such as Tibetan areas in China and Oromo areas in Ethiopia. The actions cut off internet access for already marginalized people who depend on it for communication, commerce, and education.

More governments restrict live video. As live video streaming gained popularity over the last two years with the emergence of platforms like Facebook Live and Snapchat's Live Stories, some governments have attempted to restrict it, particularly during political protests, by blocking live-streaming applications and arresting people who are trying to broadcast abuse. Considering that citizen journalists most often stream political protests on their mobile phones, governments in countries like Belarus have at times disrupted mobile connectivity specifically to prevent live-streamed images from reaching mass audiences. Officials often justified their restrictions by noting that live streaming can be misused to broadcast nudity or violence, but blanket bans on these tools prevent citizens from using them for any purpose.

Technical attacks against news outlets, opposition, and rights defenders on the rise. Cyberattacks became more common due in part to the increased availability of relevant technology, which is sold in a weakly regulated market, and in part to inadequate security practices among many of the targeted groups or individuals. The relatively low cost of cyberattack tools has enabled not only central governments, but also local government officials and law enforcement agencies to obtain and employ them against their perceived foes, including those who expose corruption and abuse. Independent blogs and news websites are increasingly being taken down through distributed denial-of-service (DDoS) attacks, activists' social media accounts are being disabled or hijacked, and opposition politicians and human rights defenders are being subjected to surveillance through the illegal hacking of their phones and computers. In many cases, such as in Bahrain, Azerbaijan, Mexico, and China, independent forensic analysts have concluded that the government was behind these attacks.

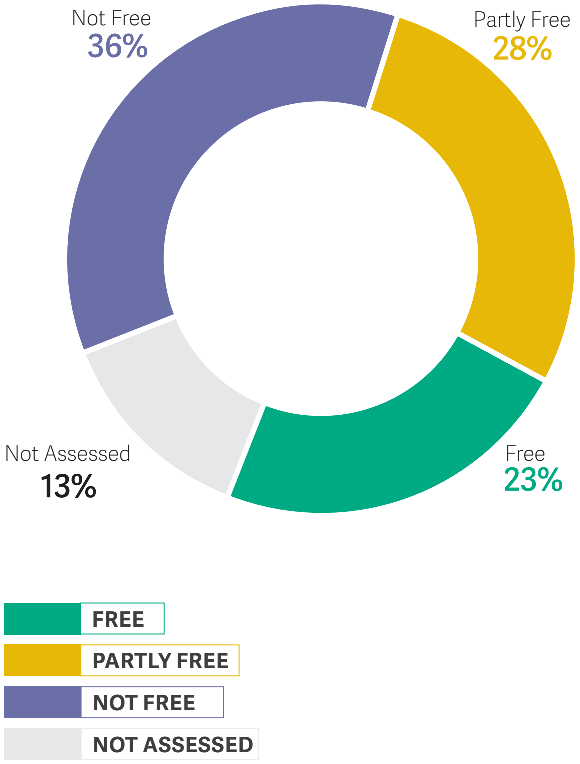
New restrictions on virtual private networks (VPNs). Although VPNs are used for diverse functions—including by companies to enable employees to access corporate files remotely and securely—they are often employed in authoritarian countries as a means of bypassing internet censorship and accessing websites that are otherwise blocked. This has made VPNs a target for government censors, with 14 countries now restricting the connections in some form and with six countries introducing new restrictions over the past year. The Chinese government, for example, issued regulations that required registration of "approved VPNs," which are presumably more compliant with government requests, and has moved to block some of the unregistered services.

Physical attacks against netizens and online journalists expand dramatically. The number of countries that featured physical reprisals for online speech increased by 50 percent over the past year—from 20 to 30 of the countries assessed. Online journalists and bloggers who wrote on sensitive topics and individuals who criticized or mocked prevailing religious beliefs were the most frequent targets. In eight countries, people were murdered for their online expression. In Jordan, for example, a Christian cartoonist was shot dead after publishing an online cartoon that lampooned Islamist militants' vision of heaven, while in Myanmar, an investigative journalist was murdered after posting notes on Facebook that alleged corruption.

Several of the practices described above are clearly outside the bounds of the law, signaling a departure from the trend observed in previous years, when governments rushed to pass new laws that regulated internet activity and codified censorship tactics. For instance, spreading fake news and smearing individuals' public image are often criminal offenses in countries where the government employs those tactics against its critics. Similarly, in a number of countries where the government is apparently behind cyberattacks affecting the human rights community, newly passed cybersecurity laws actually prohibit such activity. Even in cases of mobile shutdowns, most countries do not have specific laws authorizing the disruptions. It appears that in many countries, the internet regulations imposed in recent years apply only to civilians in practice, and government officials are able to disregard them with impunity.

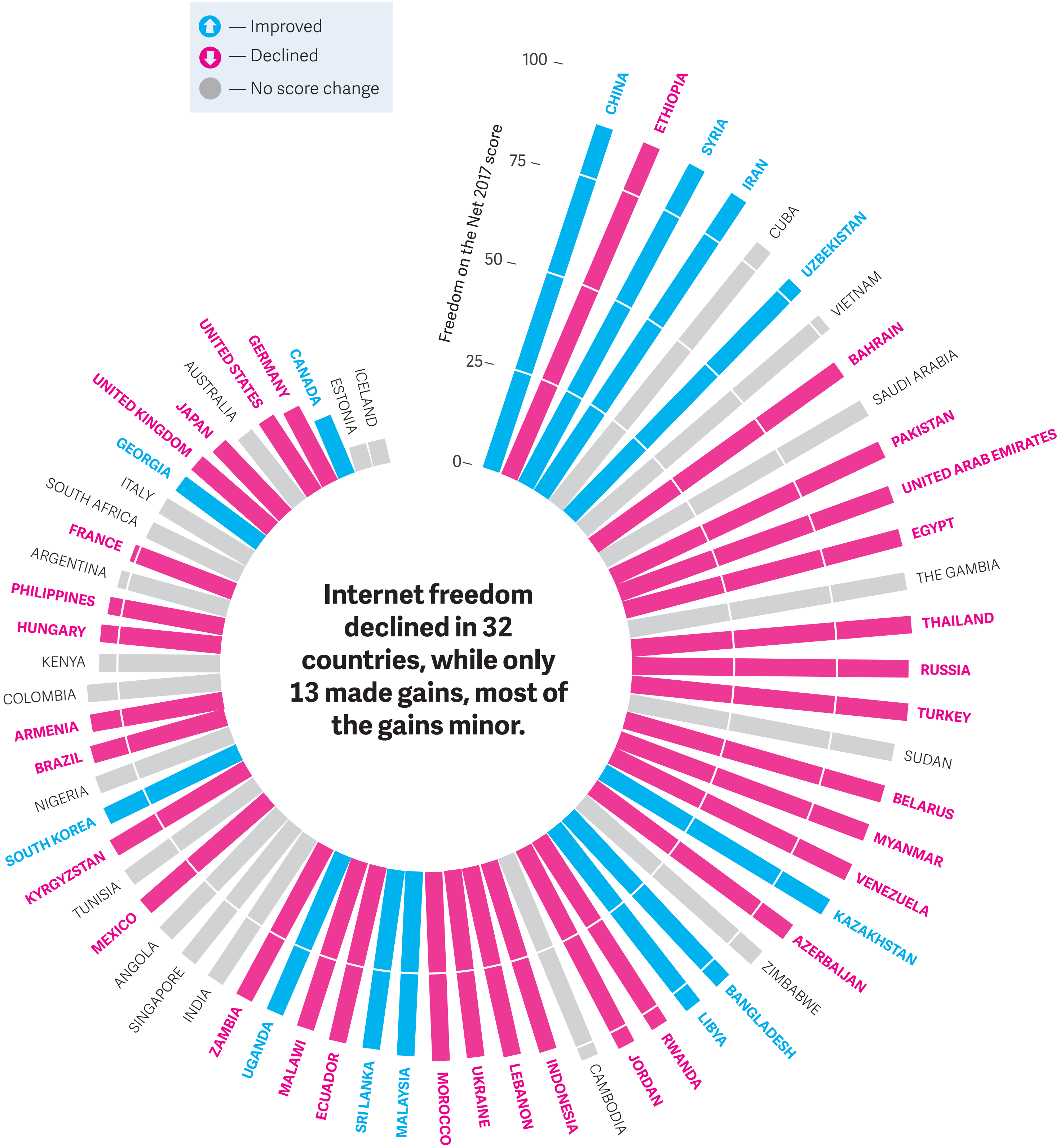
GLOBAL INTERNET POPULATION BY 2017 FOTN STATUS

FOTN assesses 87 percent of the world's internet user population.



Online manipulation and disinformation tactics played an important role in elections in the United States and at least 17 other countries.

2017 FREEDOM ON THE NET IMPROVEMENTS AND DECLINES



Tracking the global decline

Freedom on the Net is a comprehensive study of internet freedom in 65 countries around the globe, covering 87 percent of the world's internet users. It tracks improvements and declines in government policies and practices each year. The countries included in the study are selected to represent diverse geographical regions and regime types. This report, the seventh in its series, focuses on developments that occurred between June 2016 and May 2017, although some more recent events are included in individual country narratives. More than 70 researchers, nearly all based in the countries they analyze, contributed to the project by examining laws and practices relevant to the internet, testing the accessibility of select websites and services, and interviewing a wide range of sources.

Of the 65 countries assessed, 32 have been on an overall decline since June 2016. The biggest declines took place in Ukraine, Egypt, and Turkey. In Ukraine, the government blocked major Russian-owned platforms, including the country's most widely used social network (VKontakte) and search engine (Yandex), on national security grounds. Meanwhile, violent reprisals for online activity escalated in the country, with one prominent online journalist killed in a car bombing. In Egypt, the authorities blocked over 100 websites, including that of the Qatar-based news network Al-Jazeera, the independent news site *Mada Masr*, and the blogging platform Medium. Social media users received lengthy prison sentences for a range of alleged offenses, including insulting the country's president. And in Turkey, thousands of smartphone owners were arrested simply for having downloaded the encrypted communication app ByLock, which was available publicly through Apple and Google app stores, amid allegations that the app was used by those involved in the failed July 2016 coup attempt.

China was the worst abuser of internet freedom for the third consecutive year. The Chinese government's crackdown intensified in advance of the Communist Party's 19th National Congress in October 2017, which ushered in Xi Jinping's second five-year term as general secretary. The year's restrictions included official orders to delete all online references to a newly discovered species of beetle named after Xi, which the censors reportedly found offensive given the beetle's predatory nature. Meanwhile, the authorities further eroded user privacy through a new cybersecurity law that strengthened internet companies' obligation to register users under their real names and assist security agencies with investigations. Domestic companies are implementing the measures as part of a gradual move toward a unified "social credit" system—assigning people numerical scores based on their internet usage patterns, much like a financial credit score—that could ultimately make access to government and financial services dependent on one's online behavior. The cybersecurity law also requires foreign companies to store data on Chinese users within China by 2018, and many—including Uber, Evernote, LinkedIn, Apple, and AirBnb—have started to comply.

In Turkey, thousands were arrested for downloads of an encrypted communication app allegedly used by coup plotters.

Government critics received sentences of up to 11 years in prison for publishing articles on overseas websites. While such penalties are documented year after year, the July 2017 death of democracy advocate Liu Xiaobo from liver cancer while in custody was a stark reminder of the immense personal toll they may take on those incarcerated. Liu, a Nobel Peace Prize winner, had been in prison since a prodemocracy manifesto he coauthored was circulated online in 2009. News of his passing sparked a new wave of support—and censorship.

The internet freedom status of Venezuela and Armenia was downgraded. Venezuela went from Partly Free to Not Free amid a broader crackdown on political rights and civil liberties following President Nicolás Maduro's May 2016 declaration of a "state of exception and economic emergency," which was renewed in May 2017. The government blocked a handful of sites that provided live coverage of antigovernment protests, claiming the sites were "instigating war." Armed gangs physically attacked citizen and online journalists who tried to document antigovernment protests, while the political opposition and independent outlets experienced an unprecedented wave of cyberattacks, effectively taking their sites offline for periods of time and disabling their accounts. In Armenia, which dropped from Free to Partly Free, the police attacked and obstructed journalists and netizens who were trying to live stream antigovernment protests. Thousands of people demonstrated in response to the police's mis-

DISTRIBUTION OF GLOBAL INTERNET USERS BY COUNTRY AND FOTN STATUS

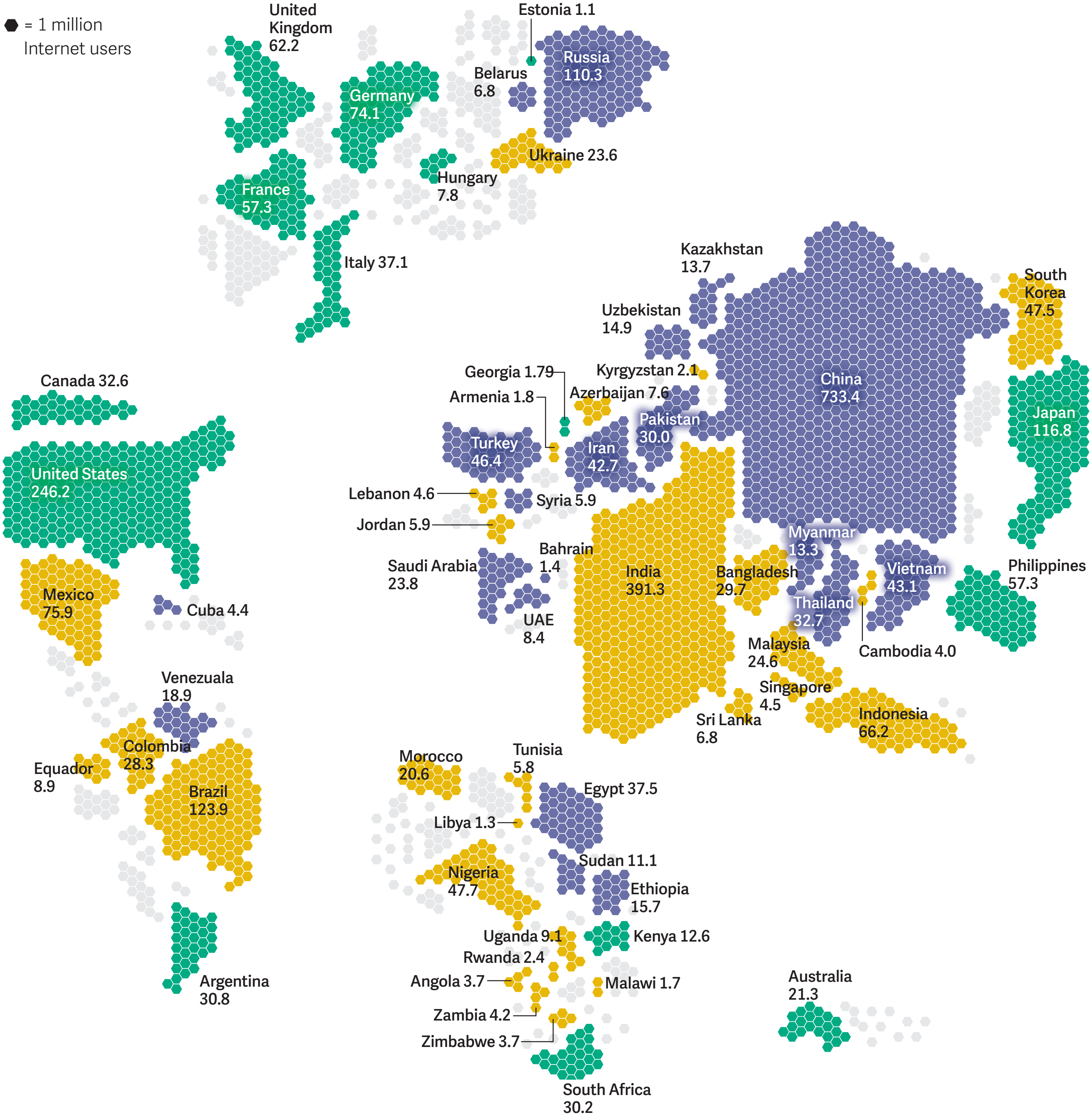
🟩 FREE

🟨 PARTLY FREE

🟪 NOT FREE

⬜ NOT ASSESSED

The 65 countries covered in *Freedom on the Net* represent 87 percent of the world's internet user population. Over 1.2 billion internet users, or forty percent of global users, live in three countries — China, India, and the United States — that span the spectrum of internet freedom environments, from Free to Not Free.



handling of a hostage situation, during which officials temporarily restricted access to Facebook.

The United States also experienced an internet freedom decline. While the online environment in the United States remained vibrant and diverse, the prevalence of disinformation and hyperpartisan content had a significant impact. Proliferation of "fake news"—particularly on social media—peaked in the run-up to the November 2016 presidential election, but it continues to be a concern. Journalists who challenge Donald Trump's positions have faced egregious online harassment.

Among other developments, after Trump assumed office as president in January 2017, U.S. Customs and Border Protection agents in March asked Twitter to reveal the owner of an account that objected to Trump's immigration policy, and backed off only after the company fought the request in court. Even more worrying was a government request in July 2017 to compel internet hosting company DreamHost to hand over all the internet protocol addresses of users who visited disruptj20.org, a website that helped coordinate Trump inauguration protests; this request was narrowed only after a legal challenge from DreamHost. Meanwhile, the new chairman of the Federal Communications Commission announced a plan in April to roll back net neutrality protections adopted in 2015.

Only 13 countries earned an improvement in their internet freedom score. In most cases, the gains were limited and did not reflect a broad shift in policy. In Libya, for example, several news websites were unblocked, and unlike in previous years, no users were imprisoned for their online activity. In Bangladesh, there was no repetition of the government's temporary 2015 blocking of popular apps like Facebook, WhatsApp, and Viber amid security concerns following the confirmation of death sentences against two Islamist leaders. And Uzbekistan, one of the most restrictive states assessed, improved slightly after the introduction of a new e-government platform designed to channel public grievances, which prompted greater citizen engagement.

Global internet user stats

Nearly **3.4 billion** people have access to the internet.

According to Freedom House estimates:

63% live in countries where ICT users were arrested or imprisoned for posting content on political, social, and religious issues.

62% live in countries where individuals have been attacked or killed for their online activities since June 2016.

52% live in countries where social media or messaging apps were blocked over the past year.

47% live in countries where online discussion of LGBTI issues can be repressed or punished.

43% live under governments which disconnected internet or mobile phone access, often for political reasons.

42% live in countries where the government employs armies of "opinion shapers" to spread government views and counter critics on social media.

Major Developments

Bots and fake news add a new sophistication to manipulation online

Repressive regimes have long sought to control the flow of information within their territories, a task rendered more difficult by the advent of the internet. When punitive laws, online censorship, and other restrictive tactics prove inadequate and comprehensive crackdowns are untenable, more governments are mass producing their own content to distort the digital landscape in their favor. Freedom House first tracked the use of paid progovernment commentators in 2009, but more governments are now employing an array of sophisticated manipulation tactics, which often serve to reinforce one another. Authoritarians have effectively taken up the same tools that many grassroots democratic activists used to disrupt the state media narrative, and repurposed them to advance an antidemocratic agenda.

Paid progovernment commentators were found in 30 of the 65 countries surveyed in this study, a new high.

The Russian government's attempted use of bots and fake news to sway elections in the United States and Western Europe has brought new attention to the issue of content manipulation. But in many countries, these tactics are used not by foreign powers, but by incumbent governments and political parties seeking to perpetuate their rule.

Progovernment commentators feign grassroots support

Progovernment commentators were found in 30 of the 65 countries surveyed in this study, up from 23 in the 2016 edition and a new high. In these countries, there are credible reports that the government employs staff or pays contractors to manipulate online discussions without making the sponsored nature of the content explicit. The evidence has been collected largely through investigative reporting, leaked government documents, and academic research. The manipulation has three principal aims: (1) feigning grassroots support for the government (also known as "astroturfing"), (2) smearing government opponents, and (3) moving online conversations away from controversial topics. The progovernment commentators tasked with achieving these goals come in many forms.

In the most repressive countries, members of the government bureaucracy or security forces are directly employed to manipulate political conversations. For example, Sudan's so-called cyber jihadists—a unit within the National Intelligence and Security Service—created fake accounts to infiltrate popular groups on Facebook and WhatsApp, fabricate support for government policies, and denounce critical journalists. A government propagandist in Vietnam has also acknowledged operating a team of hundreds of "public opinion shapers" to monitor and direct online discussions on everything from foreign policy to land rights.

In other cases, online manipulation is outsourced to the ruling party apparatus, political consultancies, and public relations firms. Investigative reporting has exposed the role of the Internet Research Agency, a Russian "troll farm" reportedly financed by a businessman with close ties to President Vladimir Putin. In the Philippines, news reports citing former members of a "keyboard army" said they could earn $10 per day operating fake social media accounts that supported Rodrigo Duterte or attacked his detractors in the run-up to his May 2016 election as president; many have remained active under his administration, amplifying the impression of widespread support for his brutal crackdown on the drug trade. In Turkey, numerous reports have referred to an organization of "AK Troller," or "White Trolls," named after the ruling Justice and Development Party, whose Turkish acronym AK also means "white" or "clean." Some 6,000 people have allegedly been enlisted by the party to manipulate discussions, drive particular agendas, and counter government opponents on social media. Journalists and scholars who are critical of the government have faced orchestrated harassment on Twitter, often by dozens or even hundreds of users.

Over the years, governments have found new methods of crowdsourcing manipulation to achieve a greater impact and avoid direct responsibility. As a result, it can be hard to distinguish propaganda from actual grassroots nationalism, even for seasoned observers. For example, the government in China has long enlisted state employees to shape online discussions, but they are now just a small component of a larger ecosystem that incorporates volunteers from the ruling party's youth apparatus as well as ordinary citizens known as "ziganwu." In official documents, the Communist Youth League described "online civilization volunteers" as people using "keyboards as weapons" to "defend the online homeland" in the ongoing "internet war."

In at least eight countries, politicians encouraged or even incentivized followers to report "unpatriotic content," harass "enemies of the state," or flood social media with comments hailing government policies—often working hand-in-hand with paid commentators and propagandists. A senior police official in Thailand invited citizens to serve as the eyes and ears of the state after the 2014 military coup, awarding $15 to those who report users for opposing the military government. Separately, over 100,000 students have been trained as "cyber scouts" to monitor and report online behavior deemed to threaten national security, while supporters of the regime wage witch hunts on Facebook, identifying and reporting other users who break strict laws against criticizing the monarchy. In Ecuador, then president Rafael Correa launched a website that sent supporters a notification whenever a social media user criticized the government, allowing progovernment commentators to collectively target political dissidents.

Bots drown out activists with nonsense and hate speech

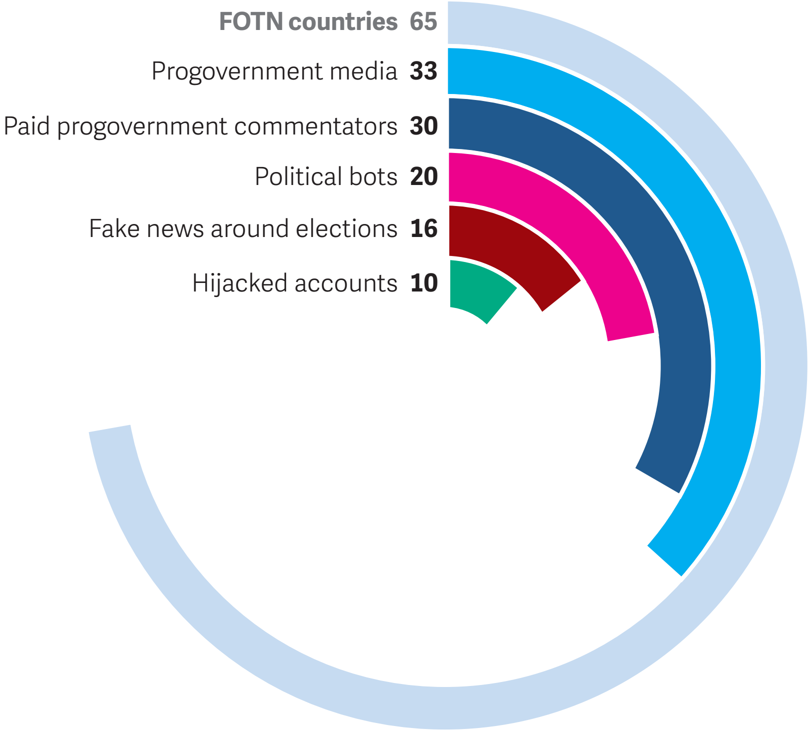
In addition to human commentators, both state and nonstate actors are increasingly creating automated accounts on social media to manipulate online discussions. In at least 20 countries, characteristic patterns of online activity suggested the coordinated use of such "bots" to influence political discourse. Thousands of fake names and profiles can be deployed with the click of a mouse, algorithmically programmed to focus on certain critical voices or keywords. They are capable of drowning out dissent and disrupting attempts to mobilize collective action online.

According to estimates by cloud services provider Imperva Incapsula, bots made up 51.2 percent of all web traffic in 2016. Many of them conduct automated tasks for commercial purposes. For example, bots now play a vital role in monitoring the health of websites, ordering products online, and pushing new content from desktop websites to mobile apps. These "good bots" are identifiable and operated by many of the largest technology companies, including Amazon, Facebook, Google, and Microsoft. Malicious bots, however, are unidentifiable by design and have made up the majority of bot activity since 2013. They can be used for hacking, spamming, stealing content, and impersonating humans in public discussions.

Studies have demonstrated the difficulty of detecting bots through any single criterion. On Twitter, bot accounts characteristically tweet frequently, retweet one another, and disseminate links to external content more often than human-operated accounts. Bots are also used in a transnational industry of artificial "likes" and followers. For example, a review of President Donald Trump's Twitter followers by *Newsweek* in May determined that only 51 percent of his 30 million followers were real.

In some cases, malicious bots have been deployed in governments' information wars against foreign adver-

PREVALENCE OF MANIPULATION TACTICS IN 65 COUNTRIES



MANIPULATION TACTICS, BY COUNTRY

Types of disinformation tactics

● –Paid progovernment commentators

● – Progovernment media and propaganda

● – Political bots

● – Fake news around elections

● – Hijacked accounts

Country	FOTN 2017 Score	Disinformation tactics										FOTN 2017 Score	Country
Angola	40	○	○	○	●	○	○	○	○	●	○	46	Lebanon
Argentina	27	○	○	●	○	○	○	○	○	●	○	54	Libya
Armenia	32	○	●	●	●	○	○	○	○	●	○	42	Malawi
Australia	21	○	○	○	○	○	○	○	○	○	●	44	Malaysia
Azerbaijan	58	●	●	●	○	●	○	○	●	○	●	39	Mexico
Bahrain	72	●	●	●	○	●	●	○	○	●	●	45	Morocco
Bangladesh	54	○	○	○	○	○	○	○	○	●	●	63	Myanmar
Belarus	64	●	●	○	○	●	○	○	○	○	○	34	Nigeria
Brazil	33	○	○	●	○	○	○	○	○	●	○	71	Pakistan
Cambodia	52	○	●	○	○	○	○	○	●	○	●	28	Philippines
Canada	15	○	○	○	○	○	○	○	●	●	●	66	Russia
China	87	●	●	○	○	●	○	●	●	●	●	53	Rwanda
Colombia	32	○	○	○	●	○	○	○	●	●	●	72	Saudi Arabia
Cuba	79	●	●	○	○	○	○	○	○	○	○	41	Singapore
Ecuador	43	●	●	●	●	●	○	○	○	○	○	25	South Africa
Egypt	68	●	●	○	○	○	○	●	●	●	○	35	South Korea
Estonia	6	○	○	○	○	○	○	○	○	○	○	43	Sri Lanka
Ethiopia	86	●	●	○	○	○	○	○	○	○	●	64	Sudan
France	26	○	○	●	●	○	●	○	●	●	●	86	Syria
Georgia	24	○	○	○	○	○	○	○	○	●	●	67	Thailand
The Gambia	67	●	●	○	●	●	○	○	○	○	○	38	Tunisia
Germany	20	○	○	○	●	○	●	●	○	●	●	66	Turkey
Hungary	29	○	●	○	○	○	○	○	○	○	○	41	Uganda
Iceland	6	○	○	○	○	○	○	○	●	○	●	45	Ukraine
India	41	○	○	○	○	○	○	○	○	●	●	69	United Arab Emirates
Indonesia	47	○	○	○	●	○	○	●	●	○	○	24	United Kingdom
Iran	85	●	●	●	○	○	○	●	●	○	○	21	United States
Italy	25	○	○	○	●	○	○	○	○	●	●	77	Uzbekistan
Japan	23	○	○	○	○	○	●	○	●	●	●	63	Venezuela
Jordan	53	○	●	○	○	○	○	○	○	●	●	76	Vietnam
Kazakhstan	62	●	●	○	○	○	○	●	○	○	○	41	Zambia
Kenya	29	●	●	●	●	○	○	○	○	○	○	56	Zimbabwe
Kyrgyzstan	37	●	○	○	○	○							

Disinformation Glossary

- **Paid progovernment commentators:** Credible reports that the government employs staff or pays contractors to manipulate political discussions online without making the sponsored nature of the content explicit.
- **Political bots:** Automated, fake accounts on social media used in coordination to amplify certain political messages.
- **Hijacked accounts:** Documented instances of progovernment hackers taking over critics' social media accounts and opposition news sites to spread disinformation.
- **Fake news around elections:** Intentionally false information engineered to resemble legitimate news, garner maximum attention, and influence voters.
- **Progovernment media and propaganda:** Online media landscape warped by frequent bribes, politicized editorial directives, or ownership takeovers by government-affiliated entities and individuals to influence political reporting.

saries and domestic opponents.

In Mexico, an estimated 75,000 automated accounts known colloquially as Peñabots have been employed to overwhelm political opposition on Twitter. When a new hashtag emerges to raise awareness about a protest or corruption scandal, government backers employ two methods to game the system in favor of President Enrique Peña Nieto. In one method, the bots promote alternative hashtags that push the originals off the top-10 list. In another method known as "hashtag poisoning," the bots flood the antigovernment hashtags with irrelevant posts in order to bury any useful information. Hashtag poisoning can have real-world consequences: Unable to access maps of police activity and safe exit routes, many peaceful protesters in Mexico were unable to flee danger zones and instead faced excessive force by the police.

Bots can also be used to smear regime opponents and promote sectarianism. In Bahrain, for example, where much of the Shiite majority has demanded political reform from the repressive Sunni monarchy, a researcher found that just over half of all tweets on the hashtag #Bahrain in a given time period consisted of anti-Shiite hate speech. Tweets featuring nearly identical language accused a prominent Shiite cleric of inciting violence against state security forces. This bot army has been mobilized in online conversations about Saudi Arabia, Yemen, and Iran, always denigrating Shiite Muslims.

Hijacked accounts spread disinformation

In at least ten countries, hackers with suspected links to the government or ruling party hijacked social media accounts and news sites in order to spread disinformation. In the Middle East, the alleged hacking of a Qatari state news site to post pro-Iranian statements attributed to high-level Qatari officials sparked an international incident. Although Qatar denied the veracity of the stories, a regional coalition led by Saudi Arabia responded with a blockade that included the obstruction of dozens of Qatari-linked news sites. Amid the hysteria, authorities in Egypt also blocked the websites of dozens of independent news outlets and human rights organizations.

> In Mexico, an estimated 75,000 automated accounts known colloquially as Peñabots have been employed to overwhelm political opposition on Twitter.

While Qatar's hacking allegations have yet to be independently confirmed, it would not be an isolated case. On the eve of Belarus's "Freedom Day" demonstration, an opposition leader and protest organizer's Facebook account was hacked in order to post fake comments discouraging people from attending the event. In Turkey, hackers have taken over the accounts of prominent journalists and activists so as to publish fake apologies in which the victims express regret for criticizing the government. Access Now reported that in Venezuela, Myanmar, and Bahrain, hackers spread disinformation through "DoubleSwitch" attacks. After gaining access to a verified account, changing the recovery email address, and altering the account handle, the hackers created a new account under the victim's name and original handle, then disseminated content from both accounts.

In at least nine countries, hackers with suspected links to the government or ruling party hijacked social media accounts and news sites to spread disinformation.

These incidents underline the role of poor cybersecurity in online manipulation. Many hackers exploit weaknesses in SMS-based two-factor authentication for social media accounts, particularly if the victim resides in a country where state-sponsored hackers may collude with state-run telecommunications companies. International tech firms have made improvements in monitoring for state-sponsored attacks, although the repeated theft or leaking of customers' personal data by cybercriminals can provide progovernment hackers with much of the confidential material they need to clear even the strongest identification hurdles.

Fake news proliferates in a new media environment

The "democratization" of content production and the centralization of online distribution channels like Twitter and Facebook has shaken up the media industry, and one unintended consequence has been the proliferation of fake news—intentionally false information that has been engineered to resemble legitimate news and garner maximum attention. Fake news has existed since the dawn of the printing press. However, its purveyors have recently developed sophisticated ways—such as gaming the algorithms of social media and search engines—to reach large audiences and mislead news consumers.

Social media are increasingly used as a primary source of news and information, but users' inability to distinguish between genuine news and lucrative or politically motivated frauds seriously reduces their value and utility. Although there is little information publicly available regarding the algorithms of Facebook, Google, Twitter, and other information gatekeepers, they have tended to promote viral or provocative articles that generate clicks, regardless of the veracity of their content. Just as upstart media organizations like BuzzFeed tailored the titles of real articles to suit Facebook's NewsFeed, enterprising Macedonian teenagers crafted click-bait headlines for fake articles in advance of the November 2016 U.S. elections, profiting immensely from Google Ads placed on their sites. Such illegitimate news content appeared on social media platforms alongside articles from legitimate outlets, with no obvious distinction between the two.

Freedom House documented prominent examples of fake news around elections or referendums in at least 16 of the 65 countries assessed. Government agents in Venezuela regularly used manipulated footage to disseminate lies about opposition protesters on social media, creating confusion and undermining the credibility of the opposition movement ahead of elections. In Kenya, users readily shared fake news articles and videos bearing the logos of generally trusted outlets such as CNN, the BBC, and NTV Kenya on social media and messaging apps in advance of the August 2017 election.

While fake news sites are not new, they are being used with increasing sophistication for political purposes. Progovernment actors in Iran have long created sites like persianbbc.ir to mimic the look of the authentic bbcpersian.com, filling them with conspiracy theories and anti-Western propaganda. More recently, Iranian hacker groups have established websites with names like BritishNews and AssadCrimes as part of more elaborate social-engineering schemes. The latter contained articles lifted from a Syrian opposition blog and was falsely registered under the name of a prominent opposition activist. Hackers created email addresses and social media profiles linking to the fake publications in order to communicate with government opponents and human rights defenders and map out their social networks. Once trust was established, the hackers targeted victims with so-called remote access trojan (RAT) programs and gained access to their devices.

Progovernment news and propaganda

The line between real news and propaganda is often difficult to discern, particularly in hyperpartisan environments where each side accuses the other of distorting facts. Societies with strong respect for media freedom and free speech allow citizens to consult a diverse range of news sources and develop an informed understanding of events. However, in over half of the countries included in the report, the online media landscape is warped by frequent bribes, politicized editorial directives, or ownership takeovers by government-affiliated entities and individuals—all of which Freedom House has observed for many years in such countries' print and broadcast sectors. The result is often an environment in which all major news outlets toe the government line. In Azerbaijan, media pluralism has been undermined by restrictions on foreign funding that leave media outlets dependent on the state-controlled domestic advertising market. In Hungary, Turkey, and Russia, the government or oligarchs with strong links to the ruling party have purchased numerous online outlets, dismissed critical journalists, and quickly altered the sites' editorial stance.

Some of the most prominent purveyors of state propaganda are governments that claim to be combating disinformation. In Cuba, where laws criminalize the dissemination of "enemy propaganda" and "unauthorized news," online media have long been dominated by state-run outlets and progovernment bloggers who defend the actions of the leadership and its foreign allies. The constitution prohibits private ownership of media outlets and allows freedom of speech and freedom of the press only if they "conform to the aims of a socialist society."

Governments in at least 14 countries actually restricted internet freedom in a bid to address various forms of content manipulation.

But in few places was the hypocritical link between state propaganda and legal restrictions on the media stronger than in Russia. Bloggers who obtain more than 3,000 daily visitors must register their personal details with the Russian government and abide by the law regulating mass media. Search engines and news aggregators were banned from including stories from unregistered outlets under a new law that took effect in January 2017. Foreign social media platforms have been pressured to move their servers within the country's borders to facilitate state control, while key local platforms have been purchased by Kremlin allies.

Diverse responses to manipulation

In a troubling trend, governments in at least 14 countries actually restricted internet freedom in a bid to address various forms of content manipulation. In Ukraine, one of the first countries to experience Russia's modern information warfare, Russian agents have operated fake Ukrainian news sites and flooded

Manipulation Armies, by the Numbers

$10
Amount a member of the Philippines' "keyboard army" can earn per day for praising President Rodrigo Duterte

6,000
Trolls enlisted by Turkey's ruling AK Party to manipulate online discussions

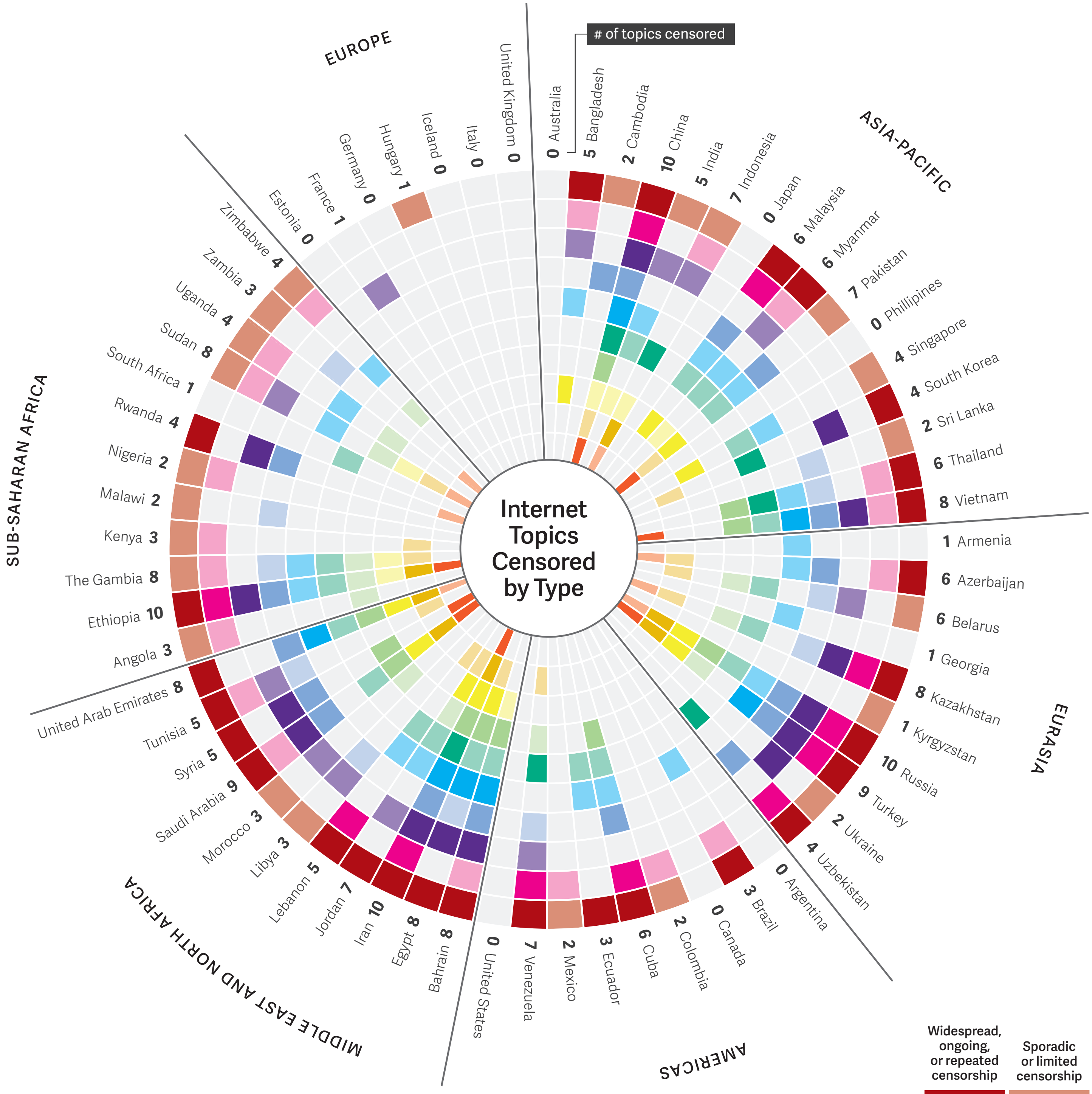
30,000
Fake accounts removed from Facebook ahead of the 2017 French elections

75,000
Automated accounts in Mexico, known colloquially as "Peñabots," employed to overwhelm political opposition on Twitter

120,000
Thai students trained as "cyber scouts" to monitor and report online behavior deemed threatening to national security

$400,000
Monthly budget of Russia's Internet Research Agency or "troll farm"

CENSORED TOPICS BY COUNTRY



	Widespread, ongoing, or repeated censorship	Sporadic or limited censorship
Criticism of Authorities	■	■
Corruption	■	■
Conflict	■	■
Political Opposition	■	■
Satire	■	■
Social Commentary	■	■
Mobilization for Public Causes	■	■
Blasphemy	■	■
LGBTI Issues	■	■
Ethnic and Religious Minorities	■	■

Censorship was reflected if state authorities blocked or ordered the removal of content, or detained or fined users for posting content on the topics considered. The chart does not consider extralegal pressures such as violence, self-censorship, or cyberattacks, even where the state is believed to be responsible.

social media with invented reports on Crimea's desire to be part of Russia, Ukrainian citizens' rejection of the European Union, and other stories that promote the Kremlin's narrative. In response, Ukrainian authorities have blocked a number of Russia-based social media platforms and search engines, joining a list of countries including China and Iran that have ordered extended bans on prominent social media services. The affected sites—Odnoklassniki, VKontakte, Yandex, and Mail.ru—were widely used by Ukrainians.

Several democratic countries are debating the appropriate response to the fake news phenomenon and, more broadly, the responsibility of intermediaries such as Google, Facebook, and Twitter to remove fraudulent or illegal content. Germany's Social Media Enforcement Law, passed in June 2017, obliges companies to take down content that is flagged as illegal in a process that lacks judicial oversight. The law is deeply problematic and may create incentives for social media companies to preemptively delete any controversial content, including legitimate speech, in order to avoid fines of up to €50 million. With similar moves proposed in Italy and the Philippines, the German law may set an unfortunate example for both democratic and repressive governments on how to use legal pressure to ensure that companies comply with local demands for censorship.

More broadly, it will take considerable time, resources, and creativity to successfully combat content manipulation and restore trust in social media in a manner that does not undermine internet and media freedom. Already, increased public awareness has resulted in pressure on internet companies to redouble their efforts to remove automated accounts and flag fake or misleading news posts. Some 30,000 fake accounts were removed from Facebook ahead of the 2017 French elections, while Google altered its search rankings to promote trusted news outlets over dubious ones. Twitter also announced that it will do more to detect and suspend accounts used for the primary purpose of manipulating trending topics.

But social media platforms and search engines are only part of the puzzle. Organizations such as First Draft News and Bellingcat provide professional and citizen journalists alike with the tools needed to verify user-generated content, monitor manipulation campaigns, and debunk fake news. More must be done to provide local, tailored solutions to the problem of manipulation in different countries. This is particularly the case in settings where many people get their news from messaging platforms like WhatsApp and Telegram, which makes false information even more difficult to detect.

State censors target mobile connectivity

Network shutdowns—defined by Freedom House as intentional restrictions on connectivity for fixed-line internet networks, mobile data networks, or both—have occurred in a growing number of countries in recent years. In the 2017 edition, 19 out of 65 countries tracked by *Freedom on the Net* had at least one network shutdown during the coverage period, up from 13 countries in the 2016 edition and 7 countries in the 2015 edition. Over the past year, authorities have often invoked national security and public safety to shut down communication networks, but in reality the pretexts have ranged from armed conflict and social unrest to peaceful protests, elections, and online "rumors" that could supposedly cause internal strife.

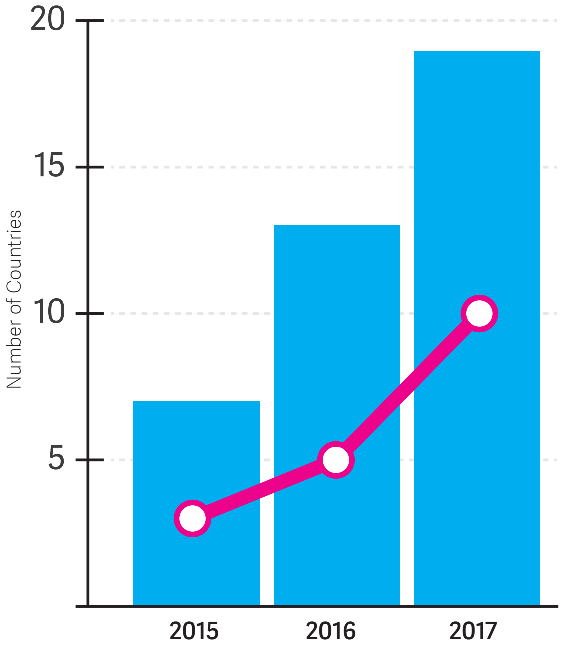
Authorities are increasingly targeting mobile service as opposed to fixed-line networks. During this report's coverage period, mobile-only disruptions were reported in 10 out of 19 countries with reported shutdowns, while incidents in most remaining countries affected mobile and fixed-line networks simultaneously. Shutdowns targeting fixed-line internet only were documented in just two countries, and they were attributed to authorities conducting tests of their ability to impose broader shutdowns in the future.

19 out of 65 countries tracked by *Freedom on the Net* had at least one network shutdown.

There are several reasons why governments may be singling out mobile connectivity. For one, mobile internet use has become the predominant mode of internet access around the world, with global traffic from mobile networks surpassing fixed-line internet traffic for the first time in late 2016. In many developing countries, the majority of internet users access the web from their mobile devices due to the increasing affordability of mobile data subscriptions and devices compared with fixed-line subscriptions. In addition, fixed-line and Wi-Fi connections are tied to specific locations or infrastructure, while mobile connections enable users to connect wherever they can get a signal, giving a mobile shutdown greater impact.

SHUTDOWNS ARE GOING MOBILE

Ten out of 19 countries specifically targeted mobile networks this year. Some countries, such as India, experienced numerous shutdown incidents that targeted either mobile, fixed, or both networks.



Mobile networks are also being targeted due to the ease with which people can use mobile devices to communicate and organize on the move and in real time, a feature that is appealing to peaceful protesters and violent terrorists alike. Targeted mobile shutdowns also leave fixed-line networks accessible for businesses and government institutions, which can help blunt the negative economic impact of the restrictions.

Mobile shutdowns cut off marginalized communities

In a troubling new trend, the authorities in at least 10 countries deliberately disrupted mobile connectivity in specific regions, often targeting persecuted ethnic and religious groups. In China, for example, Tibetan and Uighur communities have faced regular mobile shutdowns for years, most recently in a Tibetan area of Sichuan Province where officials sought to prevent the spread of news about a Tibetan monk's self-immolation to protest government repression. In Ethiopia, the government shut down mobile networks for nearly two months as part of a state of emergency declared in October 2016 amid large-scale antigovernment demonstrations by the disenfranchised Oromo and Amhara populations.

For many of the communities affected by such localized shutdowns, mobile service is the only affordable or available option for internet connectivity due to underdeveloped fixed-line infrastructure in remote regions. Consequently, the shutdowns can effectively silence a specific community, not only minimizing their ability to call attention to their political and social grievances, but also diminishing their economic development and educational opportunities.

In addition to their growing frequency, the shutdowns initiated over the past year have been longer in duration, with at least three countries—Lebanon, Bahrain, and Pakistan—experiencing regional shutdowns that lasted more than one year. In Lebanon, 160,000 residents of the northeastern border town of Arsal, many of whom are Syrian refugees, have been completely cut off from mobile internet for over two years as a security measure amid frequent clashes between the military and extremist militants. Since June 2016, Bahraini authorities have required telecom companies to disable mobile and fixed-line connections during nightly curfews in the town of Duraz, where supporters of a prominent Shiite cleric were protesting persecution by the Sunni monarchy.

Service disruptions coincide with elections, special events

Mobile shutdowns have also been deployed to stifle opposition groups during contentious elections periods. During Zambia's August 2016 presidential election, mobile broadband networks were reportedly disrupted for up to 72 hours in opposition-held regions following protests by opposition supporters who accused the electoral commission of fraud. Similarly in the Gambia, networks were shut down on the eve of a presidential election in December 2016, though in a surprise victory for democracy, the tactic failed to secure the reelection of authoritarian incumbent Yahya Jammeh, who had been in power for nearly 22 years.

Some governments restricted mobile communications during large events out of concern that they could be used to harm public security. In the past year, the authorities in at least three cities in the Philippines directed telecom providers to shut down mobile networks during public festivals and parades; Philippine officials had previously restricted mobile connectivity during the pope's visit in 2015. Though the shutdown directives were all narrow in scope and duration and communicated to the public, the repeated events have helped normalize shutdowns as a legitimate government measure, despite their disproportionate nature and profound effect on freedom of expression.

App restrictions and price increases curb mobile access

Indirect methods of control over mobile connectivity typically receive less attention than network shutdowns, but they can have the same effect of disrupting essential communications. In keeping with a trend highlighted in *Freedom on the Net 2016*, popular mobile-specific apps were repeatedly singled out for restrictions during the past year. WhatsApp remained the most targeted communication tool, experiencing disruptions in 12 of the 65 countries assessed. In Turkey, for example, the authorities regularly throttled traffic for WhatsApp to render it virtually inaccessible during politically charged events, while officials in Zimbabwe blocked it for several hours during large antigovernment protests.

Artificial regulation of mobile data prices was also used to indirectly restrict access. After WhatsApp was unblocked in Zimbabwe, the government reportedly hiked the cost of mobile data plans by 500 percent to limit further civic organizing. When mobile networks are not shut down altogether in India's restive state of Jammu and Kashmir, the authorities often suspend pay-as-you-go mobile data plans, which most acutely affects low-income residents who cannot afford subscriptions.

Governments restrict live video, especially during protests

Internet users faced restrictions or attacks for streaming live video in at least nine countries. Live broadcasting tools and channels were subject to blocking, and several people were detained to halt real-time coverage of antigovernment demonstrations.

Streaming video in real time has become more widely popular since the launch of a now-defunct mobile app, Meerkat, in early 2015. Many apps have since added live-streaming features, and deliver content to large global networks. The ability to stream live content directly from a mobile device without the need for elaborate equipment or a distribution strategy has made the technology more accessible. Dedicated news outlets and other content producers also continue to stream live content from their own websites, and some are now doing so in conjunction with apps and social media platforms. Often this allows them to bypass regulations specific to traditional broadcasters, and to reach new audiences.

People stream all sorts of things, from cultural events to everyday interactions. But live video is an important tool for documenting state abuse. In Armenia, digital journalist Davit Harutyunyan reported that police officers assaulted him and broke his equipment to stop him from sharing live footage of police attacking other journalists as they covered antigovernment demonstrations. Even in democracies such as the United States, live-streaming tools have become critical to social justice causes. In one case, live video broadcast on social media by the girlfriend of black motorist Philando Castile after he was fatally shot by police in Minnesota in July 2016 helped bring the incident to nationwide prominence.

After WhatsApp was unblocked in Zimbabwe, the government reportedly hiked the cost of mobile data plans by 500 percent.

Journalists have embraced live streaming, and it has developed into an accessible alternative to broadcast television channels, especially in countries whose traditional media outlets do not tell the full story. Before May 2017 elections in Iran, reformist figures who supported President Hassan Rouhani's quest for a second term used Instagram Live to cover campaign events and nightly programs despite being sidelined by the state broadcaster IRIB, which has a virtual monopoly on traditional broadcast media. In a testament to the success of this strategy, the protocol that allows Instagram users to stream video was briefly blocked, and when it became accessible again, the hard-line candidate Ebrahim Raisi embraced the platform as well.

Government censors have had to adapt to the trend. In Bahrain, the information ministry banned news websites from streaming live video altogether in July 2016. Others, like Iran when it blocked Instagram, used more ad hoc methods to disrupt live streaming when it was already in progress. Venezuelan regulators ordered service providers to block three websites that broadcast live as tens of thousands of protesters marched against President Maduro in April 2017.
In June, live coverage of anticorruption protests in Russia was interrupted when the electricity supply

to the office of opposition leader Aleksey Navalny was intentionally cut off, leaving his YouTube channel Navalny Live without light and sound.

The public use of smartphones to document events in real time turned ordinary internet users into citizen journalists—and easy targets for law enforcement officials. At least two video bloggers were arrested and a third was fined for broadcasting antigovernment Freedom Day protests in Belarus; local colleagues observed that they lack the institutional support and legal protections of their professional counterparts. Yet a Belarusian animal rights worker was fined in a separate case because a court found that her live video from a rescue shelter violated a law governing mass media broadcasts.

China, Iran, and Syria consistently produce the most pervasive attacks by state-affiliated actors, but the weakly regulated market for military-grade cyber tools has lowered the financial bar for engaging in such activity.

Live streaming has earned notoriety for enabling users to broadcast nudity, drug use, or even violence. Some countries restricted real-time broadcasts to curb obscenity, but the effects extended to journalism and digital activism. Singaporean streaming app Bigo Live was shuttered for a month in Indonesia until it brokered a deal with the government to limit streaming activity that violates Indonesia's broad bans on obscene or otherwise "negative" content. And in China, police in southern Guangdong Province shut down hundreds of live-streaming channels during a purge of pornography and other illegal content—a category that includes banned news and commentary.

Cyberattacks hit news outlets, opposition, and rights defenders

A wave of extraordinary cyberattacks caused significant disruptions and data breaches over the past year. Millions of unsecured "internet of things" devices like online baby monitors and coffee machines were hijacked and used to strike the Domain Name System provider Dyn with DDoS attacks, resulting in outages at some of the web's most popular platforms. Showcasing increasingly bold political motivations, hackers also infiltrated the servers of the U.S. Democratic National Committee in 2016 and the campaign of French presidential candidate Emmanuel Macron in 2017. While these intrusions made headlines, similar attacks have hit human rights defenders, opposition members, and media outlets around the world at a higher rate than ever before, often with the complicity of their own governments. Technical attacks against government critics were documented in 34 of the 65 countries assessed, up from 25 in the 2016 edition. Rather than protecting vulnerable users, numerous governments took additional steps to restrict encryption, which further exposed their citizens to cyberattacks.

Security vulnerabilities present government-affiliated entities with an opportunity to intimidate critics and censor dissent online while avoiding responsibility for their actions. It is often difficult to identify with certainty those responsible for anonymous cyberattacks, including when suspicions of government involvement are high. The likes of China, Iran, and Syria consistently produce the most pervasive attacks by state-affiliated actors, but the dynamic and weakly regulated market for military-grade cyber tools has lowered the financial bar for engaging in such activity. Even local law enforcement agencies can now persecute their perceived foes with limited oversight. In fact, technical attacks currently represent the second most common form of internet control assessed by Freedom House, behind arrests of users for political or social content.

Activists and media outlets often have only minimal defenses against technical attacks, which can result in censorship, surveillance, content manipulation, and intimidation. Many attacks still go unreported, especially when there are no clear channels to document such incidents, or when the victims fear reprisals for speaking out.

Independent websites are temporarily disabled

Activists and media outlets in at least 18 countries reported service interruptions caused by cyberattacks—especially DDoS attacks, in which simultaneous requests from many computers overwhelm and disable a website or system. These types of attacks have become an easy and relatively inexpensive way to retaliate against those who report on sensitive topics.

Eurasia and Latin America were the regions that featured the most successful attacks. In Azerbaijan, the independent online news platform Abzas reported receiving a series of DDoS attacks that lasted for several days in January 2017. The website was inaccessible until it migrated to a more secure host. A forensic investigation tracked the IP addresses that launched the attack to several Azerbaijani government institutions. Venezuelan news and civil society organizations noted a surge in the number of reported attacks in early 2017. These included an attack against Acción Solidaria, an organization that supports people living with HIV/AIDS in the country. The disruption temporarily prevented the group from informing users about the distribution of medicines.

Hacking enables surveillance of reporters and dissidents

Victims reportedly had their devices or accounts hacked, with suspected political motives, in at least 17 countries. The threat of surveillance can have a chilling effect on the work of journalists, human rights defenders, and opposition political activists, who were specifically targeted in a number of cases during the past year.

Large-scale phishing campaigns such as "Nile Phish" in Egypt attempted to obtain sensitive information from human rights organizations through deceitful emails. In the United Arab Emirates (UAE), spyware developed by the Israeli firm NSO—which says it only markets the technology to law enforcement and intelligence agencies—was employed against human rights defender Ahmed Mansoor, echoing previous reports on government contracts with the Italian company Hacking Team to monitor rights activists.

NSO spyware was also used against prominent Mexican journalists, human rights lawyers, and activists, who received highly personalized and often intimidating messages. One of the many targets was a lawyer representing parents of 43 student protesters who disappeared in 2014. Days after he clicked on a link in a text message purportedly seeking his help, a recording of a call between him and one of the parents appeared online.

Encryption legislation opens a back door to abuse

Rather than taking measures to protect businesses, citizens, and vulnerable groups from these cybersecurity threats, many governments are moving in the opposite direction.

Technical Attacks

Technical attacks were documented against opposition, government critics, independent media, and human rights activists in 34 out of 65 countries assessed. These were the three most common effects.

WEBSITES TAKEN OFFLINE

Reported in

18 countries

Hackers hit the websites of *El Pitazo* and *Caraota Digital* during Venezuela's political turmoil, forcing the news outlets to post stories directly on their social media accounts.

Abzas, a news site in Azerbaijan, became inaccessible from DDoS attacks immediately after publishing articles critical of the government.

PRIVATE DATA STOLEN OR ONLINE ACTIVITIES MONITORED

Reported in

17 countries

At least 22 journalists, human rights lawyers, and activists were targeted with government spyware in Mexico.

Seven human rights organizations currently on trial in Egypt received over 90 phishing attempts in a coordinated scheme to obtain sensitive information

WEBSITES AND SOCIAL MEDIA ACCOUNTS VANDALIZED

Reported in

16 countries

Unknown hackers defaced the website of the Lebanese Medical Association for Sexual Health shortly after the organization launched a pro-LGBTI campaign.

In Belarus, individuals hijacked the Facebook account of a protest organizer and posted messages discouraging his followers from attending.

Restrictions on encryption continued to expand, perpetuating a trend that *Freedom on the Net* has tracked for a number of years. At least six countries—China, Hungary, Russia, Thailand, the United Kingdom, and Vietnam—recently passed or implemented laws that may require companies or individuals to break encryption, offering officials so-called backdoor access to confidential communications.

Encryption scrambles data so that it can only be read by the intended recipient, offering an essential layer of protection for activists and journalists who need to communicate securely. But even democratic governments often perceive it merely as a tool to shield terrorist and other criminal activity from law enforcement agencies.

European countries have been quick to legislate in the wake of terrorist attacks, introducing measures that could compromise security for everyone. Anti-terrorism legislation passed in Hungary in July 2016 requires providers of encrypted services to grant authorities access to client communications. The United Kingdom's Investigatory Powers Act, passed in November 2016, could be used to require companies to "remove electronic protection" from communications or data where technically feasible. "Real people often prefer ease of use ... to perfect, unbreakable security," Home Secretary Amber Rudd said in July 2017. But UN special rapporteur David Kaye has found that encryption and anonymity are essential for upholding free expression and the right to privacy.

Other governments have cited cybersecurity and counterterrorism priorities to justify measures that clearly grant state agencies the power to surveil activists and journalists in the context of harsh crackdowns on dissent. Recent amendments to Thailand's computer crimes law that could compel service providers to "decode" computer data are particularly concerning. Privacy International has challenged Microsoft for trusting the country's national root certificates by default, potentially enabling the military government to falsify website credentials, capture users' log-in details, and downgrade encrypted connections. Similar concerns had been raised in the past over Chinese-issued root certificates and the potential for abuse. In repressive countries like these, private messages are often used to prosecute government critics. A Thai military court sentenced a political activist to more than 11 years in prison in January 2017 based partly on transcripts that supposedly documented a private Facebook Messenger exchange.

How requirements for intermediaries to decrypt all communications will work in practice remains unclear, especially in cases of end-to-end encryption, in which decryption keys are held on the users' devices rather than on a company's servers. A low level of technical literacy among policymakers has often translated into legislation that is problematic in terms of both human rights and implementation. In Kazakhstan, for example, moves to facilitate government monitoring of encrypted traffic through a "National Security Certificate" were shelved after authorities realized the law's impracticalities.

New cybersecurity tools offer some hope for mitigation

Despite these often problematic regulations from governments, private companies are attempting to provide customers with improved security measures. Google has signaled its intention to roll out further protections against "man-in-the-middle" attacks on its Chrome web browser. Like Facebook, Microsoft, Twitter, and others, the company also alerts users who it suspects are victims of an attack by state-sponsored hackers.

While commercial protection can be expensive, some private initiatives have offered free protection for news outlets and human rights sites that cannot afford commercial fees. Examples include Project Shield (Google), Project Galileo (Cloudflare), and Deflect. In one case, Project Shield helped the Angolan independent news site *Maka Angola* to successfully fend off recurring DDoS attacks.

Such services can assist in combating some of the most pervasive attacks, but civil society organizations and independent media outlets still struggle to keep up with the overwhelming array of tactics used by their opponents in cyberspace, let alone build up the necessary awareness and capacity to proactively prevent and mitigate these threats.

VPNs face rise in both usage and restrictions

VPNs channel an internet user's entire connection through a remote server, often in a different country, enabling access to content that is blocked domestically; some also encrypt or hide users' activity from hackers or internet service providers (ISPs). Six countries—Belarus, China, Egypt, Russia, Turkey, and the UAE—stepped up efforts to control these tools in the past year, by either passing legislation that bans censorship circumvention or blocking websites or

KEY INTERNET CONTROLS BY COUNTRY

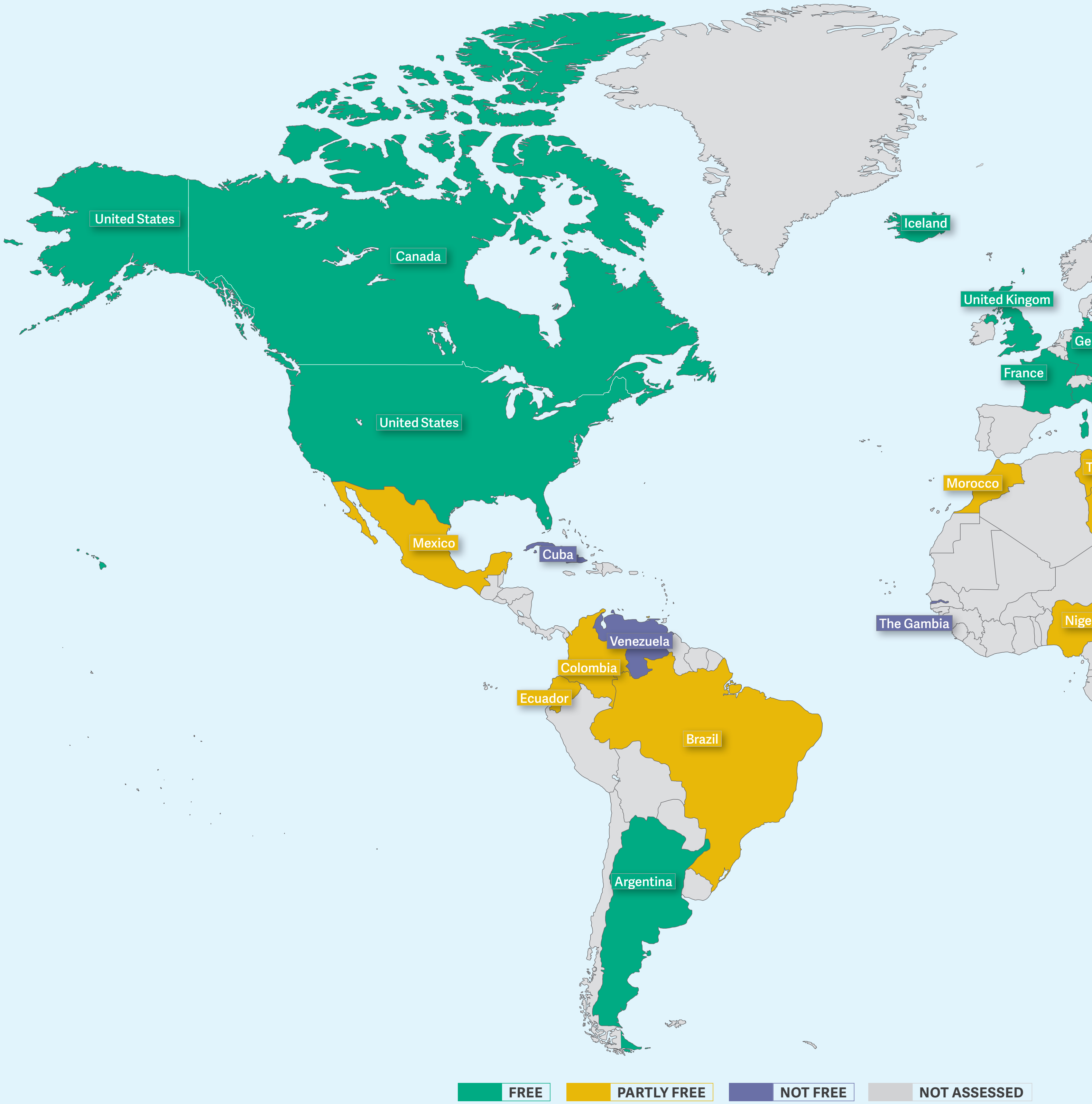
Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2016 to May 2017; cells with an asterisk (*) represent events that occurred after the coverage period until September 2017, when the report was sent to print. The Key Internet Controls reflect restrictions on political, social, or religious content. For a full explanation of the methodology, see page 35.

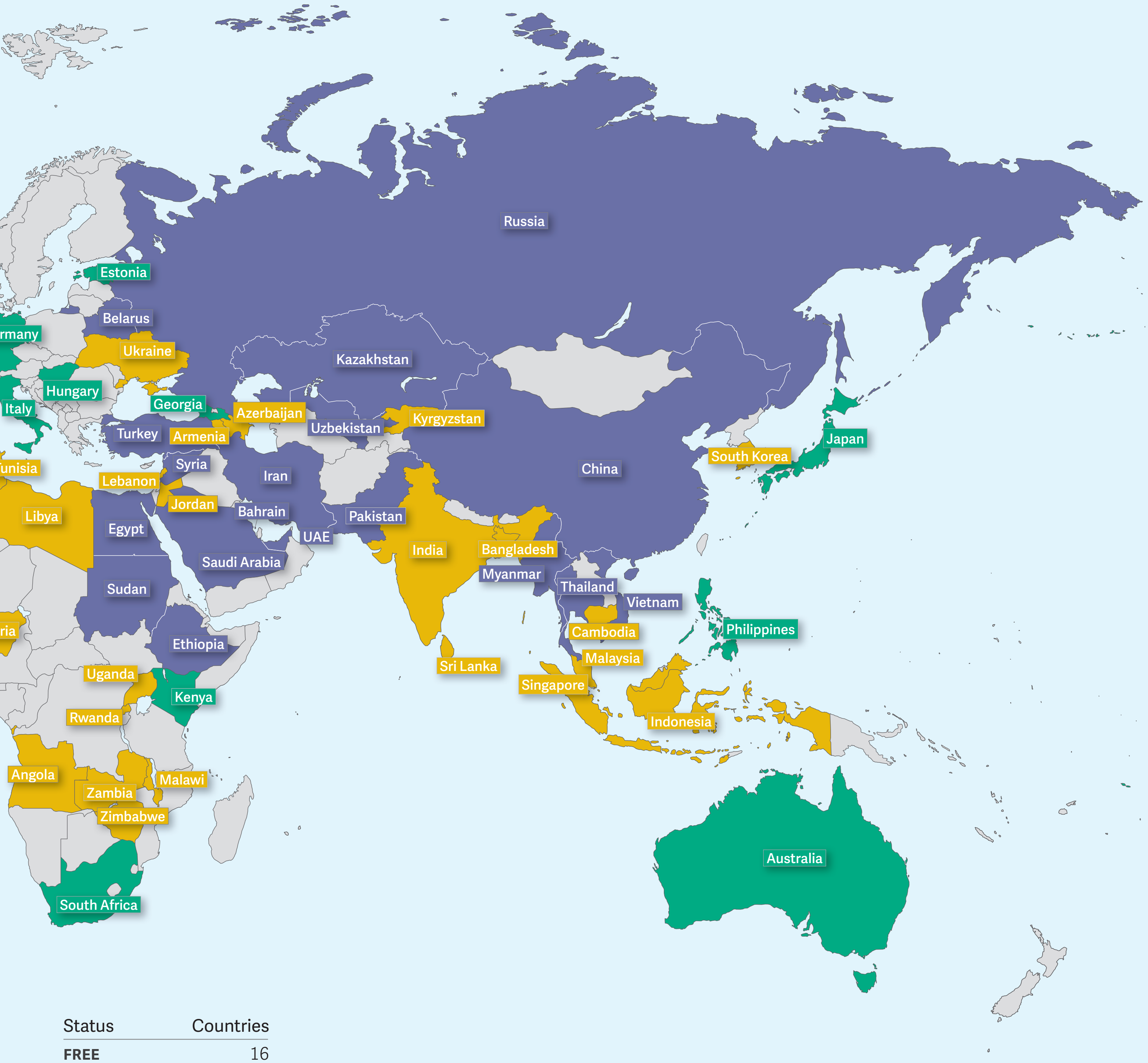
NO KEY INTERNET CONTROLS OBSERVED	FOTN Score
Australia	21
Canada	15
Colombia	32
Estonia	6
Iceland	6
Japan	23
South Africa	25

Types of key internet controls

COUNTRY	# KICs employed	Social media or communications apps blocked	Political, social, or religious content blocked	Localized or nationwide ICT shutdown	Progovernment commentators manipualte online discussions	New law or directive increasing censorship or punishment passed	New law or directive increasing surveillance or restricting anonymity passed	Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content	Blogger or ICT user physically attacked or killed (including in custody)	Technical attacks against government critics or human rights organizations	FOTN SCORE
Angola	1					■					40
Argentina	1									■	27
Armenia	3	■							■	■	32
Azerbaijan	9	■	■	■	■	■	■	■	■	■	58
Bahrain	7	■	■	■	■			■	■	■	72
Bangladesh	4	■	■	■				■			54
Belarus	7		■	■	■		■	■	■	■	64
Brazil	3	■						■	■		33
Cambodia	3		■					■		■	52
China	9	■	■	■	■	■	■	■	■	■	87
Cuba	5	■	■		■			■	■		79
Ecuador	4				■	■			■	■	43
Egypt	7	■	■	■	■			■	■	■	68
Ethiopia	9	■	■	■	■	■	■	■	■	■	86
France	3					■	■			■	26
The Gambia	7	■	■	■	■			■	■	■	67
Georgia	1	■									24
Germany	1					★	■				20
Hungary	2						■		■		29
India	5	■	■	■				■	■		41
Indonesia	7	■	■			■	■	■	■	■	47
Iran	6	■	■		■			■	■	■	85
Italy	0						★				25
Jordan	4	■	■					■	■		53
Kazakhstan	7	■	■	■	■		■	■		■	62
Kenya	2				■	★		■			29
Kyrgyzstan	1		★		■						37
Lebanon	4		■	■				■		■	46
Libya	1			■							54
Malawi	1					■					42
Malaysia	4	■	■		■			■			44
Mexico	4				■			■	■	■	39
Morocco	4	■			■			■		■	45
Myanmar	5				■		■	■	■	■	63
Nigeria	1							■			34
Pakistan	7		■	■		■	■	■	■	■	71
Phillipines	3			■	■					■	28
Russia	8	■	■		■	■	■	■	■	■	66
Rwanda	5		■		■	■		■	■		53
Saudi Arabia	6	■	■		■			■	■	■	72
Singapore	2					■		■			41
South Korea	2		■					■			35
Sri Lanka	1		■								43
Sudan	3				■			■		■	64
Syria	6		■	■	■			■	■	■	86
Thailand	6		■		■	■	■	■	■		67
Tunisia	2							■		■	38
Turkey	7	■	■	■	■	■		■		■	66
Uganda	3							■	■	■	41
Ukraine	8	■	■	■	■	■		■	■	■	45
United Arab Emirates	7	■	■		■	■		■	■	■	69
United Kingdom	1						■				24
United States	1								★	■	21
Uzbekistan	6	■	■		■			■	■	■	77
Venezuela	6	★	■		■	■		■	■	■	63
Vietnam	6		■	■	■			■	■	■	76
Zambia	2			■				■			41
Zimbabwe	2	■						■			56
June 2016-May 2017 coverage period		25	31	19	30	17	14	42	30	34	

FREEDOM ON THE NET 2017

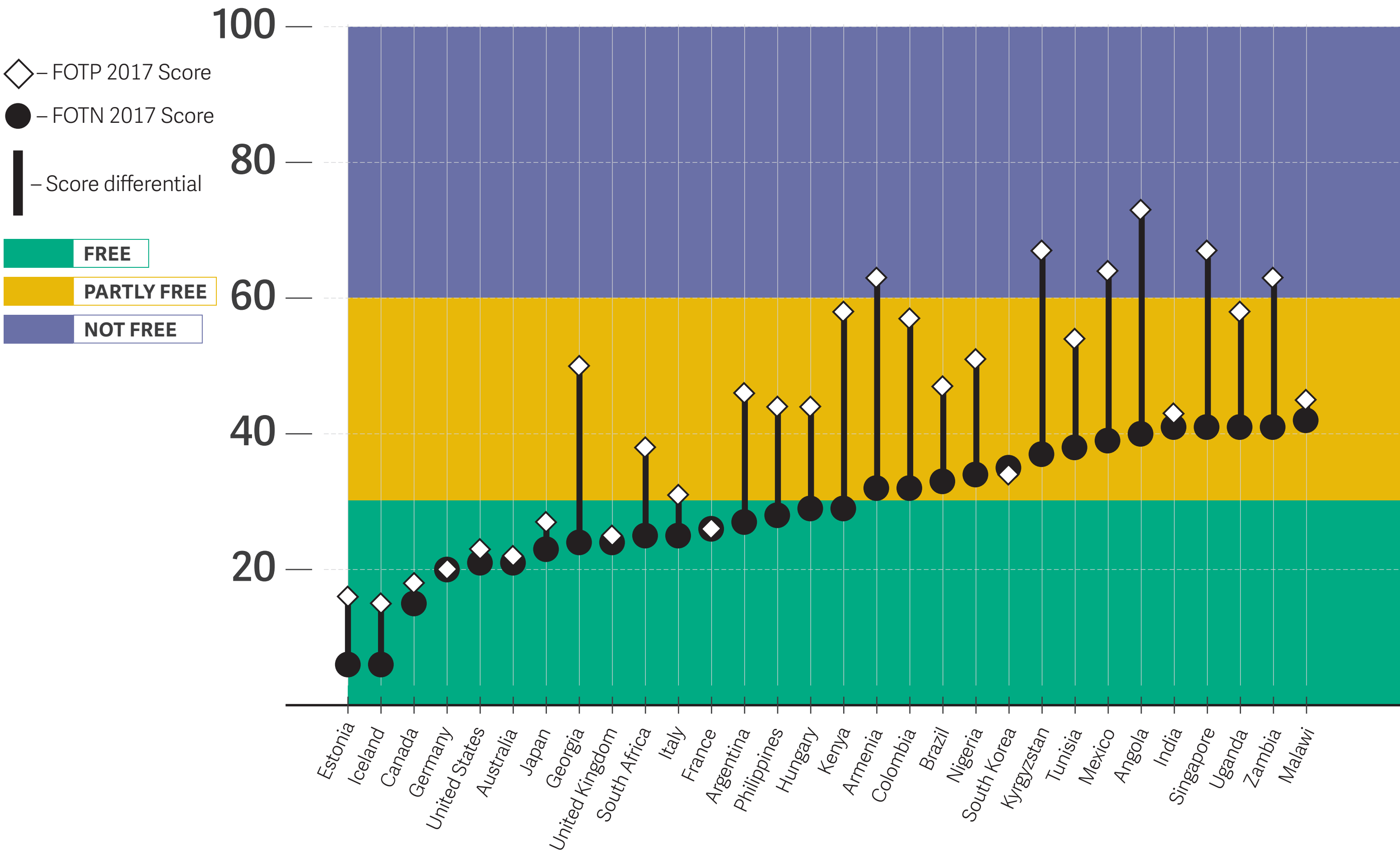




Status	Countries
FREE	16
PARTLY FREE	28
NOT FREE	21
Total	**65**

Freedom on the Net 2017 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.

INTERNET FREEDOM VS. PRESS FREEDOM

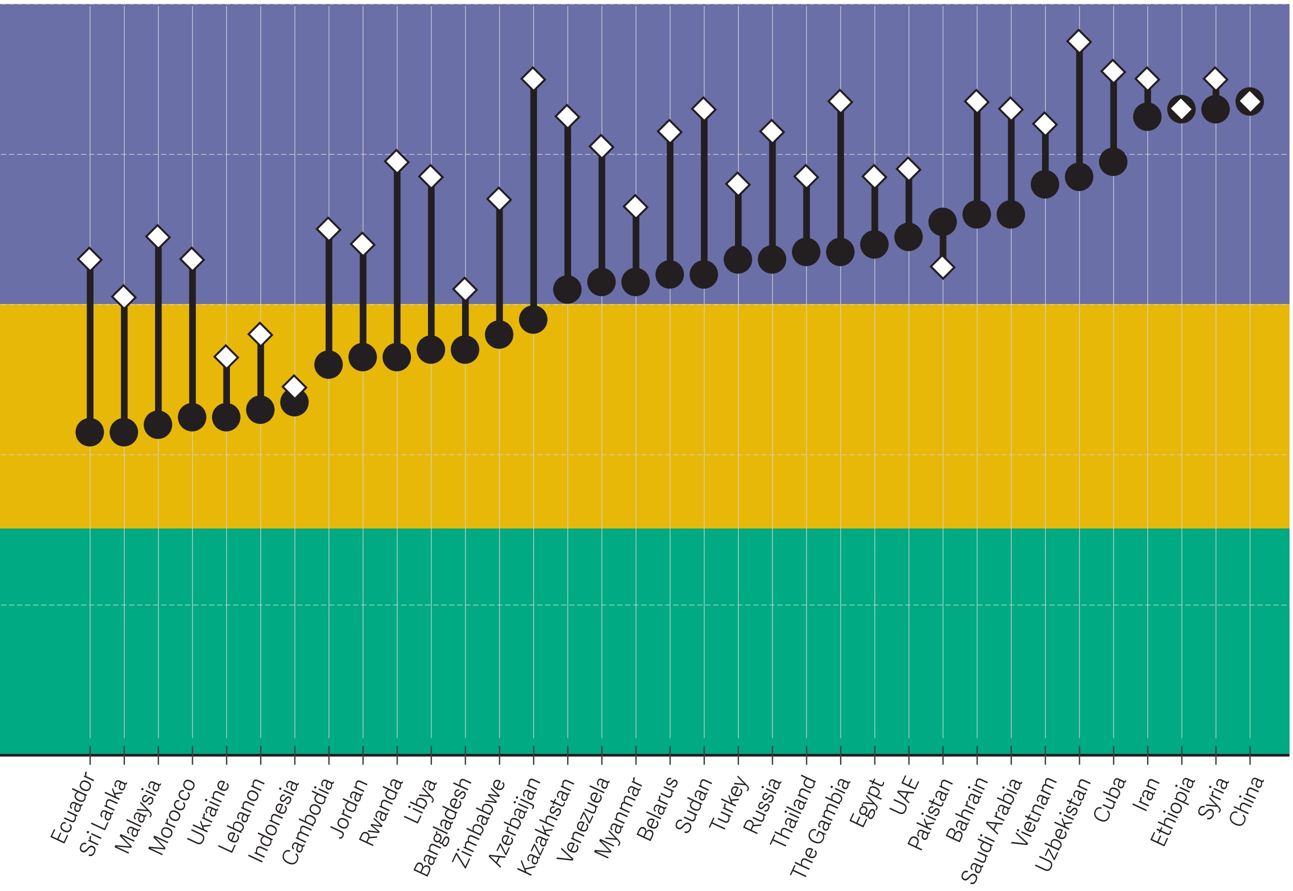


network traffic associated with VPNs. Such crackdowns often follow periods of aggressive censorship that prompt users to seek out ways to bypass the new information restrictions. The government in Egypt, which began blocking independent news websites for the first time in December 2015, censored at least five websites offering VPNs in 2017.

Campaigns against VPNs are unpopular and difficult to enforce. Many people depend on VPNs for different functions, including corporate employees accessing remote file servers and security-conscious internet users logging onto open Wi-Fi networks in public. In countries that block international news and information, local scientists, economists, and even government officials rely on VPNs to stay informed.

For this reason, no country has sought to ban VPNs completely. Instead, the most repressive states are moving toward a two-tier system that would authorize certain VPNs for approved uses and ban the rest. Even if VPN traffic proves impossible to regulate comprehensively, states can steer users toward domestic providers that are more likely to cooperate with local law enforcement and security agencies, and create laws to penalize anyone caught using a secure connection for the wrong reason.

Chinese authorities passed a series of regulations in the past year, first to license VPN providers, then requiring ISPs to block those that are unlicensed; in July 2017, Apple informed several VPN operators that their apps were no longer accessible through the company's Chinese app store because they were not in compliance. In the UAE, internet users and businesses scrambled to understand the implications of new amendments to the cybercrime law, which prescribed heavy fines and possible prison terms for the misuse of VPNs to commit fraud or crime. Separately, Russia passed a law obliging ISPs to block websites offering VPNs that can be used to access banned content; Russian authorities raided the local offices and seized servers belonging to one foreign VPN provider, Private Internet Access, in 2016. VPNs have been periodically



In the majority of the 65 countries featured in this report, the internet is significantly more free than news media in general. This difference is evident from the comparison between a country's score on *Freedom on the Net* 2017 and its score on Freedom House's *Freedom of the Press* 2017 index. The latter examines access to news content in any medium, including the internet, while the former focuses on access to the internet for any purpose, including news reporting or consumption.

Only two countries—South Korea and Pakistan—have worse scores for internet freedom than for press freedom, in part because individuals are accused of wrongdoing based on social media posts. In South Korea, penalties for defamatory speech carry heavier penalties online than off.

Countries scoring in the "Partly Free" range in *Freedom on the Net* 2017 have the largest average gap between the two indexes compared with countries in the "Free" and "Not Free" ranges, reflecting much greater internet freedom than press freedom. These "Partly Free" countries also have the lowest average internet penetration rates, an indication that their governments may move to restrict the internet once more residents become active online.

restricted in at least nine other countries, including Iran, where government authorities reportedly created their own VPN tools that allowed users to access banned content but subjected all of their activities to state monitoring.

Some VPNs are harder to monitor and block, offering stronger security protocols and strict policies against exposing user data. But repressive governments specifically target the more secure tools. Tor, a project that encrypts and anonymizes web traffic by routing it through a complex network of volunteer computers, was subject to new blocking orders amid tightening censorship in Belarus, Turkey, and Egypt. Blocking orders may pertain to the website where users download dedicated software required to access the Tor network, or to traffic from the computers that make up the network itself. Such measures may not eradicate Tor from any one country, but they do make it harder for the general population to access. Users who could not reach the website in the past year continued to share options for downloading the software by email—but those seeking access have to know whom to ask.

Physical attacks on netizens and online journalists spread globally

Physical attacks in reprisal for online activities were reported in 30 countries, up from 20 in the 2016 edition of *Freedom on the Net*. In eight countries, people were murdered for writing about sensitive subjects online. And in four of those countries—Brazil, Mexico, Pakistan, and Syria—such murders have occurred in each of the last three years. The most frequent targets seem to be online journalists and bloggers covering politics, corruption, and crime, as well as people who express religious views that may contrast with or challenge the views of the majority. Perpetrators in most cases remained unknown, but their actions often aligned with the interests of politically powerful individuals or entities.

In eight countries, people were murdered for writing about sensitive subjects online.

Physical violence is a crude but effective censorship tactic, especially in countries where prominent websites provide a key outlet for independent investigative reporting, and where the traditional media are often affiliated with the government. Pavel Sheremet, an investigative journalist with the *Ukrayinska Pravda* website in Ukraine, was killed by a bomb planted in his vehicle in Kyiv in July 2016. A year later, the murder remained unsolved, and local journalists have exposed serious flaws in the investigation carried out by the Ukrainian authorities.

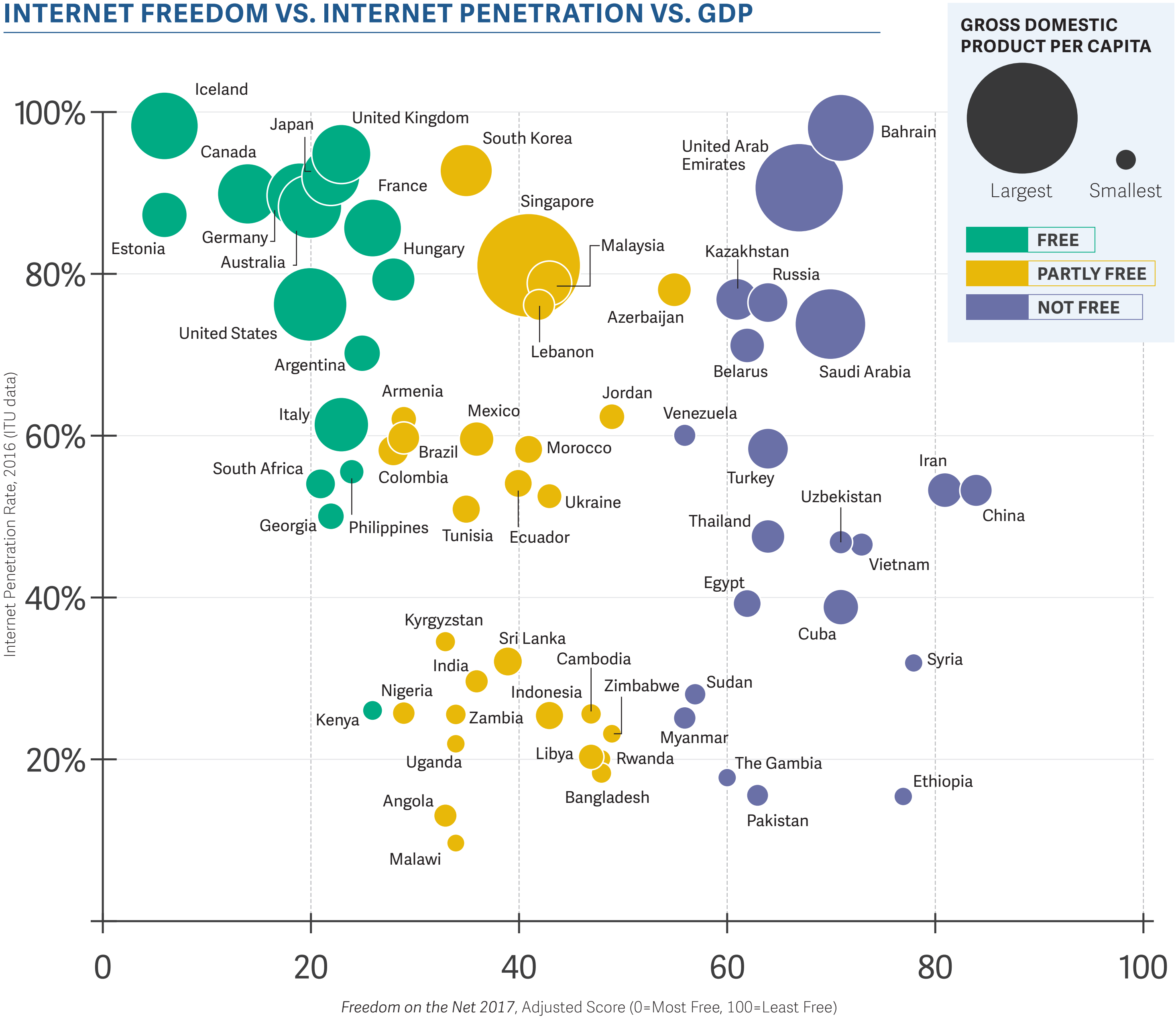
Journalists in some countries use informal social media channels to supplement or amplify their more formally published work, attracting reprisals. Soe Moe Tun, a print journalist with the *Daily Eleven* newspaper in Myanmar, was beaten to death less than a week after he republished digital images of his reporting notebooks on Facebook. The notes named individuals who allegedly colluded in illegal logging in the northwestern Sagaing region.

Assailants in several reported cases sought to remove online content. Gertrude Uwitware, a broadcast journalist in Uganda, was abducted for eight hours in April 2017 by unknown perpetrators. They ordered her to delete social media posts in which she had expressed support for an academic who was jailed the same month for calling authoritarian president Yoweri Museveni "a pair of buttocks" online.

Religious groups are also adapting to the internet, and opinions once shared within a restricted circle of acquaintances are more likely to attract the attention of extremists who monitor social media for opportunities to punish perceived insults or apostasy. In Pakistan, where a court recently sentenced an internet user to death for committing blasphemy on Facebook, a student in Khyber Pakhtunkhwa Province was killed on campus by a mob that accused him of posting blasphemous content online. In September 2016, Christian writer Nahed Hattar was shot dead outside a courthouse in Jordan, where he was on trial for insulting Islam on Facebook with a cartoon satirizing terrorists' vision of heaven. Such attacks often succeed in silencing more than just the victim, encouraging wider self-censorship on sensitive issues like religion.

The state's failure to punish perpetrators of reprisal attacks for online speech perpetuates a cycle of impunity. But the government's harmful role was even more direct in seven countries where individuals detained as a result of their online activities reported that they were subjected to torture. They included Bahrain, where human rights activist Ebtisam al-Saegh said she was sexually assaulted by security agents after her May 2017 arrest for criticizing the state on Twitter.

INTERNET FREEDOM VS. INTERNET PENETRATION VS. GDP



The figure above depicts the relationship between internet freedom, internet access, and a country's gross domestic product (GDP) per capita. The x-axis considers a country's score in the 2017 edition of *Freedom on the Net*, adjusted to exclude aspects related to internet access. Levels of internet penetration are plotted against the y-axis, using 2016 statistics from the United Nations International Telecommunication Union (ITU). Finally, the size of each plot is indicative of its GDP per capita (at purchasing power parity, PPP), according to the latest figures from the World Bank.

While wealth generally translates to greater access, neither are a decisive indicator of free expression, privacy, or access to information online, as evidenced by the range of internet freedom environments represented at the top of the chart. The Gulf countries lead a cluster of rentier economies investing in high-tech tools to restrict online freedoms. Meanwhile, as "partly free" countries in sub-Saharan Africa and Southeast Asia continue to develop, they would be wise to consider a free and open internet as a mechanism for a prosperous, diversified economy.

65 COUNTRY SCORE COMPARISON

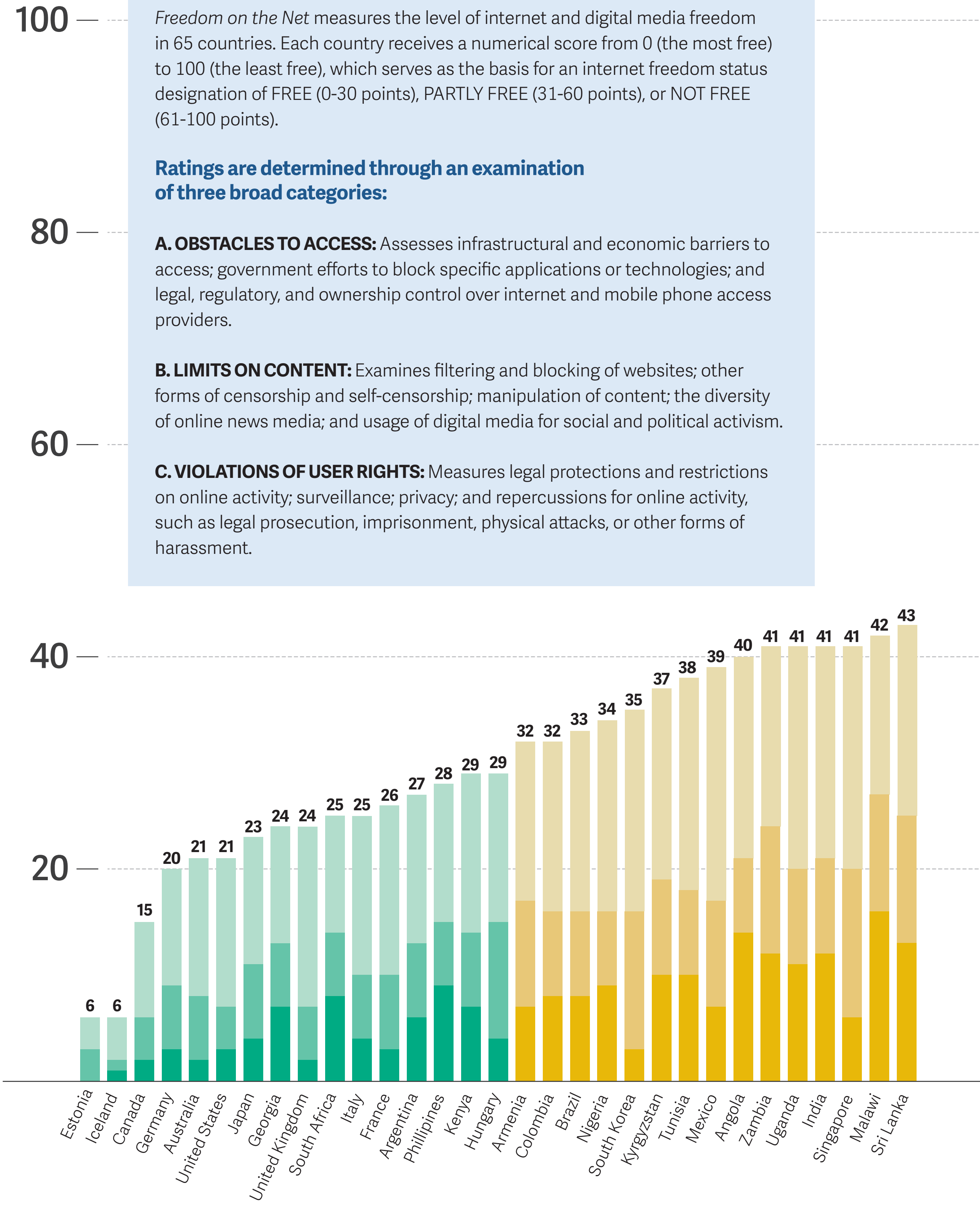
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points), or NOT FREE (61-100 points).

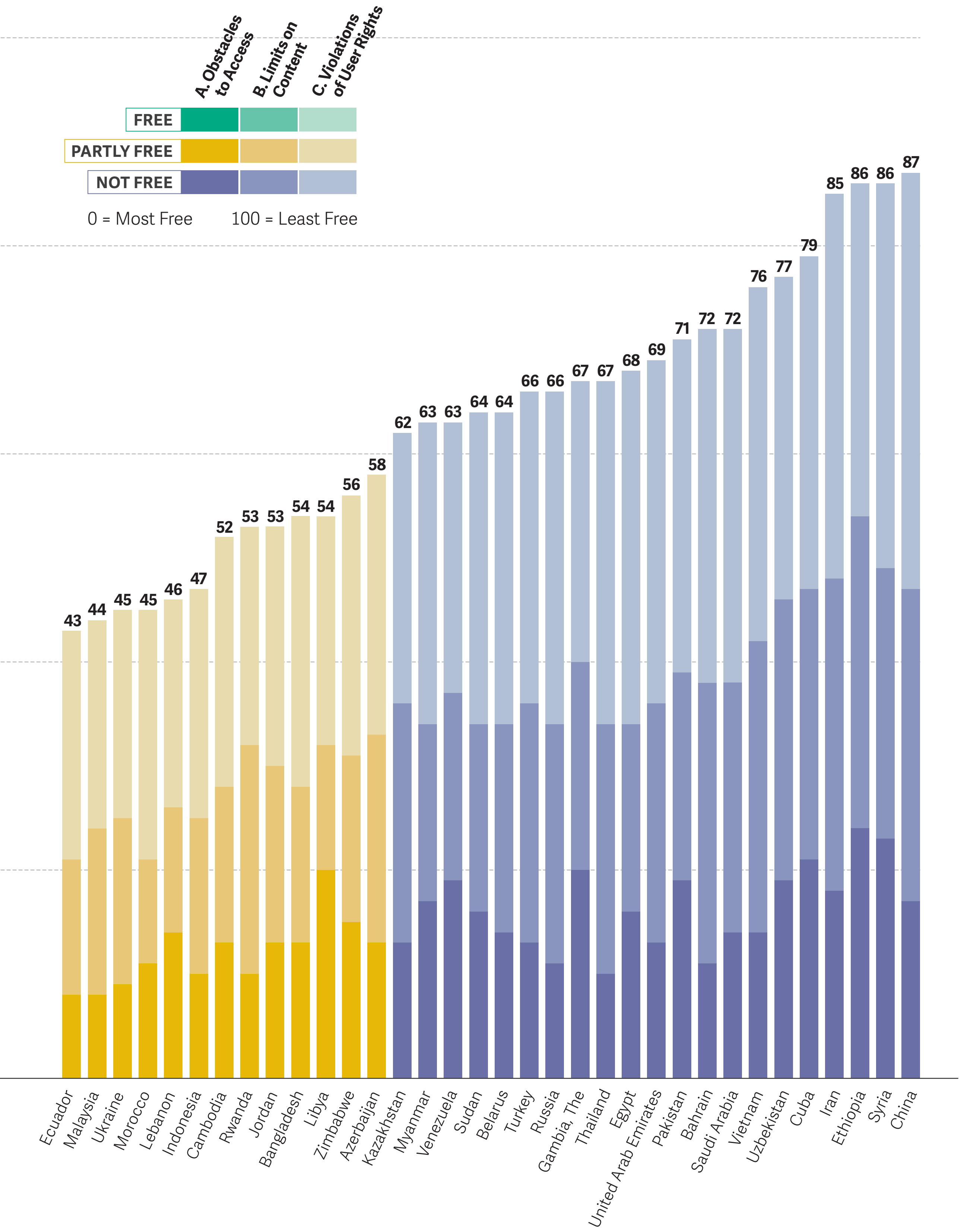
Ratings are determined through an examination of three broad categories:

A. OBSTACLES TO ACCESS: Assesses infrastructural and economic barriers to access; government efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers.

B. LIMITS ON CONTENT: Examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.

C. VIOLATIONS OF USER RIGHTS: Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.




A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights
FREE
PARTLY FREE
NOT FREE
0 = Most Free
100 = Least Free
Ecuador 43
Malaysia 44
Ukraine 45
Morocco 45
Lebanon 46
Indonesia 47
Cambodia 52
Rwanda 53
Jordan 53
Bangladesh 54
Libya 54
Zimbabwe 56
Azerbaijan 58
Kazakhstan 62
Myanmar 63
Venezuela 63
Sudan 64
Belarus 64
Turkey 66
Russia 66
Gambia, The 67
Thailand 67
Egypt 68
United Arab Emirates 69
Pakistan 71
Bahrain 72
Saudi Arabia 72
Vietnam 76
Uzbekistan 77
Cuba 79
Iran 85
Ethiopia 86
Syria 86
China 87

REGIONAL GRAPHS

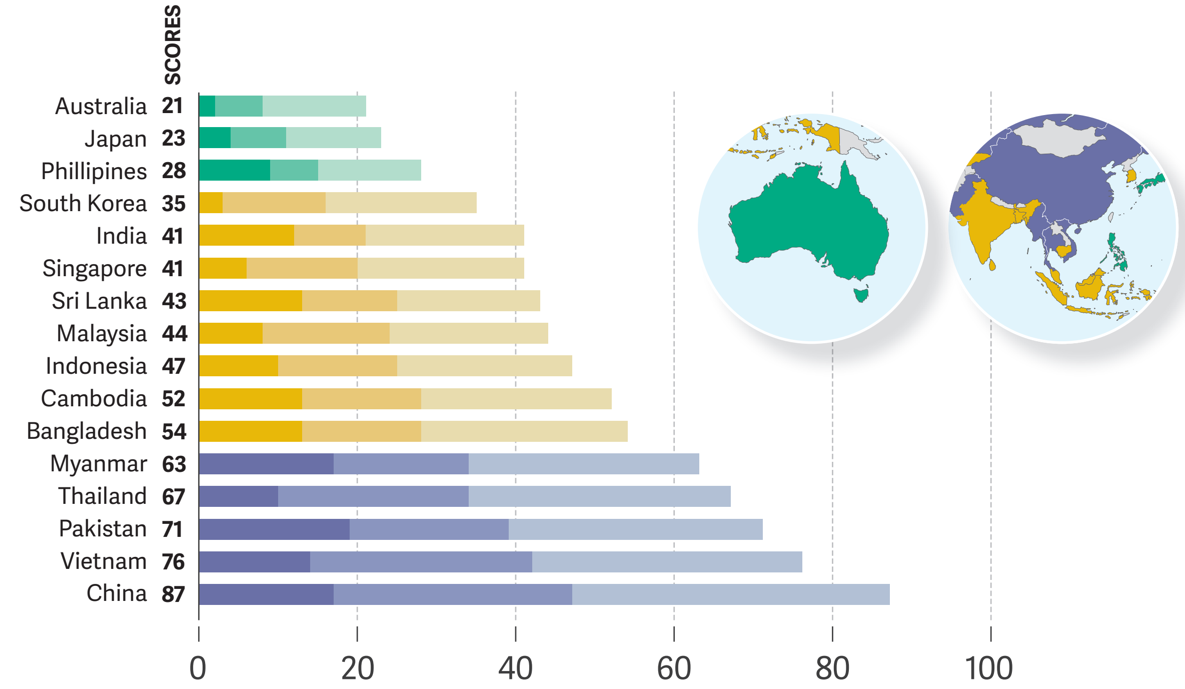
Freedom on the Net 2017 covers 65 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

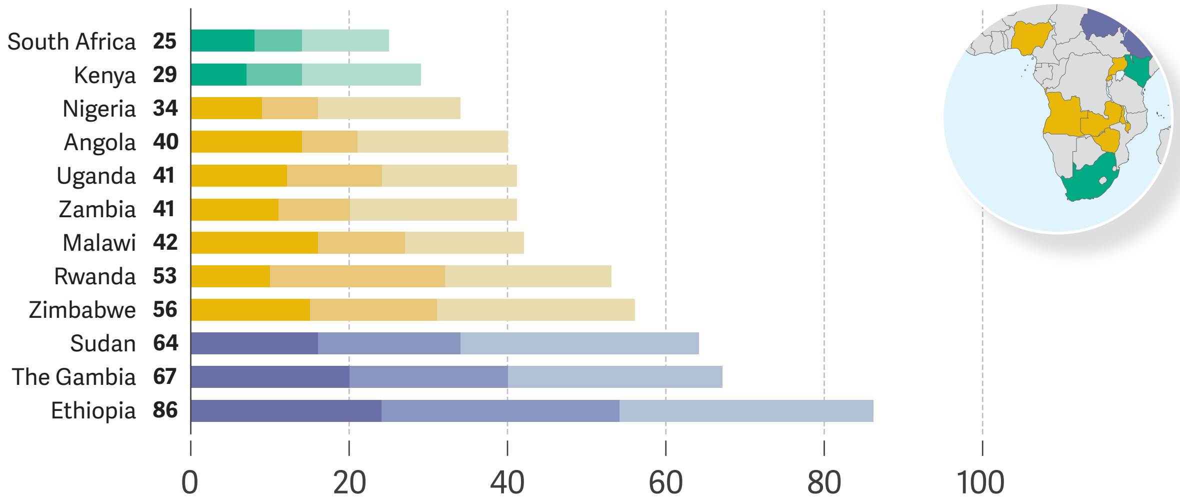
	A	B	C
FREE	🟩	🟩	🟩
PARTLY FREE	🟨	🟨	🟨
NOT FREE	🟦	🟦	🟦

0 = Most Free
100 = Least Free

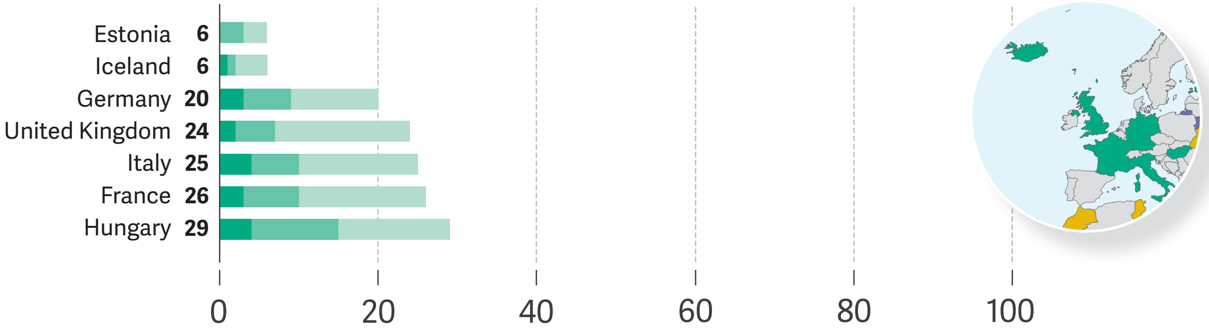
Asia-Pacific



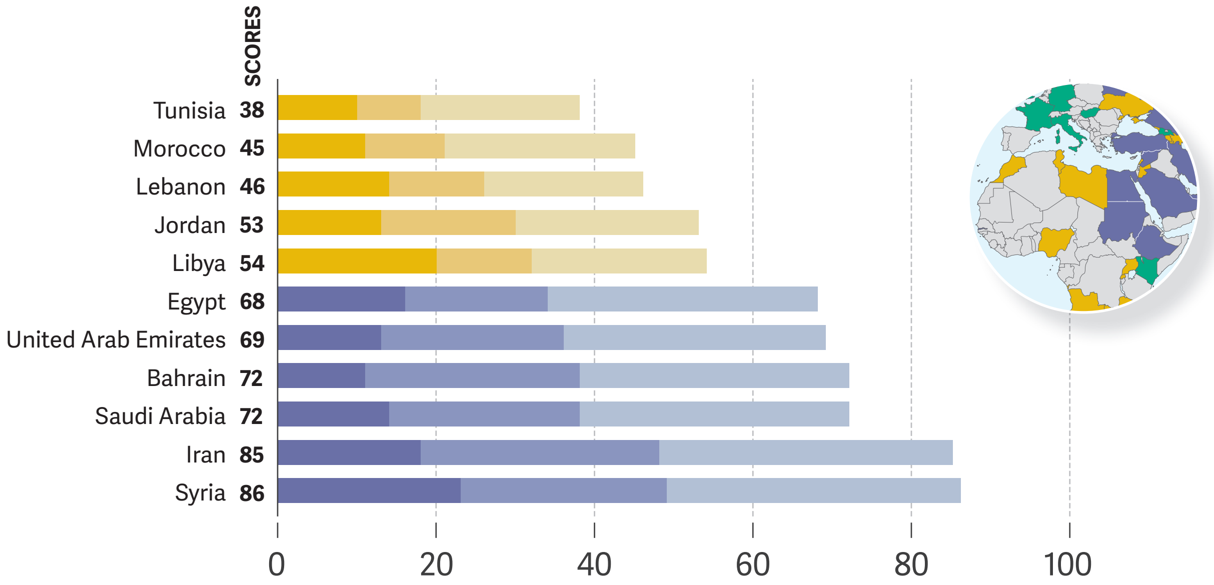
Sub-Saharan Africa



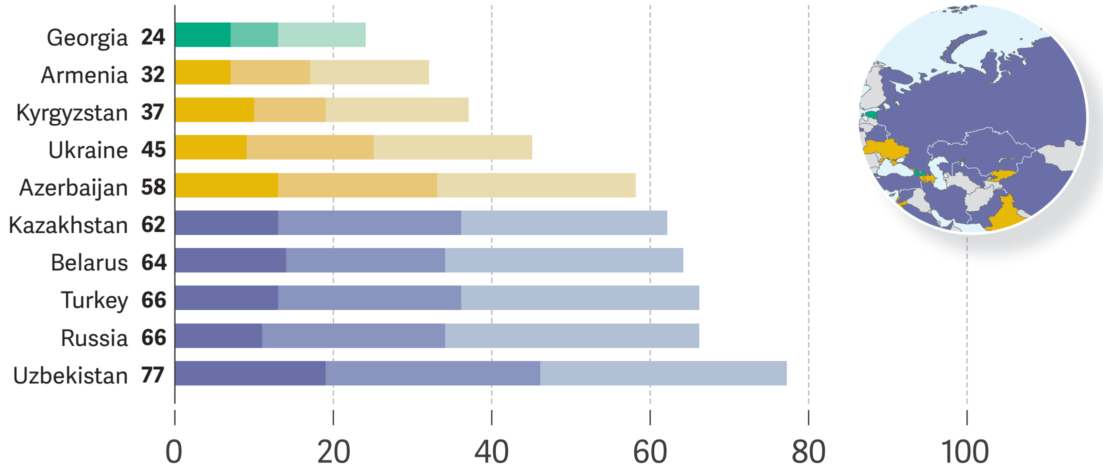
Europe



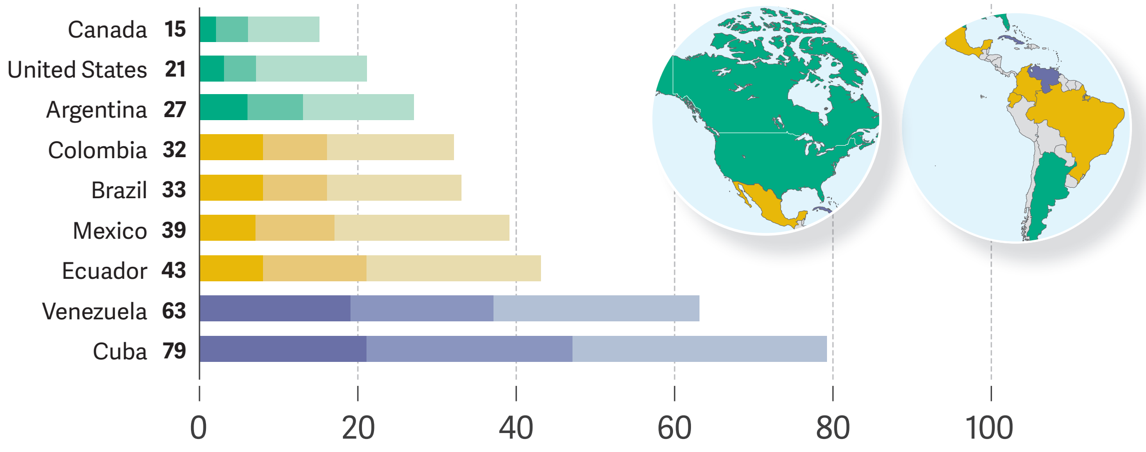
Middle East and North Africa



Eurasia



Americas



OVERVIEW OF SCORE CHANGES

	Overall			Category Scores & Trajectories						Status
Country	FOTN 2016	FOTN 2017	Overall Trajectory	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights		*Freedom on the Net* 2017
Asia-Pacific										
Australia	21	21		2		6		13		🟢
Bangladesh	56	54	▲	13	▲	15	▼	26	▲	🟡
Cambodia	52	52		13	▲	15		24	▼	🟡
China	88	87	▲	17	▲	30		40		🟣
India	41	41		12		9		20		🟡
Indonesia	44	47	▼	10	▲	15	▼	22	▼	🟡
Japan	22	23	▼	4		7		12	▼	🟢
Malaysia	45	44	▲	8	▲	16		20		🟡
Myanmar	61	63	▼	17		17		29	▼	🟣
Pakistan	69	71	▼	19	▼	20		32	▼	🟣
Philippines	26	28	▼	9		6	▼	13	▼	🟢
Singapore	41	41		6		14		21		🟡
South Korea	36	35	▲	3		13	▲	19	▼	🟡
Sri Lanka	44	43	▲	13	▲	12		18		🟡
Thailand	66	67	▼	10		24	▼	33		🟣
Vietnam	76	76		14		28		34		🟣
Eurasia										
Armenia	30	32	▼	7	▼	10		15	▼	🟡
Azerbaijan	57	58	▼	13	▲	20	▼	25	▼	🟡
Belarus	62	64	▼	14	▼	20	▲	30	▼	🟣
Georgia	25	24	▲	7	▲	6		11		🟢
Kazakhstan	63	62	▲	13	▲	23		26		🟣
Kyrgyzstan	35	37	▼	10		9	▼	18		🟡
Russia	65	66	▼	11	▼	23		32		🟣
Turkey	61	66	▼	13		23	▼	30	▼	🟣
Ukraine	38	45	▼	9	▼	16	▼	20	▼	🟡
Uzbekistan	79	77	▲	19	▲	27	▲	31		🟣
Americas										
Argentina	27	27		6		7		14		🟢
Brazil	32	33	▼	8		8	▼	17		🟡
Canada	16	15	▲	2	▲	4		9		🟢
Colombia	32	32		8		8		16		🟡
Cuba	79	79		21		26		32		🟣
Ecuador	41	43	▼	8		13	▼	22	▼	🟡
Mexico	38	39	▼	7	▲	10		22	▼	🟡
United States	18	21	▼	3		4	▼	14	▼	🟢
Venezuela	60	63	▼	19	▼	18	▼	26	▼	🟣

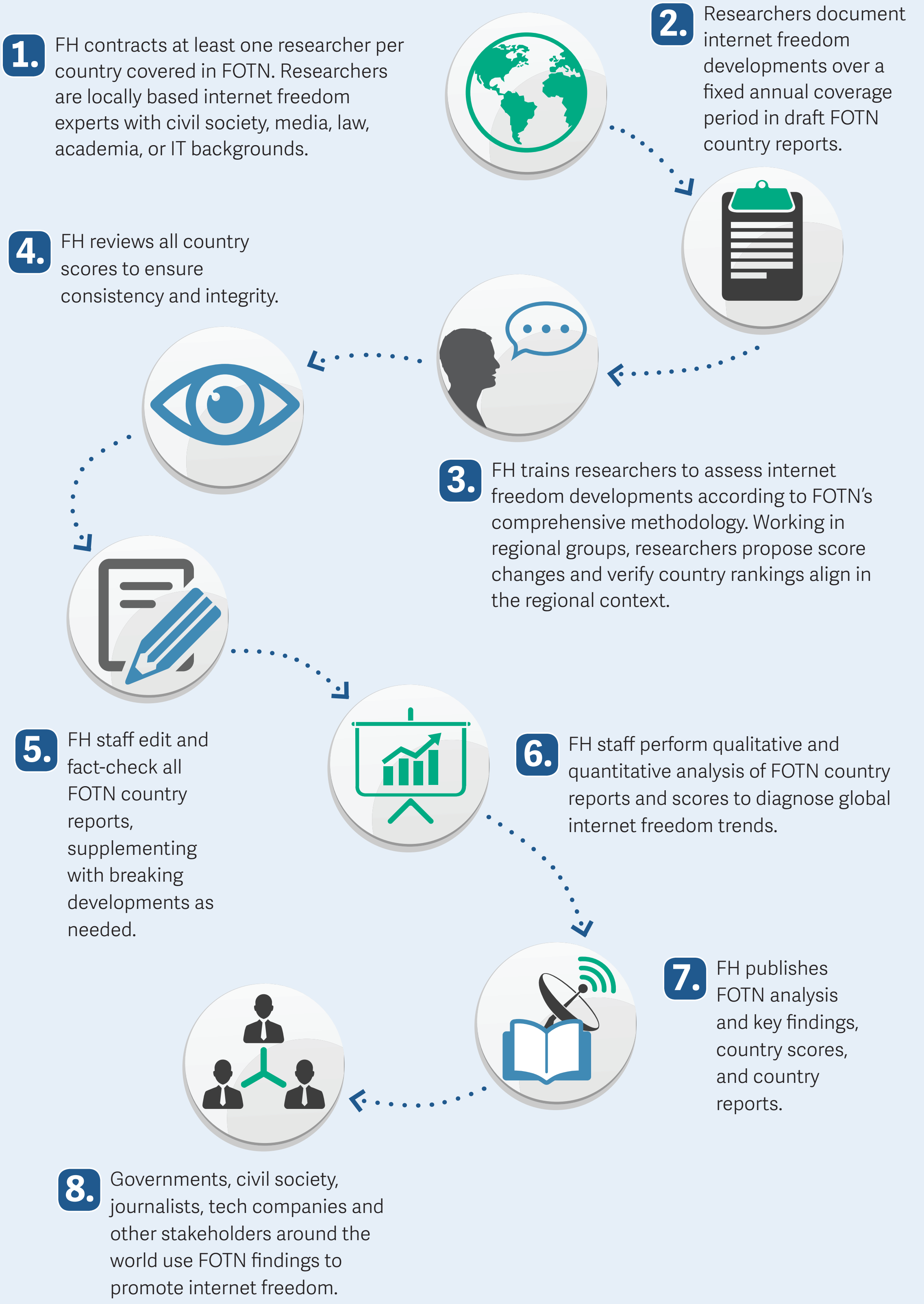
	Overall			Category Scores & Trajectories						Status
Country	**FOTN 2016**	**FOTN 2017**	**Overall Trajectory**	**A. Obstacles to Access**		**B. Limits on Content**		**C. Violations of User Rights**		***Freedom on the Net* 2017**
Middle East & North Africa										
Bahrain	71	72	▼	11	▼	27		34		🟣
Egypt	63	68	▼	16	▼	18	▼	34	▼	🟣
Iran	87	85	▲	18	▲	30	▲	37		🟣
Jordan	51	53	▼	13		17	▼	23	▼	🟡
Lebanon	45	46	▼	14	▼	12		20		🟡
Libya	58	54	▲	20		12	▲	22	▲	🟡
Morocco	44	45	▼	11	▲	10	▼	24	▼	🟡
Saudi Arabia	72	72		14		24		34		🟣
Syria	87	86	▲	23	▲	26		37		🟣
Tunisia	38	38		10		8		20		🟡
United Arab Emirates	68	69	▼	13	▲	23	▼	33	▼	🟣
Sub-Saharan Africa										
Angola	40	40		14		7		19		🟡
Ethiopia	83	86	▼	24	▼	30	▼	32		🟣
The Gambia	67	67		20	▼	20	▲	27		🟣
Kenya	29	29		7	▲	7		15	▼	🟢
Malawi	41	42	▼	16		11	▼	15		🟡
Nigeria	34	34		9	▲	7		18	▼	🟡
Rwanda	51	53	▼	10		22	▼	21	▼	🟡
South Africa	25	25		8		6		11		🟢
Sudan	64	64		16		18		30		🟣
Uganda	42	41	▲	11	▲	9	▲	21	▼	🟡
Zambia	38	41	▼	12	▼	12	▼	17		🟡
Zimbabwe	56	56		16	▼	15	▲	25		🟡
Europe										
Estonia	6	6		0		3		3		🟢
France	25	26	▼	3		7	▼	16		🟢
Germany	19	20	▼	3		6	▼	11		🟢
Hungary	27	29	▼	4	▲	11	▼	14	▼	🟢
Iceland	6	6		1		1		4		🟢
Italy	25	25		4		6		15		🟢
United Kingdom	23	24	▼	2		5		17	▼	🟢

▼ = Decline ▲ = Improvement
Blank = No Change

🟩 FREE 🟨 PARTLY FREE 🟪 NOT FREE

A *Freedom on the Net* score increase represents a negative trajectory (▼) for internet freedom, while a score decrease represents a positive trajectory (▲) for internet freedom.

Freedom on the Net Research Process



1. FH contracts at least one researcher per country covered in FOTN. Researchers are locally based internet freedom experts with civil society, media, law, academia, or IT backgrounds.

2. Researchers document internet freedom developments over a fixed annual coverage period in draft FOTN country reports.

3. FH trains researchers to assess internet freedom developments according to FOTN's comprehensive methodology. Working in regional groups, researchers propose score changes and verify country rankings align in the regional context.

4. FH reviews all country scores to ensure consistency and integrity.

5. FH staff edit and fact-check all FOTN country reports, supplementing with breaking developments as needed.

6. FH staff perform qualitative and quantitative analysis of FOTN country reports and scores to diagnose global internet freedom trends.

7. FH publishes FOTN analysis and key findings, country scores, and country reports.

8. Governments, civil society, journalists, tech companies and other stakeholders around the world use FOTN findings to promote internet freedom.

Methodology

Freedom on the Net provides analytical reports and numerical scores for 65 countries worldwide. Assigning scores allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. The accompanying country reports provide narrative detail to support the scores.

The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The numerical ratings and reports included in this study particularly focus on developments that took place between June 1, 2016 and May 31, 2017, although the analysis in the Key Internet Controls graph and the Topics Censored table covers developments through the end of September, when this year's edition was sent to press.

Freedom on the Net is a collaborative effort between a small team of Freedom House staff and an extensive network of local researchers and advisors in 65 countries. Our in-country researchers have diverse backgrounds—academia, blogging, traditional journalism, and tech— and track developments from their country of expertise. In the most repressive environments, Freedom House takes care to ensure researchers' anonymity or, in exceptional cases, works with individuals living outside their home country.

What We Measure

The *Freedom on the Net* index measures each country's level of internet and digital media freedom based on a set of methodology questions developed in consultation with international experts to capture the vast array of relevant issues that enable internet freedom (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users' rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country. While digital media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

The Scoring Process

The methodology includes 21 questions and nearly 100 subquestions, divided into three categories:

- **Obstacles to Access** details infrastructural and economic barriers to access, legal and ownership control over internet service providers , and independence of regulatory bodies;
- **Limits on Content** analyzes legal regulations on content, technical filtering and blocking of websites, self-censorship, the vibrancy and diversity of online news media, and the use of digital tools for civic mobilization;
- **Violations of User Rights** tackles surveillance, privacy, and repercussions for online speech and activities, such as imprisonment, extralegal harassment, or cyberattacks.

Each question is scored on a varying range of points. The subquestions guide researchers regarding factors they should consider while evaluating and assigning points, though not all apply to every country. Under each question, a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment. Points add up to produce a score for each of the subcategories, and a country's total points for all three represent its final score (0-100). Based on the score, Freedom House assigns the following internet freedom ratings:

- Scores 0-30 = Free
- Scores 31-60 = Partly Free
- Scores 61-100 = Not Free

After researchers submitted their draft scores in 2017, Freedom House convened regional review meetings via numerous international conference calls with Freedom House staff and around 70 local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores—based on set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

Key Internet Controls Explained

In the Key Internet Controls Table (page 21), Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2016 to May 2017; cells with an asterisk (*) represent events that occurred after the coverage period until September 2017, when the report was sent to print. Incidents are based on *Freedom on the Net* research and verified by in-country researchers. The Key Internet Controls reflect restrictions on political, social, or religious content.

- **Social media or communications apps blocked:** Entire apps or key functions of social media, messaging, and calling platforms temporarily or permanently blocked to prevent communication and information sharing.
- **Political, social, or religious content blocked**: Blocking or filtering of domains, URLs, or keywords, to limit access to specific political, social, or religious content.
- **Localized or nationwide information and communication technology (ICT) shutdown:** Intentional disruption of internet or cellphone networks in response to political or social events, whether temporary or long term, localized or nationwide.
- **Progovernment commentators manipulate online**

discussions: Strong indications that individuals are paid to distort the digital information landscape in the government's favor, without acknowledging sponsorship.

- **New law or directive increasing censorship or punishment passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to censor or punish legitimate online activity.
- **New law or directive increasing surveillance or restricting anonymity passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to surveil or expose the identity of citizens using the internet with legitimate intent.
- **Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content:** Any arrest, prosecution, detention that is credibly perceived to be in reprisal for digital expression, including trumped up charges. Brief detentions for interrogation are not reflected.
- **Blogger or ICT user physically attacked or killed (including in custody):** Any physical attack, kidnapping, or killing that is credibly perceived to be in reprisal for digital expression. This includes attacks while in custody, such as torture.
- **Technical attacks against government critics or human rights organizations:** Cyberattacks against human rights organizations, news websites, and individuals sharing information perceived as critical, with the clear intent of disabling content or exposing user data, and motives that align with those of agencies that censor and surveil the internet. Targets of attacks considered here may include critics in exile, but not transnational cyberattacks, even with political motives.

Censored Topics by Country Explained

In the Censored Topics by Country graphic (page 16), Freedom House staff documented a selection of topics that were subject to censorship in the 65 countries covered. Countries were included if state authorities blocked or ordered the removal of content, or detained or fined users for posting content on the topics considered. The chart does not consider extralegal pressures like violence, self-censorship, or cyberattacks, even where the state is believed to be responsible. To capture a comprehensive data set, the chart includes incidents over a two-year span, between June 2015 and September 2017, and distinguishes between pervasive and sporadic censorship. All data is based on *Freedom on the Net* research and verified by in-country researchers.

- **Criticism of the Authorities:** Content perceived as criticism of the state or its representatives, including the government, military, ruling family, police, judiciary, or other officials.
- **Political Opposition:** Content affiliated with political groups or opponents, including in the diaspora.
- **Corruption:** Accusations or exposés of corruption or misuse of public funds.
- **Blasphemy:** Content perceived as insulting or offending religion.
- **Mobilization for Public Causes:** Calls to protest or campaigns on political, social, or human rights issues.
- **Satire:** Humorous or ironic commentary on political or social issues.
- **Ethnic and Religious Minorities:** Content related to marginalized groups, including ethnic and religious minorities.
- **LGBTI Issues:** Content related to lesbian, gay, bisexual, transgender, or intersex individuals.
- **Conflict:** Discussion or reporting on local or international instances of violence, conflict, or terrorism.
- **Social Commentary:** Content that is not overtly political, including on economic, environmental, cultural, or educational issues.

Checklist of Questions

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.

A. OBSTACLES TO ACCESS (0-25 POINTS)

1. To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)

- Does poor infrastructure (electricity, telecommunications, etc.) limit citizens' ability to receive internet in their homes and businesses?
- To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?
- To what extent is there internet and mobile phone access, including data connections or satellite?
- Is there a significant difference between internet and mobile phone penetration and access in rural versus urban areas or across other geographical divisions?
- To what extent are broadband services widely available in addition to dial-up?

2. Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)

- In countries where the state sets the price of internet access, is it prohibitively high?
- Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?
- Do low literacy rates (linguistic and "digital literacy") limit citizens' ability to use the internet?
- Is there a significant difference between internet penetration and access based on gender, or across ethnic or socio-economic societal divisions?
- To what extent are software, news, and other information available online in the main local languages spoken in the country?

3. Does the government impose restrictions on ICT connectivity and access to particular social media and communication apps permanently or during specific events? (0-6 points)

- Does the government place limits on the amount of bandwidth that access providers can supply?
- Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?
- Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?
- Does the government block protocols and tools that allow for instant, person-to-person communication (VoIP, instant messaging, text messaging, etc.), particularly those based outside the country (e.g. Skype, WhatsApp, etc.)?
- Does the government block protocols, social media, and/or communication apps that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?
- Is there blocking of certain tools that enable circumvention of online filters and censors?

4. Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)

Note: Each of the following access providers are scored separately:

1a. Internet service providers (ISPs) and other back-bone internet providers (0-2 points)

1b. Cybercafes and other businesses entities that allow public internet access (0-2 points)

1c. Mobile phone companies (0-2 points)

- Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?
- Is it legally possible to establish a private access

provider or does the state place extensive legal or regulatory controls over the establishment of providers?

- Are registration requirements (i.e. bureaucratic ”red tape”) for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?
- Does the state place prohibitively high fees on the establishment and operation of access providers?

5. To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)

- Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?
- Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?
- Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?
- Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?
- Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?

B. LIMITS ON CONTENT (0-35 POINTS)

1. To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)

- Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?
- Is there significant filtering of text messages or other content transmitted via mobile phones?
- Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of email or text messages, etc?
- Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?

2. To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)

- To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?
- To what degree do government officials or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?
- Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?
- Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?

3. To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)

- Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to

restrict access to certain content are proportional to their stated aim?
- Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?
- Do state authorities block more types of content than they publicly declare?
- Do independent avenues of appeal exist for those who find content they produced to have been subjected to censorship?

4. Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)
- Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?
- Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?
- Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?

5. To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)
- To what degree do government officials or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?
- Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?
- Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?
- Does the government employ, or encourage content providers to employ, individuals to post progovernment remarks in online bulletin boards and chat rooms?
- Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?

6. Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)
- Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, email applications, blog hosting platforms, etc.) to be economically viable?
- Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?
- Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?
- To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?
- To what extent do users have access to free or low-cost blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?

7. To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)
- Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?
- Does the public have ready access to media outlets or websites that express independent, balanced views?
- Does the public have ready access to sources of information that represent a range of political and social viewpoints?
- To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community

organizations or religious, ethnic and other minorities?
- To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?

7. To what extent have individuals successfully used the internet and other ICTs as sources of information and tools for mobilization, particularly regarding political and social issues? To what extent are such mobilization tools available without government restriction? (0-6 points)
- To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?
- To what extent are online communication tools or social networking sites (e.g. Twitter, Facebook) used as a means to organize politically, including for "real-life" activities?
- Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)
- Does the constitution contain language that provides for freedom of speech and of the press generally?
- Are there laws or legal decisions that specifically protect online modes of expression?
- Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?
- Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?
- Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?

2. Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)
- Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an email, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)
- Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?
- Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?
- Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?
- Are there penalties for libeling officials or the state in online content?
- Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?

3. Are individuals detained, prosecuted, or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)
- Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?
- Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via email or text messages?
- Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?
- Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?
- Are penalties for "irresponsible journalism" or "rumor mongering" applied widely?
- Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of "libel tourism")?

4. Does the government place restrictions on anonymous communication or require user registration? (0-4 points)

- Are website owners, bloggers, or users in general required to register with the government?
- Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government?
- Are users prohibited from using encryption software to protect their communications?
- Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?

5. To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)

- Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of email and mobile text messages?
- To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?
- Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?
- Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?
- Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?

6. To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)

Note: Each of the following access providers are scored separately:

6a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)

6b. Cybercafes and other business entities that allow public internet access (0-2 points)

6c. Mobile phone companies (0-2 points)

- Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?
- Are access providers prosecuted for not doing so?
- Does the state attempt to control access providers through less formal methods, such as codes of conduct?
- Can the government obtain information about users without a legal process?

7. Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)

- Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?
- Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?
- Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?
- Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?

8. Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats? (0-3 points)

- Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyberespionage, data gathering, DDoS attacks), including those originating from outside of the country?
- Have websites belonging to opposition or civil society groups within the country's boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?
- Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?
- Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by nonstate actors from within the country's borders) and are they enforced?

Contributors

Freedom House Research Team

- Sanja Kelly, Director, *Freedom on the Net*
- Mai Truong, Program Manager, Africa Editor
- Adrian Shahbaz, Research Manager, MENA Editor
- Madeline Earp, Senior Research Analyst, Asia Editor
- Jessica White, Research Analyst, Americas and Europe Editor
- Rose Dlougatch, Senior Research Associate, Eurasia Editor

Report Authors and Advisors

- **Argentina:** Valeria Milanes, Eduardo Ferreyra, Jeannette Torrez, Leandro Ucciferri, Free Expression & Privacy team, Association for Civil Rights (ADC)
- **Armenia:** Artur Papyan, Editor and Contributor, RFE/RL, and media development consultant
- **Australia:** Dr. Alana Maurushat, Senior Lecturer, Faculty of Law, and Co-Director, Cyberspace Law and Policy Community, The University of New South Wales
- **Azerbaijan:** Arzu Geybulla, Azerbaijani journalist
- **Brazil:** Fabrício Bertini Pasquot Polido, Tenured Professor, Law School of the Federal University of Minas Gerais, and Founder of the Research Institute of Internet and Society (IRIS)
- **Canada:** Allen Mendelsohn, Canadian lawyer specializing in internet and technology law and lecturer of internet law at McGill University's Faculty of Law
- **Colombia:** María Juliana Soto, Juan Diego Castañeda, Joan López, Fundación Karisma
- **Cuba:** Ted Henken, Associate Professor of Sociology and Latin American Studies at Baruch College, CUNY
- **Ecuador:** Andrés Delgado-Ron, Researcher, Universidad Tecnológica Equinoccial
- **Estonia:** Katrin Nyman Metcalf, Professor, Institute of Law, School of Business and Governance, Tallinn University of Technology, and Programme Director of Research and Legal Aspects, e-Governance Academy
- **France:** Jean-Loup Richet, Researcher, University of Nantes and ESSEC
- **The Gambia:** Demba Kandeh, Lecturer, School of Journalism and Digital Media, University of The Gambia
- **Georgia:** Teona Turashvili, Analyst, Institute for Development of Freedom of Information (IDFI)
- **Germany:** Philipp Otto, Founder and Head, iRights.Lab think tank and iRights.Media publishing house, Editor in Chief, iRights.info, political strategist, advisor to the German government and companies; Henning Lahmann, Senior Policy Advisor, iRights.Lab
- **Hungary:** Dalma Dojcsák and Máté Szabó, Hungarian Civil Liberties Union
- **Iceland:** Caroline Nellemann, independent consultant, specialist in digital media and civic engagement
- **India:** Sarvjeet Singh, Programme Manager, Centre for Communication Governance at National Law University, Delhi; Nishtha Sinha and Vaibhav Dutt, Students, B.A., LL.B. (Hons.), National Law University, Delhi
- **Indonesia:** Indriaswati Dyah Saptaningrum, Senior Researcher, ELSAM (The Institute for Policy Research and Advocacy)
- **Iran:** Kaveh Azarhoosh, independent researcher and student at the Oxford Internet Institute
- **Italy:** Philip di Salvo, PhD candidate at Università della Svizzera and freelance journalist; Antonella Napolitano, Communications Manager, Italian Coalition for Civil Liberties and Rights (CILD)

- **Japan:** Dr. Leslie M. Tkach-Kawasaki, Associate Professor, University of Tsukuba
- **Jordan:** Jordan Open Source Association (JOSA)
- **Kazakhstan:** Adilzhan Nurmakov, Senior Lecturer, KIMEP University
- **Kenya:** Moses Karanja, Researcher, The Citizen Lab
- **Kyrgyzstan:** Artem Goryainov, IT Programs Director, Public Foundation CIIP
- **Lebanon:** SMEX
- **Libya:** Fadil Aliriza, journalist, researcher, political analyst, and Tunisia Project Manager, Carnegie Endowment for International Peace
- **Malawi:** Gregory Gondwe, journalist
- **Malaysia:** K Kabilan, Managing Editor, BeritaDaily.com, and online media consultant
- **Mexico:** Paola Ricaurte Quijano, Associate Research Professor, School of Humanities and Education, Tecnológico de Monterrey
- **Morocco:** Bouziane Zaid, Visiting Associate Professor, American University of Sharjah
- **Myanmar:** Min Zin, Executive Director, Institute for Strategy and Policy: Myanmar
- **Nigeria:** ‘Gbenga Sesan, Executive Director, Paradigm Initiative
- **Pakistan:** Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan; Shmyla Khan, Project Manager, Digital Rights Foundation
- **Singapore:** Cherian George, Professor, School of Communication, Hong Kong Baptist University
- **South Africa:** Zororo Mavindidze, independent researcher
- **South Korea:** Dr. Yenn Lee, Doctoral Training Advisor, School of Oriental and African Studies, University of London
- **Sri Lanka:** N.V. Nugawela, independent researcher, Colombo
- **Sudan:** Azaz Elshami, independent researcher and development consultant
- **Syria:** Dlshad Othman, information security expert
- **Uganda:** Lillian Nalwoga, Policy Officer, CIPESA, and President, Internet Society Uganda Chapter
- **Ukraine:** Dariya Orlova, Senior lecturer at Kyiv-Mohyla School of Journalism
- **United Kingdom:** Aaron Ceross, Researcher in Cyber Security, University of Oxford
- **United States:** Laura Reed, independent researcher
- **Uzbekistan:** Daniil Kislov, Editor-in-Chief of Ferghana News Agency; Ernest Zhanaev, English Editor of Ferghana News Agency
- **Venezuela:** Raisa Urribarri, Emeritus Professor at Universidad de Los Andes, Venezuela, and Journalist, Researcher and Consultant on ICT issues

The analysts for the reports on Angola, Bahrain, Bangladesh, Belarus, Cambodia, China, Egypt, Ethiopia, Rwanda, Philippines, Russia, Saudi Arabia, Thailand, Tunisia, Turkey, United Arab Emirates, Vietnam, Zambia and Zimbabwe are independent internet researchers who have requested to remain anonymous.

Manipulation and disinformation techniques could enable authoritarian regimes to expand their power, while permanently eroding user confidence in online media and the internet as a whole.

Freedom House

Freedom House is a nonprofit, nonpartisan organization that supports democratic change, monitors freedom, and advocates for democracy and human rights.

1850 M Street NW, 11th Floor
Washington, DC 20036

111 John Street, Suite 810
New York, NY 10038

www.freedomhouse.org
facebook.com/FreedomHouseDC
@FreedomHouseDC

202.296.5101 | info@freedomhouse.org