Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**1390**
Land:	Syrien
Kilde:	Freedom House
Titel:	Freedom on the Net 2020 – Syria
Udgivet:	14. oktober 2020
Optaget på baggrundsmaterialet:	22. december 2020

Freedom House

Syria

FREEDOM ON THE NET 2020

17

NOT FREE

/100

A. Obstacles to Access	6 /25
B. Limits on Content	8 /35
C. Violations of User Rights	3 /40

LAST YEAR'S SCORE & STATUS
17 /100 **Not Free**

Scores are based on a scale of 0 (least free) to 100 (most free)

Overview

TOP

Internet freedom in Syria is severely restricted due to government repression of dissent and the effects of the ongoing civil war. Journalists

and online activists operate in an acutely dangerous environment, and security forces often arrest, detain, and torture citizens and journalists for their online activity. Amid the war-related economic crisis, the authorities have implemented an “internet rationing” scheme that limits the amount of data citizens are able to use each month. Censorship is rampant, specifically targeting opposition news sites and antigovernment content.

Political rights and civil liberties in Syria are severely compromised by one of the world’s most repressive regimes and by other belligerent forces in the civil war. The regime prohibits genuine political opposition and harshly suppresses freedoms of speech and assembly. Corruption, enforced disappearances, military trials, and deaths in custody are endemic in government-controlled areas. Residents of contested regions or territory held by nonstate actors are subject to additional abuses, including intense and indiscriminate combat, sieges and interruptions of humanitarian aid, and mass displacement.

Key Developments, June 1, 2019 – May 31, 2020

- In March 2020, the Ministry of Communications and Technology began implementing an “internet rationing” system, which resulted in price increases. If a subscriber exceeds the threshold for use of a broadband connection, the speed is reduced (A1).
- The Turkish government launched a military offensive in northeastern Syria in November 2019, during which Turkish internet service providers (ISPs) shut off connectivity for customers in the affected region (A3).
- Users took part in a number of online campaigns to protest the civil war, the economic situation, and forced military service, though many Syrians still engage in self-censorship to avoid reprisals by the authorities (B8).
- The jihadist militant group Hay’at Tahrir al-Sham (HTS) continued to abduct and detain journalists and media activists in areas under its control (C3).

TOP

- It was reported during the coverage period that media activist Alaa Nayef al-Khader had died due to torture after more than two years in Syrian government custody (C7).

A. Obstacles to Access

Mobile phone and internet penetration rates increased during the coverage period. Nonetheless, the government maintains a tight grip on the internet infrastructure in the territory under its control, which has gradually expanded since 2015. In November 2019, Turkish ISPs that provide service in northern Syria shut off internet access during a Turkish military offensive against Kurdish-led forces in the northeast.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**1** / 6

Syria's telecommunications infrastructure is one of the least developed in the Middle East, and broadband connections are difficult to acquire. [1] Conditions worsened beginning in 2011, when electricity outages increased dramatically as a violent government crackdown on public protests evolved into outright civil war. Damage to infrastructure is particularly severe in cities that the government has lost or retaken by force, largely due to heavy bombardment and other conflict-related destruction. Although the government continued to reclaim territory during the coverage period, [2] telecommunications services in the recaptured areas remained limited. [3] Parts of the country that are not held by the government have developed alternative, decentralized systems for securing internet connectivity. Areas in the northwest near the border with Turkey are served by Turkish ISPs, [4] while areas in the northeast have internet connections from Turkish and Iraqi companies. [5]

TOP

According to a January 2020 report by DataReportal, internet penetration had reached 47 percent, up from 33 percent the previous year. [6] While mobile broadband penetration was at just 15 percent, mobile broadband coverage was quite high, with about 85 percent of the population covered

by third-generation (3G) networks in 2019. [7] Average fixed-line download speeds decreased by 35.2 percent, to 5.91 Mbps, while average mobile download speeds rose by 8.06 percent, to 21.05 Mbps, between 2019 and 2020. Average fixed-line upload speeds decreased by 47.3 percent, to 7.04 Mbps, while average mobile upload speeds rose by 16.65 percent, to 9.67 Mbps, between 2019 and 2020. [8]

The telecommunications sector has been negatively affected by the ongoing conflict in Syria. The Emergency Telecommunications Cluster, which is led by the World Food Programme, was formally activated in 2013 and works to provide telecommunications services to the humanitarian community responding to the crisis in Syria. [9] During the 60th cycle of the Damascus International Exhibition in 2017, the mobile service providers Syriatel and MTN Syria announced the launch of fourth-generation (4G) high-speed internet networks. [10]

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**1** / 3

Broadband connections in Syria are expensive to acquire. [1]

The price, speed, and availability of internet service varies across regions. Prices have remained fairly consistent since mid-2017, when, according to a price list published by the Syrian Computer Society Network, the monthly cost for a 1 Mbps ADSL (asymmetric digital subscriber line) connection was 2,400 Syrian pounds ($11). [2] As of September 2018, the cost of 1 GB of mobile network data from Syriatel and MTN Syria was 4,000 pounds ($19) per month. [3] The monthly fees for a 1 Mbps internet connection were approximately $10 in rebel-controlled areas of northern Syria as of early 2019. [4] The average annual per capita income is 418,739 pounds ($870). [5] TOP

About one-third of the country is disconnected from Syrian ISP networks. Syrians in such areas have turned to WiMax (worldwide interoperability for microwave access) connections, internet cables, or Turkish Wi-Fi

operators; these provide service to local distributors, which in turn provide subscriptions to residents. Many also rely on mobile phone connections from Turkish providers in rebel-controlled areas of northern Syria. Telephone centers in those regions similarly install ADSL lines for subscribers using Turkish ISPs. [6] Areas in northeastern Syria are served by both Turkish and Iraqi ISPs. [7]

In March 2020, the Ministry of Communications and Technology began implementing an "internet rationing" system, which reportedly resulted in price increases. If a subscriber exceeds a certain threshold for the use of ADSL, the connection speed is reduced. [8]

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**3** / 6

The government has carried out extensive and repeated internet shutdowns since 2011, though no major disruptions were observed during the latest coverage period.

Internet shutdowns by Turkish authorities have also been frequent throughout the conflict. Between October and November 2019, Turkish forces and allied Syrian rebel militias attacked the Kurdish-led Syrian Democratic Forces (SDF) in northeastern Syria. During the offensive, Turkish authorities cut off internet service in almost all of the areas controlled by the SDF in northern Syria. [1] Similarly, in January 2018, when Turkish forces initiated a military offensive in the northwestern district of Afrin against the People's Protection Units (YPG), the same Syrian Kurdish militia that leads the SDF coalition in the northeast, Turkish authorities cut off internet service for most of northern Syria. [2] The following month, the jihadist militant group HTS—formerly known as Jabhat al-Nusra—cut off the internet in many cities and towns in Idlib Governorate in response to a protest movement against its presence in the city of Idlib; the movement had been supported by a parallel campaign on social media (see B8). [3] In government-controlled areas, Syrian

TOP

authorities restricted internet access for several hours per day during secondary school exams in May and June 2018, which had a negative impact on some businesses. [4]

Throughout the spring of 2019, Syrians reported difficulty using the messaging platform WhatsApp, specifically when sending photos, videos, and audio clips. These disruptions reportedly occurred in government-controlled territories. Connectivity was reportedly restored by the end of May, but no official statement was issued by the Ministry of Communications and Technology or internet companies regarding the cause of the poor WhatsApp service. [5]

In October 2018, the Syrian Telecommunications Regulatory Authority (SYTRA)—since renamed the Syrian Telecommunications and Post Regulatory Authority (SY-TPRA)—revealed that it was considering a ban on Voice over Internet Protocol (VoIP) services, including WhatsApp, in order to mitigate revenue losses for the traditional telecommunications sector. [6] However, WhatsApp and other VoIP services had not been blocked at the end of the coverage period. [7] Since the bans were proposed, people have used virtual private network (VPN) apps to guard against any restrictions.

In areas controlled by the government, the Syrian Telecommunications Establishment (STE) serves as both an ISP and a telecommunications regulator, providing the government with tight control over the internet infrastructure. [8] In addition, private fixed-line and mobile ISPs are required to sign a memorandum of understanding to connect to the international internet via gateways controlled by the Syrian Information Organization (SIO). [9] While users in northern Syria continue to rely on Turkish networks for internet service, [10] Syrian networks are the main source of internet access in central and southern Syria, where the government and its allies have recovered most territory from rebel forces. [11]

TOP

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**1** / 6

Syrian laws permit the establishment of privately owned ISPs, though obtaining a commercial license requires approval from the security services. Approval is based on a "security audit" of the applicant, whose political background and positions, relatives, and associates are all scrutinized. [1] The process poses a challenge to anyone with links to dissidents or other opponents of the regime.

There are currently 27 licensed ISPs in Syria, [2] and three are owned by state-affiliated entities: Tarassul, which is owned by the STE; SCS-NET, which is owned by the Syrian Computer Society; and Ibaa, which is owned by the military and dedicated to Syrian military personnel and their families, as well as the families of military casualties and veterans. [3] While the number of ISPs has increased, entry into the market remains difficult due to the country's instability and resulting damage to infrastructure. [4]

Independent satellite-based connections are prohibited, although they are still heavily employed, also due to the damage that information and communication technology (ICT) infrastructure has sustained during the war. [5] ISPs and cybercafés operating in government-controlled areas must obtain a permit from the STE and another security permit from the Interior Ministry. [6] Cybercafé owners are required to monitor customers and record their activities (see C6).

There are two dominant mobile phone providers: Syriatel, owned by Rami Makhlouf, a cousin of President Bashar al-Assad, and MTN Syria, a subsidiary of the South African company MTN. The entry of a third major mobile provider has been under discussion since 2010. [7] However, during a parliamentary session in April 2018, the minister of communications and technology stated that such a company would need to guarantee a minimum amount of revenue to the state before it could receive a license. [8] In 2015, the contracts of Syriatel and MTN Syria were modified from build, operate, and transfer (BOT) agreements, in which the networks would ultimately be transferred to STE, into more traditional licensing contracts. [9] Any new mobile provider would also have to create its own infrastructure.

TOP

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

Syria's ICT market and internet policy are regulated by the SY-TPRA and the STE, [1] which owns all fixed-line infrastructure. The STE is a government body established in 1975 as part of the Ministry of Communications and Technology. [2] Domain-name registration is managed by the Syrian Computer Society. [3]

B. Limits on Content

The government engages in extensive filtering of websites related to politics, ethnic and religious identity, human rights, and foreign affairs. A number of opposition websites were blocked or reblocked during the coverage period. High levels of self-censorship persist amid threats and violent reprisals for online activities, particularly in areas under government control.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	**1** / 6

Authorities block access to a variety of online materials. While some sites were unblocked in previous years, new obstructions were imposed during the latest coverage period, and the government's expanding territorial control meant that existing restrictions were more widely enforced.

Since the beginning of the civil war, a number of websites have been employed to mobilize people to protest or resist the regime, including those linked to the network of activists known as the Local Coordination Committees (LCCs). In government-controlled territory, many of these sites have been subject to blocking, as have opposition websites and the sites of human rights organizations; content that is critical of the regime's

TOP

political, cultural, social, or economic policies; criticism of specific high-level government officials; and sites that expose official corruption.

In 2019, the authorities reimposed blocks on a number of websites, such as those of the Syrian Human Rights Committee and the Syrian Observatory for Human Rights, after lifting bans on them in 2018. [1] The authorities have previously banned websites that used Wix, an Israeli site-building company.

In 2018, authorities similarly restored blocks on several opposition media websites, including the newspaper *Enab Baladi* and SouriaLi Radio, after unblocking them in 2017. [2] The targeted outlets were significant sources of independent information. [3] Even some progovernment journalists relied on the sites for news on regions under opposition control. [4] A number of other websites remained blocked, including that of the Kuwaiti newspaper *Al-Seyassah* and *Souriatna*, a magazine that offers the perspectives of young Syrians.

No formal reasons have been provided for many past decisions to block or unblock websites. For example, a number of regional media sites were unblocked without explanation by the end of 2017, including Al-Jazeera, Al-Arabiya, *Asharq al-Awsat*, Qatar's *Al-Arab* newspaper, and *Al-Hayat*. [5] Many nonpolitical websites were unblocked as well, such as Wikipedia and the WordPress blog-hosting service. Notably, the block on the Israeli country domain (.il) was also lifted with no official rationale. By contrast, the Ministry of Communications and Technology justified the April 2018 blocking of 160 pornographic websites by claiming that it would protect children and facilitate higher internet speeds. [6]

Facebook has been accessible since the government lifted a four-year block on the social network in 2011. The video-sharing website YouTube was also unblocked. Some activists suspected that the regime eased restrictions on the platforms in order to track citizens' online activities and identities (see C5). As of April 2019, both were among the three most visited websites in the country. Other social media platforms such as Twitter are also available. [7] Skype has suffered frequent disruptions, either due to low speeds or intermittent blocking by authorities.

TOP

Antivirus software and updates to operating systems remain blocked due to US sanctions. [8] The government continues to block circumvention tools that are used to access censored content, internet security software that can prevent state surveillance, and other applications that enable anonymous communications. By employing deep packet inspection (DPI) filtering on the Syrian network, authorities were able to block secure communication tools such as OpenVPN, Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPsec) in 2011. [9] They remained inaccessible at the end of the coverage period.

Censorship is implemented by the STE and private ISPs using various commercially available software programs. Independent reports in recent years pointed to the use of ThunderCache software, which is capable of "monitoring and controlling a user's dynamic web-based activities as well as conducting deep packet inspection." [10] Authorities have also used technology provided by the Italian company Area SpA to improve their censorship and surveillance capabilities, according to evidence from 2011. [11] Analysis revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites. [12] The *Wall Street Journal* identified efforts that year to block or monitor tens of thousands of opposition websites or online forums covering the uprising. [13]

The government has allegedly filtered text messages since 2011, with an initial focus on the dates of planned protests. In 2012, Bloomberg reported that a special government unit known as Branch 225 had ordered Syriatel and MTN Syria to block text messages containing keywords like "revolution" or "demonstration." The providers reportedly implemented the directives with the help of technology originally purchased from two Irish firms to restrict spam. [14]

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?	**TOP 1 / 4**

Censorship of news sites and social media content in government-controlled areas remained severe and appeared to intensify during the coverage period. For example, in late 2019, a media organization barred its employees from publishing any objections or complaints about the living conditions or security situation on social media without the approval of the administration [1] . This came after the director of the organization received a warning from one of the intelligence security branches in response to an employee's Facebook post, which criticized the security forces' interactions with journalists who were highlighting social problems and difficulties in Syria.

A July 2019 report from Reporters Without Borders noted that a journalist's Facebook post was taken down after he was expelled from Syria. In the post, Rida al-Basha, who worked for the Lebanese television outlet Al-Mayadeen, criticized the treatment of journalists in Syria by asking, "Why did you promulgate a media law if you apply to journalists the laws that are used to prosecute murderers, drug traffickers and thieves?" [2] It is unclear why the post was taken down, but journalists have often expressed their frustrations on the situation in Syria and then taken down their posts for fear of reprisals (see B4).

In July 2018 a journalist in Damascus was forced to remove a Facebook post on living conditions in the country after security services instructed him to abstain from discussing such matters. [3] Separately that September, an activist was urged by his organization's management to "unlike" a Facebook post by someone who had previously been critical of President al-Assad; the organization had received a call of complaint from one of the security services. [4]

In the past, authorities have forced the owners of some websites to shut them down, and according to the digital security organization SecDev, Facebook has suspended the pages of dozens of opposition groups, media outlets, and independent nongovernmental organizations (NGOs) over the years. [5] Activists have expressed suspicion that Facebook users sympathetic to President al-Assad may be filing complaints against the pages en masse to trigger their suspension for violating user guidelines. In late 2013, Razan Zeitouneh of the Violations

TOP

Documentation Center shared a letter urging Facebook to keep such pages open, stating that “Facebook pages are the only outlet that allows Syrians and media activists to convey the events and atrocities to the world.” [6] Representatives from Facebook have cited the difficulties of distinguishing between legitimate and fabricated complaints, particularly since many armed extremists use the platform.

Activists and human rights advocates expressed dismay that thousands of videos and dozens of channels documenting war crimes and human rights abuses were removed from YouTube beginning in mid-2017, after the platform applied a "machine learning" algorithm to identify any content that could violate its terms of service. Between January and April 2019, some 34 Syria-related YouTube channels were removed. [7] Some of these channels belonged to media organizations with a long history of documenting human rights violations in the country since 2011. YouTube has since restored a number of channels and reposted thousands of clips that were mistakenly removed.

As of December 2019, there were no cases of takedown requests from Syria in Facebook’s Transparency Report. [8]

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**0** / 4

Decisions surrounding online censorship lack transparency, and ISPs do not publicize the details of how blocking is implemented or which websites are banned, though government officials have publicly admitted to engaging in such censorship. When users seek access to a blocked website, they receive a blank page or an error message implying a technical problem. The STE is known to implement blocking decisions; it is unclear which state agencies typically makes the decisions, though security and intelligence bodies are believed to play an important role. Following a request to unblock the news site Al-Nazaha in 2008, the Ministry of Communications and Technology informed a court that “the

TOP

website was blocked under the direction of Branch 225," [1] one of the branches of the Military Intelligence Directorate.

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**0** / 4

Self-censorship is widespread online, and it has increased in recent years as users contend with arbitrary redlines as well as threats and violent reprisals for critical content (see C7). Sensitive topics include President al-Assad, his late father, the military, the ruling Baath Party, and influential government officials. Subjects such as religious and ethnic tensions and corruption allegations related to the president's family are also off-limits. Most users are careful to avoid dangerous topics and refrain from visiting blocked websites. [1] Given the government's surveillance capabilities, there is a risk in accessing even unblocked sites that are associated with the opposition.

Mohamad Harsho, the editor of the website Hashtag Syria, was arrested in April 2019 for posting an article about a government plan to increase fuel prices; other journalists and online users have been wary of commenting about fuel prices online (see C3). [2]

Some outlets and journalists have stopped publishing in response to government pressure and harassment. After dozens of prosecutions and arrests of journalists over the preceding two years, in mid-2019 three journalists announced that they had stopped their work in the profession. For example, in May 2019, Ali Hassoun, editor in chief of *Al-Ayam* newspaper, announced that he would retire from journalism, stating that the current period was "the harshest in the history of the Syrian press due to escalating restrictions on the freedom of press." [3] *Al-Ayam* has since halted publication because of "the crisis affecting media work in Syria." [4]

TOP

In December 2018, the office of the news site Damascus Now, one of the largest progovernment outlets, was raided and its director and founder, Wissam al-Tayr, was arrested (see C3 and C7). Some reports noted that

al-Tayr had posted a poll about the fuel crisis on Facebook before he was detained; [5] he had announced plans to conduct a series of polls on government performance. [6] The outlet ceased all publishing, including on social media, though it resumed activity several weeks later. [7]

According to activists and journalists, the absence of information regarding al-Tayr's fate and another journalist's suspension from work over a Facebook post were intended to intimidate and deter internet users from discussing matters related to living conditions, corruption, and fuel prices. Similarly, other attacks and assassinations targeting digital activists and journalists have forced many to self-censor their publications and social media interactions (see C7). [8]

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**1** / 4

The government and its allies have employed a range of tactics to manipulate online content and discredit unfavorable news reports, though it is often difficult to attribute these actions directly to the regime. The Syrian Electronic Army (SEA), a progovernment activist group, hacks the websites of opposition forces, human rights organizations, and foreign media outlets (see C8). Journalists with domestic outlets sometimes receive telephone calls from government officials who issue "directions" on how to cover particular events. [1] The government also supports and promotes websites that provide progovernment coverage. These outlets typically rely on the reporting of the official Syrian Arab News Agency (SANA), with the same wording often evident across multiple sites.

According to the Syrian Observer, in recent years the semiofficial media apparatus in Syria has stepped up its efforts to "regulate the image and flow of information through communication sites and limits that to images and information which it approves." [2]

TOP

During the coverage period, there was an increase in progroverment media-sponsored hate speech. According to a study by the Syrian Center

for Media and Freedom of Expression, proregime hate speech is used more often by progovernment media than by opposition media or those active in Kurdish-controlled areas. The report noted that the government has significant influence on the media narrative and that outlets follow "a central authority represented by the Ministry of Information and then the security authorities, which makes their editorial policy unified and well-studied towards the promotion of the Syrian regime's political discourse." [3]

In a February 2020 Middle East Eye article, a number of journalists expressed their dismay at the lack of independence among some foreign-backed opposition media projects, noting their highly inaccurate reports promoting the rebel Free Syrian Army, which had a negative impact as people lost confidence in local media. [4]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**0** / 3

International sanctions that restrict financial transactions with Syria have made it difficult for residents to purchase a domain or host their websites in countries such as the United States, among other key services related to content publication. For instance, the magazine *Syrian Oxygen* was unable to obtain SSL certificates for its website from US providers in 2016, apparently because the domain Syrianoxygen.com contains the word "Syria." In November 2018, Coursera and Udemy, which offer online courses, blocked their sites in Syria due to sanctions implemented by the United States. [1] A large number of students in Syria relied on these platforms, as they were unable to attend university due to conflict-related blockades or mandatory military service. [2] The move forced many students to resort to using a VPN to reach the blocked platforms, which threatened to further weaken their already slow internet connections.

TOP

B7 0-4 pts

Does the online information landscape lack diversity?	**1** / 4

With the onset of the civil war, a proliferation of citizen journalism and social media activism provided the Syrian public with an alternative view of domestic events, [1] especially as trust in state media outlets declined. [2] Facebook is commonly used as a news source, and citizen journalists still cover the conflict through this and other social media platforms (see B8). However, factors including the government's military gains and the expansion of website blocking have limited the diversity of information available in more recent years (see B1). While Facebook hosts a variety of sources, ordinary users are fearful of accessing certain pages in light of state surveillance. *Enab Baladi*'s Facebook page is accessible, for example, but many users would be reluctant to visit and read full articles, given that *Enab Baladi* is an opposition outlet.

In areas under government control, some activists and journalists have had to use a VPN in order to obtain information from websites blocked by the STE, such as *Enab Baladi*, whose site was blocked repeatedly between 2017 and 2019, and those of NGOs including the Syrian Observatory for Human Rights. [3]

Because of the economic situation and the Ministry of Communications and Technology's decision to implement "internet rationing" in March 2020, many users must limit their internet activity to basic necessities, such as communicating with family and friends. This means avoiding news reports, especially videos, which would quickly consume or exceed their monthly data limits (see A2). The system has effectively allowed the Syrian regime to limit access to unfavorable content without directly blocking it. [4]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**4** / 6

TOP

Online tools have proven crucial for Syrians inside and outside the country who seek to document human rights abuses, campaign for the

release of imprisoned activists, or disseminate news from the front lines of the conflict.

One project called the Syria Observatory consists of channels on social media networks that are linked to other observatories inside Syria; the group aims to reduce the number of casualties and damage caused by air strikes by spreading detailed warnings of approaching warplanes. The observatory works largely through a Telegram channel and the Facebook Messenger application. [1] Communication platforms have become particularly important for other purposes. For example, the US-based Syrian American Medical Society has used WhatsApp to conduct telemedicine. [2]

The civil war has been called the first “YouTube war” due to the volume of human rights violations, military battles, and postconflict devastation that has been captured in videos posted to the site. [3] Indeed, as the government shifted to the use of heavy arms and missiles against opposition fighters early in the conflict, the role of citizen journalists shifted from live event coverage to documentation of the bloody aftermath of attacks. Although many obstacles stand in the way of media coverage, citizen journalists have developed techniques to deliver reporting from remote areas and conflict zones. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, rebel groups, and civil society organizations, mostly documenting attacks.

Many Syrians use Facebook to share news, discuss events, release statements, and coordinate both online and offline activities. [4] In January 2020, residents of Al-Suwayda Governorate in southern Syria used the platform to call for several protests against corruption and deteriorating economic conditions under the campaign slogan "We Want to Live." [5] Activists have also used WhatsApp groups to organize demonstrations, with the caveat that there are no political dimensions to the mobilizations and that the goals are purely socioeconomic, since many people will not participate in any political activity for fear of arrest and prosecution (see B4).

TOP

In July 2019, having spent more than seven years in the Syrian army, a number of soldiers and their families launched a Facebook campaign to end their military service and appealed to President al-Assad under the slogan "We Want to Be Released." According to the law, obligatory military service lasts up to 18 months, but few conscripts and reserve soldiers have been allowed to end their service since the conflict began in 2011. [6]

In October 2018, residents of Al-Suwayda Governorate used Facebook and WhatsApp to organize a sit-in to demand that the government negotiate with the Islamic State (IS) militant group for the release of kidnapped civilians. [7] In November of that year, activists in the city of Idlib issued a statement via Facebook calling for a vigil in front of the Ministry of Justice to protest conditions in HTS-controlled areas, including kidnappings and arrests and the deterioration of the security and economic situation. [8]

Despite such mobilization efforts, civic activists using online tools face daunting obstacles. Many have left Syria for Turkey after receiving threats or being arrested, and authorities have reportedly filtered text messages on dates close to scheduled demonstrations (see B1).

C. Violations of User Rights

Journalists and media activists, including those aligned with the regime, were reportedly abducted and detained by HTS during the reporting period, and others have been tortured while in detention. Government surveillance remains a problem, and during the coronavirus pandemic there were reports of malicious mobile applications with links to the government being disguised as COVID-19 tracking apps.

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**TOP** **0** / 6

While freedom of speech and the press are protected by the constitution, these rights are not respected in practice. The judiciary lacks independence, and its decisions are often arbitrary. Some civilians have been tried before military courts.

Law Number 9, enacted in March 2018, established specialized courts for criminal cases related to communications and technology. [1] Some analysts viewed the creation of such courts as a positive step; judges on the new courts would be specially trained to handle technology issues. However, the general lack of judicial independence in Syria also led to concerns that the law would be used to further suppress freedom of expression and criminalize critics of the regime. It is unclear how specifically the law has been put into action.

While a 2011 media law, Decree 108, ostensibly prohibits the arrest of journalists, other clauses, including those related to national security, undermine freedom of expression. [2] Journalists continue to be arrested under other laws in practice.

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	**0** / 4

Laws such as the penal code, the 1963 State of Emergency Law, and the 2001 Press Law are used to control traditional media and arrest journalists or internet users based on vaguely worded violations such as "threatening national unity" or "publishing false news that may weaken national sentiment." [1] Defamation offenses are punishable with up to one year in prison if the comments target the president and up to six months in prison for libel against other government officials, including judges, military personnel, or civil servants. [2] The 2012 cybercrime law allows prison sentences of up to three years and fines of up to 250,000 Syrian pounds ($1,160) for anyone who incites or promotes crime through computer networks. [3]

TOP

In a March 2019 interview, the leading public prosecutor for information and telecommunication crimes, Hibatullah Mohammed Seifo, said the penal code criminalizes the publication on social media of false news that causes fear and panic, with prison sentences ranging from three years to 15 years with hard labor. Article 287 stipulates that the broadcasting of false or exaggerated news abroad that undermines the prestige of the state or its financial standing is subject to a minimum prison sentence of six months, in addition to a fine of up to 10,000 pounds ($47). Article 309 similarly criminalizes the broadcasting of false news or claims that undermine confidence in the "state currency." [4] The ambiguity of these articles provides the authorities with broad discretion to arrest journalists and activists.

C3 0-6 pts

Are individuals penalized for online activities?	**1** / 6

Since antigovernment protests broke out in 2011, the authorities have detained large numbers of internet users, including well-known bloggers and citizen journalists. While it is difficult to obtain information on recent arrests, some 28 professional and citizen journalists and media assistants, including bloggers and online activists, were imprisoned as of 2020, according to Reporters Without Borders. [1]

Pressure against generally progovernment journalists, including through arrests, was observed during the coverage period. [2] Between July 2018 and July 2019 at least 13 progrovernment Syrian journalists were charged or threatened by Syrian intelligence forces in relation to what they reported, including online content. According to Reporters Without Boarders, the most common charges are "undermining the nation's morale and harming the prestige of the state." [3]

In May 2020, journalist Nada Mashraki was arrested, and her personal Facebook page was deactivated. Mashraki is the editor for Latakkia News Network, a Facebook news page with more than 180,000 subscribers. Her husband, who helps run the outlet, was also arrested. She was

TOP

accused of “publishing false news to undermine the prestige of the state and insulting the judiciary” after writing a story about judicial corruption in Syria. [4] As of June 2020 neither Mashraki nor her husband had been released.

Journalist Mohamad Harsho, founder of the Hashtag Syria website, was arrested in April 2019 after publishing an article about the government's plans to end gasoline subsidies. Harsho was released after the intelligence authorities obtained guarantees that the outlets would withdraw the article and issue an apology. [5] Also that April, war correspondent Raef Salameh was arrested and detained for a month on charges of managing a Facebook page that was critical of the Ministry of Health. [6] In July 2019, journalist Rabea Kalawandy was arrested without explanation and then released a month later.

In December 2018, authorities raided the office of the news website Damascus Now and arrested its director, Wissam al-Tayr; his colleague, Sonail Ali, was arrested several days later and released after 10 days. [7] The raid took place two days after al-Tayr wrote on Facebook that Damascus Now would begin conducting opinion polls in order to evaluate the performance of government ministries (see B4). [8] Al-Tayr’s whereabouts remained unknown during the coverage period, but according to reports published in August 2019, he was released after being detained for months (see C7). [9]

In February 2020, doctor and activist Amjad Badran was imprisoned for five days. According to his Facebook page, he was arrested because of a comment posted to the page from a fake account, though the nature of the comment was not specified. Badran had previously been detained for three days in May 2019 due to a post on his Facebook page that criticized a government official. [10]

Other human rights activists who work online have also been targeted. Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in 2012, arresting 14 employees. [11] One SCM member and civil rights blogger, Razan Ghazzawi, [12] was detained for 22

TOP

days. [13] The other members were released in 2015 after three years in pretrial detention.

The militant group HTS has detained a number of journalists and activists in areas under its control. In June 2019, HTS seized media activist Maan Bakkour at his home in the Idlib countryside and confiscated his equipment without explanation. As of June 2020, he had not been released. [14] In July 2019, a correspondent from the newspaper *Zaman al-Wasl*, Jumah Haj Hamdo, was detained in the western countryside of Aleppo without explanation. He was freed a week later. [15] Similarly, in September 2019, media activist Ahmed Rahhal was seized after members of HTS raided his house in Idlib and confiscated his media equipment. He was reportedly targeted because he published a video attacking the leadership of HTS and accusing them of corruption and plundering of funds. [16] As of June 2020, he had not yet been released. In November 2019, HTS released journalist Amjad al-Maleh after a two-year detention; [17] the militant group had reportedly "sentenced" al-Maleh to death on spying charges in December 2018. [18] In December 2019, the South African journalist Shiraz Mohamed was released after three years in detention, apparently by one of the groups affiliated with HTS. [19]

The Syrian Ministry of Interior's branch for combating information crimes has summoned a number of journalists for questioning about content posted online. The journalist Bilal Soleiteen, editor of the website Syrian Snack, was summoned to the branch for three days in May 2019. [20] In September 2019, lawyer Aahed Koujah was summoned, investigated, and detained for a day by the information crime branch for a post on her Facebook account in which she criticized the judiciary. [21]

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**2** / 4

TOP

According to the 2011 media law, applicants seeking government accreditation for a media website must confirm the identities of its owners and hosts. [1]

Anonymous communication online is restricted, but remains possible. Although registration is required to purchase a mobile phone, in recent years activists have used the SIM cards of slain friends and colleagues in order to shield their identities. Mobile phones from neighboring countries like Turkey and Lebanon have also been widely used since 2012.

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	**0** / 6

The breadth of state surveillance violates users' right to privacy.

Activists and bloggers released from custody have reported that they were pressured by security agents to provide the passwords for their Facebook, Gmail, Skype, and other online accounts. [1]

In April 2020, researchers found 71 malicious mobile applications associated with a single server whose IP address was held by Tasawul, the internet provider owned by the STE. One of these applications took advantage of the COVID-19 pandemic situation, claiming to test body temperature when in fact it was obtaining sensitive information from victims' devices, for instance by taking screenshots, identifying geolocation, and accessing the phone's cameras and voice recordings. [2]

Sophisticated phishing and malicious-software attacks that target online activists for surveillance began to be reported in 2012. [3] The US-based Electronic Frontier Foundation (EFF) found that malware programs called Darkcomet RAT (remote access tool) and Xtreme RAT had been found on activists' computers and were capable of capturing camera images, logging keystrokes, stealing passwords, and more. Both applications sent the data back to the same IP address in Syria and were circulated via email and messaging platforms. [4] Later, EFF reported the appearance of a fake YouTube channel carrying opposition videos that requested users' log-in information and prompted them to download an update to Adobe Flash, which was in fact a malware program that enabled data to be stolen from their computer. Upon its discovery, the fake channel was

TOP

taken down. [5] Exploiting the need for circumvention and encryption tools among activists and opposition members, authorities have developed fake Skype encryption programs and a fake VPN application, both containing harmful software. [6]

A 2014 report by Kaspersky Lab revealed that some 10,000 victims' computers had been infected with RATs in Syria, as well as in other Middle Eastern countries and the United States. The attackers sent messages via Skype, Facebook, and YouTube to dupe victims into downloading surveillance malware. One file was disguised as a spreadsheet listing the names of activists and "wanted" individuals. The perpetrators, though not identified, were found to be from Syria and Russia, based on the IP addresses of the command and control servers. Moreover, one of the IP subnets led back to the STE. [7]

A 2018 Citizen Lab report revealed that "middleboxes were being used" by Turk Telecom, one of the cross-border ISPs in northern Syria, "to redirect hundreds of users attempting to download certain legitimate programs to versions of those programs bundled with spyware." [8] The report added that "targeted users in Turkey and Syria who downloaded Windows applications from official vendor websites including Avast Antivirus, CCleaner, Opera, and 7-Zip were silently redirected to malicious versions by way of injected HTTP redirects." This affected a number of devices used by the YPG. Since January 2018, the YPG have been attacked by Turkish air and ground forces operating in northern Syria.

Some activists attributed the 2011 unblocking of Facebook and YouTube to the government's desire to monitor online activities. In recent years, authorities have utilized ThunderCache software and technology from the Italian company Area SpA for surveillance (see B1).

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	TOP **0** / 6

Surveillance is rampant on domestic ISPs, which are closely aligned with government security forces. Cybercafé owners are compelled to monitor and record their customers' activities (see A4).

The 2012 Law for the Regulation of Network Communication against Cybercrime requires websites to clearly publish the names and details of their owners and administrators. [1] The owner of a website or online platform is also required "to save a copy of their content and traffic data to allow verification of the identity of persons who contribute content on the network" for a period of time to be determined by the government. [2] Failure to comply may cause the website to be blocked and is punishable by a fine of 100,000 to 500,000 pounds ($470 to $2,300). If the violation is found to have been deliberate, the website owner or administrator may face three months to two years in prison as well as a fine of 200,000 to 1 million pounds ($930 to $4,700). [3]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	**0** / 5

Once in custody, citizen journalists, bloggers, and other detainees frequently endure beatings and torture at the hands of government authorities. Lethal violence is also a concern; according to Reporters Without Borders, a total of 10 journalists, citizen journalists, and media assistants were killed in Syria in 2019, and two additional journalists were killed in February 2020. [1]

Home raids and the seizure of property by authorities continued throughout the coverage period, as did harassment and torture of online activists held in Syrian prisons.

In July 2019, a prison official reportedly informed the family of media activist Alaa Nayef al-Khader that he had died under torture in Sednaya Military Prison after more than two years in detention. [2] In August 2019, the family of activist Samer al-Saloum was informed that he had been executed by HTS after being held by the militant group for a year and a

TOP

half. Saloum was responsible for the printing and distribution of the political magazine *Alghorbal*, which included anti-HTS content. [3]

In November 2018, masked gunmen assassinated activists Raed Fares and Hamoud Junaid in the town of Kafranbel in the Idlib countryside, which is controlled by HTS. Fares was the director of the local Radio Fresh, which is broadcast on platforms including YouTube and SoundCloud and has criticized hard-line groups such as HTS. He had previously been arrested by the same group for broadcasting music, after which he replaced the music with animal noises. He was also asked not to host women as guests, but instead he added sound effects to women's voices to make them resemble those of men. [4] Junaid was a journalist and photographer for Radio Fresh. [5]

In December 2018, authorities raided the office of the news website Damascus Now and arrested its director, Wissam al-Tayr (see C3). The raid took place two days after he wrote on Facebook that Damascus Now would begin conducting opinion polls in order to evaluate the performance of government ministries. [6] In June 2019, HTS seized media activist Maan Bakkour at his home in the Idlib countryside and confiscated his equipment without explanation. [7] Similarly, in September 2019, HTS fighters raided the Idlib home of media activist Ahmed Rahhal, confiscating his media equipment and taking him to an unknown location (see C3). [8] He apparently remained in HTS custody at the end of the coverage period.

In June 2020, it was reported that HTS fighters had beaten and abused 13 journalists who were covering a joint Turkish-Russian patrol in northern Idlib Governorate. The militants also smashed the journalists' equipment. In the past HTS leaders have threatened to kill journalists for covering anti-HTS protests in the area. [9]

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**TOP** **0** / 3

While the SEA, a group of progovernment hackers, pioneered technical attacks against the opposition early in the conflict, numerous hacker groups linked to Hezbollah, IS, Russia, and Iran have also developed operations in Syria.

In 2016, Citizen Lab published research on Group 5, a hacker collective noted for its use of "Iranian Persian dialect tools and Iranian hosting companies." [1] It established websites with names such as AssadCrimes as part of its elaborate social-engineering schemes. [2] The AssadCrimes site contained articles lifted from a Syrian opposition blog and was falsely registered under the name of Nour al-Ameer, a prominent opposition activist. The perpetrators 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 their networks. Once trust was established, the attackers targeted victims with RAT programs and gained access to their devices.

According to the cybersecurity group FireEye, Russia's Federal Security Service (FSB) stepped up technical attacks against Syrian human rights organizations and opposition groups beginning in 2015 in a major campaign to glean intelligence and disrupt coverage of human rights violations by Russian forces. [3] Separately, in late 2014, Citizen Lab released a report on malware attacks targeting groups that documented human rights abuses committed by IS. [4]

In May 2018, it was reported that the SEA was continuing to target activists and dissidents, including by sending links—via popular communications platforms such as WhatsApp and Telegram—that would trick them into installing malware. [5] Previously, the SEA had drawn attention by hacking major international media outlets and organizations, including the websites of the *New York Times*, [6] the US Marine Corps, [7] Facebook, [8] Human Rights Watch, [9] *Forbes*, [10] and the *Washington Post*. [11] A December 2018 briefing at the Black Hat conference revealed that the SEA has used a malware program called SilverHawk, which is delivered through fake updates of communications applications, or via fabricated versions of popular programs such as Microsoft Word and YouTube. SilverHawk malware allows perpetrators to

TOP

access data once a targeted user accepts the fake programs with a Google Android device, and it can activate an infected phone's microphone and camera. [12]

Though the SEA's precise relationship with the regime is unclear, there is evidence of links to or support from the government. The SEA registered its domain in 2011 on servers maintained by the regime-affiliated Syrian Computer Society. [13] In a 2011 speech, President al-Assad explicitly praised the SEA and its members, [14] and state-run media have provided positive coverage of the group's actions. [15]

On Syria

See all data, scores & information on this country or territory.

See More ›

Country Facts

Global Freedom Score
0 /100 **Not Free**

Internet Freedom Score
17 /100 **Not Free**

Freedom in the World Status
Not Free

Networks Restricted
Yes

Social Media Blocked
No

Websites Blocked
Yes

TOP

Pro-government Commentators
Yes

Users Arrested
Yes

In Other Reports

Freedom in the World 2020

Other Years

2019

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org

TOP