Syria
Not Free
17
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

Overview

Internet freedom remained heavily restricted in Syria. While no major internet shutdowns occurred during the coverage period, blocking of numerous websites persisted. Moreover, individuals continued to face a serious risk of violence in reprisal for their online activity.

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 an ongoing civil war. The regime prohibits genuine political opposition and harshly suppresses
freedoms of speech and assembly. Corruption, enforced disappearances, military trials, and torture are rampant 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, 2018 - May 31, 2019

- Unlike in previous years, no major internet shutdowns were reported during the coverage period. However, the regime of President Bashar al-Assad maintains a tight grip on the internet infrastructure in areas under its control (see A1).

- State authorities reimposed blocks on the independent websites Enab Baladi and SouriaLi Radio, which had been unblocked in 2017. A variety of other websites, including those of human rights groups and online tools used to circumvent censorship, remained blocked during the coverage period (see B1).

- A number of progovernment journalists were arrested, including Wissam al-Tayr in December 2018; al-Tayr's whereabouts remained unknown as of late 2019. Also in December 2018, the Islamist militant group Hay'at Tahrir al-Sham (HTS) reportedly issued a death sentence against media activist Amjad al-Maleh (see C3).

- In November 2018, activists and journalists Raed Fares and Hamoud Junaid were shot dead by masked gunmen in Idlib Governorate. Both were affiliated with Radio Fresh, which is broadcast on platforms including YouTube and SoundCloud and has criticized militant groups like HTS (see C7).

A Obstacles to Access

Mobile phone subscriptions and internet penetration increased during the coverage period, and unlike in previous years, no major internet shutdowns were observed. Nonetheless, the government maintains a tight grip on the internet infrastructure in
the territory under its control, which has expanded since 2015.

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

Syria’s telecommunications infrastructure is one of the least developed in the Middle East, and broadband connections are difficult to acquire.\textsuperscript{1} Conditions worsened after 2011, with electricity outages increasing 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 reclaimed a large amount of territory during the coverage period,\textsuperscript{2} telecommunications services in the recaptured areas remained limited.\textsuperscript{3} Parts of the country that are not held by the government have developed alternative, decentralized systems for securing internet connectivity.

According to a January 2019 report by DataReportal, internet penetration reached 33 percent, up from 30 percent the previous year.\textsuperscript{4} The number of mobile phone subscriptions per 100 residents increased from 90 in 2017 to 98 in 2018.\textsuperscript{5} Average fixed-line connection speed increased by 17 percent, to 8.07 Mbps, while average mobile connection speed rose by 54 percent, to 18.23 Mbps, between 2018 and 2019.\textsuperscript{6}

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.\textsuperscript{7}

\begin{itemize}
  \item \textsuperscript{1} Kyle Wansink, Syria - Telecoms, Mobile, Broadband and Forecasts, BuddeComm, \url{http://bit.ly/1OdycSD}.
  \item \textsuperscript{2} https://www.bloomberg.com/news/articles/2019-01-14/who-s-still-fighting...
  \item \textsuperscript{3} Communication with Syrian activists, February 2019. Signal call
  \item \textsuperscript{6} https://datareportal.com/reports/digital-2019-syria
  \item \textsuperscript{7} Launch of 4G service at Damascus International Fair. Al Watan newspaper.
\end{itemize}
Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?

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, the main mobile service providers, 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.\(^4\) The average monthly per capita income is 33,000 pounds ($154).\(^5\)

About half of the country is disconnected from Syrian internet service provider (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, who 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.\(^6\)

---

\(^1\) Kyle Wansink, Syria - Telecoms, Mobile, Broadband and Forecasts, BuddeComm, \texttt{http://bit.ly/1OdycSD}.


\(^4\) Communication with Syrian activists, February 2019. Signal call

\(^5\) Labor Observatory for Studies and Research, “The Syrian’s living costs are 7 times higher than his income”. [Arabic] June 6, 2017, \texttt{http://syriasteps.com/?d=126&id=151984&in_main_page=1}.

\(^6\) "Syrian company provides "Internet" service in the town of Sarmin Idleb", 12
Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?

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

In January 2018, when Turkish forces initiated a military offensive in the Afrin area against the People’s Protection Units (YPG), a Syrian Kurdish militia, Turkish authorities cut off internet service for most of northern Syria. The following month, the jihadist militant group HTS (formerly 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. In government-controlled areas, Syrian 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.

In October 2018, the Syrian Telecommunication Regulatory Authority (SYTRA) revealed that it was considering a ban on voice over internet protocol (VoIP) services, such as WhatsApp, in order to mitigate revenue losses for the traditional telecommunications sector. However, WhatsApp and other VoIP services had not been blocked at the end of the coverage period.

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. 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). While users in northern Syria continue to rely on Turkish networks for internet service, Syrian networks are the main source of internet access in central and southern Syria, where the government and its allies have recovered most territory.

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. 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, 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
While the number of ISPs has increased, entry into the market remains difficult due to the country’s instability and resulting damage to infrastructure. Independent satellite-based connections are prohibited, although they are still heavily employed due to the damage that information and communication technology (ICT) infrastructure has sustained as a result of the conflict. ISPs and cybercafés operating in government-controlled areas must obtain a permit from the STE and another security permit from the Interior Ministry. 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 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. 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. 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. Any new mobile provider would also have to create its own infrastructure.

1. Interview with former employee of the intelligence service, Communications Department, 9 March 2019. Signal call
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?

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

B Limits on Content

The government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. At least two opposition websites were blocked 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?

Authorities block access to a variety of online materials. While some sites were unblocked in previous years, new blocks 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 territories, 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 political, cultural, social, or economic policies; criticism of specific high-level government officials; and sites that expose official corruption.

Authorities blocked several Syrian opposition websites during the coverage period, including the newspaper Enab Baladi and SouriaLi Radio, after unblocking them in 2017. The targeted outlets were significant sources of independent information. Even some progovernment journalists relied on the sites for news on regions under opposition control.

A number of other websites remained blocked, including that of the Kuwaiti newspaper Al-Seyassah, the sites of human rights groups such as the Syrian Observatory for Human Rights, and Souriatna, a magazine that offers the perspectives of young Syrians. As of May 2019, the previously blocked Syrian Human Rights Committee website appeared to be accessible.

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. 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.

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 unblocked the sites 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. Skype has suffered frequent disruptions, either due to low speeds or intermittent blocking by authorities.

Antivirus software and updates to operating systems remain blocked due to US sanctions. 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. 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.” Authorities have also used technology provided by the Italian company Area SpA to improve their censorship and surveillance capabilities, according to evidence from 2011. Analysis revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites. The Wall Street Journal identified efforts that year to block or monitor tens of thousands of opposition websites or online forums covering the uprising.

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.

- 1. While the precise timeline cannot be determined, Enab Baladi was blocked sometime between September and October 2018 and Souriali Radio after March 2018, based on communications with a source in Damascus and internal research.
- 5. "Syrian government: Sex is forbidden", Al-Akhbar newspaper 25 Abril 2018,
[In Arabic], https://al-akhbar.com/Media_Tv/248822


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?

Censorship of news sites and social media content in government-controlled areas remained severe and appeared to intensify somewhat during the coverage period. For example, 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. An activist was urged by his organization’s management in September 2018 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.3

In the past authorities have forced the owners of some websites to shut them down, and according to digital security organization SecDev, Facebook has suspended the pages of dozens of opposition groups, media outlets, and independent nongovernmental organizations (NGOs) over the years.4 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 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.”5 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 in mid-2017, after the platform applied a "machine learning" algorithm to identify any content that could violate its terms of service. YouTube has since restored a number of channels and reposted thousands of clips that were mistakenly removed.

- 1. Interviews with several senior journalists in Damascus
- 2. Interview with a Syrian journalist, located in areas controlled by the Syrian government, March 2019. Signal call
- 3. Interview with Syrian blogger, located in areas controlled by the Syrian government, March 2018. Signal call
- 5. https://www.theatlantic.com/international/archive/2014/02/the-syrian-op...

B3 0-4 pts
Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?04

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 agency 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 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?

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, or influential government officials. Subjects including 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.

Websites have censored themselves in response to government pressure. After the office of the news site Damascus Now was raided in December 2018 and its director, known as Wissam al-Tayr, was arrested (see C3 and C7), the outlet ceased all publishing, including on social media.\(^2\) When it resumed activity several weeks later, no mention was made of al-Tayr’s arrest and disappearance.
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 (see C7) is intended to intimidate and deter internet users from discussing matters related to living conditions and corruption. Similarly, other attacks and assassinations targeting digital activists and journalists (see C7) have forced many to self-censor their publications and social media interactions.3

1. Email from an anonymous Syrian blogger.
2. https://www.syja.org/uploads/advance_content/file/advance_content_4_vio...
3. Interview with a Syrian activists and journalists, located in areas controlled by the Syrian government, February - March 2019. Signal call

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? 14

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 groups, 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 SANA, the official state news agency, with the same wording often evident across multiple sites.


B6 0-3 pts
Are there economic or regulatory constraints that negatively affect users’ ability to publish content online? 03

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, 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 because they were unable to attend university due to conflict-related blockades or mandatory military service.2

2. Discussions on Facebook pages and other online groups, spring 2019.

B7 0-4 pts
Does the online information landscape lack diversity? 14

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 (see B1) have limited the diversity of information available in more recent years. 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.


B8 0-6 pts
Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly on political and social issues?

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, and disseminate news from the front lines of the conflict. Communication applications have become particularly important. A WhatsApp group called the Monitors was created by people in regime-controlled areas to warn individuals living in rebel-controlled territories of impending Syrian and Russian air raids.1 The US-based Syrian American Medical Society has used WhatsApp for telemedicine, in one instance guiding a veterinarian who delivered twin babies by caesarean section in the besieged town of Madaya.2 Activists have also established the Syria Observatory, a group of channels on social media networks linked to other observatories inside Syria; the group aims to reduce the number of casualties and damage caused by air strikes by spreading warnings of approaching warplanes, including their whereabouts, potential targets, and estimated arrival times, in addition to the exact time of observation. The observatory works through a Telegram channel and a Facebook Messenger application.3

Many Syrians are active on Facebook, using it as a platform to share news, discuss events, release statements, and coordinate both online and offline activities.4

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.5 Indeed, as the government shifted to the use of heavy arms and missiles against opposition fighters earlier in the conflict, the role of citizen journalists shifted from live event coverage to documenting 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.

In October 2018, residents of As-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.6 In November 2018, 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.7

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, including those aligned with the regime, were detained during the coverage period, and one was disappeared. A media activist was reportedly sentenced to death by HTS and others have been tortured while in detention. Two activists and journalists who were critical of extremist groups such as HTS were shot dead by masked gunmen in Idlib.

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?

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.

In March 2018, the government passed Law Number 9, which established specialized courts for criminal cases related to communications and technology. Some analysts view the creation of such courts as a positive step; judges on the new courts will be specially trained to handle technology issues. However, the lack of judicial independence in Syria has led to concerns that the law could be used to further suppress freedom of expression and criminalize critics of the regime.

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.

- 1. “While choosing the judges according to this law, it should be considered that they have been trained on combating communication and technology crimes, or have gained practical experience in such kind of cases”. Article 6 of Act No. 9 of 2018. Syrian Arab News Agency. 25 March 2018. [Arabic]. https://www.sana.sy/?p=730729

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?

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.” 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. 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

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 provide the authorities with broad discretion to arrest journalists and activists.

1. Syrian Penal Code, art. 285, 286, 287

C3 0-6 pts
Are individuals penalized for online activities? 16

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 two dozen professional and citizen journalists, including bloggers and online activists, were imprisoned as of 2019, according to Reporters Without Borders. 1
Pressure against generally progovernment journalists, including through arrests, was observed during the coverage period. In December 2018, the office of the news website Damascus Now, one of the largest progovernment outlets, was raided, and its director, known as Wissam al-Tayr, was arrested; his colleague, Sonail Ali, was arrested several days later and released after 10 days. Al-Tayr’s whereabouts remained unknown at the end of the coverage period (see C7). 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.

Rida al-Basha, a reporter for the pro-Damascus Lebanese television channel Al-Mayadeen, was issued an arrest warrant in November 2018 at the request of a Baath Party leader; al-Basha had criticized Aleppo’s municipal elections and called for a boycott on his personal Facebook account. The case was ultimately dropped.

In July 2018, the Ministry of Interior’s information crimes branch arrested Ammar al-Ezzo, the director of a press office in Aleppo, on the charge of managing an anonymous website that publicizes cases of corruption by state officials. The same branch arrested war photographer Amer Diraw in August for sending information to the website. It was later revealed that a senior official in the Baath Party had filed a case against them; Diraw was released in December after his family convinced the party leader to drop the case, and al-Ezzo appeared to have been released by the end of the coverage period.

Human rights activists who work online are also targeted. Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in 2012, arresting 14 employees. One SCM member and civil rights blogger, Razan Ghazzawi, was detained for 22 days. The other members were released in 2015 after three years in pretrial detention.

HTS forces arrested a number of digital activists in Idlib Governorate on various charges, such as “media work against HTS.” This charge was leveled against media activists Amjad al-Maleh, Hussam Mahmoud, Hassan Younis, and Bakr Younis when they were arrested in December 2017. Hussam Mahmoud was released in June 2018, and Hassan Younis and Bakir Younis were released in January 2018. In December 2018, Amjad al-Maleh reportedly received a death sentence for “giving coordinates of positions of the Lebanese Hezbollah and the Islamic State.
organization to Israel and the International Coalition." However, according to a January 2019 report from Human Rights Watch, an HTS representative “said that al-Maleh, whose whereabouts remain unknown, had not been sentenced to death.”

- 2. https://syrianobserver.com/EN/features/48993/the-regime-punishes-promin...
- 5. https://www.syja.org/en/home/periodic-reports/36/advance-contents/31533...
; https://www.enabbaladi.net/archives/262277
- 7. https://www.syja.org/uploads/advance_content/file/advance_content_4_vio...
- 8. some Facebook pages are saying that he was released. [in Arabic] https://bit.ly/2VYTakI

C4 0-4 pts
Does the government place restrictions on anonymous communication or encryption?

According to a 2011 media law, applicants seeking government accreditation for a media website must confirm the identities of its owners and hosts.
Anonymous communication is possible online, but it is restricted. Registration is required to purchase a mobile phone, and 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 been widely used since 2012.


C5 0-6 pts
Does state surveillance of internet activities infringe on users’ right to privacy?

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

Activists and bloggers released from custody have reportedly been pressured by security agents to provide the passwords for their Facebook, Gmail, Skype, and other online accounts.1

Sophisticated phishing and malicious-software attacks targeting online activists for surveillance began to be reported in 2012.2 The US-based Electronic Frontier Foundation (EFF) found that malware 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 programs.3 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 taken down.4 Exploiting the need for circumvention and encryption tools among activists and opposition members, authorities have developed fake Skype encryption tools and a fake VPN application, both containing harmful software.5

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.6

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.” 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).

- 1. Interviews with released bloggers, names were hidden.
- 7. https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices...
Are service providers and other technology companies required to aid the government in monitoring the communications of their users?

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

The Law for the Regulation of Network Communication against Cybercrime, passed in 2012, requires websites to clearly publish the names and details of their owners and administrators. 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. 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).  

- Law of the rulers to communicate on the network and the fight against cyber crime” art. 5-12. Informal English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-I....
- “Law of the rulers to communicate on the network and the fight against cyber crime” art. 2.
- “Law of the rulers to communicate on the network and the fight against cyber crime” art. 8.

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

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, eight citizen journalists were killed in 2018.  

The director of the online news outlet Damascus Now, known as Wissam al-Tayr, was arrested in December 2018 (see C3). As of May 2019, the reason for his arrest
was unclear, and his whereabouts were unknown.2

Journalist Rida al-Basha, for whom an arrest warrant was issued in November 2018 (see C3), was later dismissed by her employer, the Lebanese television station Al-Mayadeen.3

In November 2018, photojournalist and activist Bilal Srewel, who works online, was arrested by a Turkish-backed opposition militia, the Sultan Murad Division, in the northern Syrian district of Afrin. He was tortured and beaten before being released three days later.4

Also 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. Raed and Hamoud were among the most prominent civilian activists in the area. Raed 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.5 Hamoud was a journalist and photographer for Radio Fresh.6

• 2. https://syrianobserver.com/EN/features/48993/the-regime-punishes-promin...
• 4. https://drive.google.com/file/d/1ENflnVJajHc bqjLktON5NbWDblorZ8s/view

C8 0-3 pts
Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?

While the SEA, a group of progovernment hackers, pioneered technical attacks against the opposition, 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 while executing more 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 out their networks. Once trust was established, the attackers targeted victims with RAT programs and gained access to their devices.

Numerous reports have detailed the spillover of the conflict into the online sphere. 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 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 that would trick them into installing malware. The links were sent via popular communications platforms, including WhatsApp and Telegram. 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 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 at least tacit 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...
12. https://www.forbes.com/sites/thomasbrewster/2018/12/05/syrian-electronic... 
Country Facts

- **Freedom in the World Status**
  - Not Free

- **Networks Restricted**
  - Yes

- **Social Media Blocked**
  - No

- **Websites Blocked**
  - Yes

- **Pro-government Commentators**
  - Yes

- **Users Arrested**
  - Yes

Previous Reports
• 2018 Report