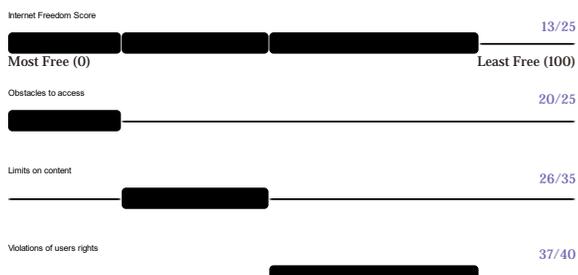


Syria Country Report | Freedom on the Net 2018



Key Developments:

June 1, 2017 - May 31, 2018

- Mobile phone penetration increased and internet access became more affordable across several regions (see Availability and Ease of Access).
- Numerous regional and Lebanese media websites, Wikipedia, and the WordPress blogging platform were unblocked in 2017. The block on the Israeli domain (.il) was also lifted (see Blocking and Filtering).
- Self-censorship has increased amid growing threats and violent reprisals for online posts (see Media, Diversity, and Content Manipulation; and Intimidation and Violence).
- In August 2017, it was confirmed that digital activist Bassel Khartabil Safadi was executed by the regime's security forces in 2015. He had been detained in 2012 for his democratic activism (see Intimidation and Violence).
- Law Number 9, passed in March 2018, establishes specialized courts for criminal cases related to communication and technology; critics worry the courts could be used to further suppress freedom of expression online (see Legal Environment).

Introduction:

Despite heavy restrictions on internet freedom, the cost and availability of internet access improved over the past year. The unexplained unblocking of several websites was offset by heightened self-censorship amid growing threats and violent reprisals for online activities.

In a positive development, authorities unblocked a number of regional and Lebanese media websites by the end of 2017, including Al Jazeera, Al Arabiya, *Asharq al-Awsat*, the Qatari *Al-Arab* newspaper, and *Al-Hayat*. In addition to the Syrian websites *The New Syrian*, *Enab Baladi*, and Souriali Radio. Many nonpolitical websites were also unblocked, such as Wikipedia and the WordPress blogosphere. Notably, the block on the Israeli domain (.il) was also lifted. No formal rationale was provided for the unblocking decision, though analysts think that as the government has gained ground in the civil war, it may be trying to demonstrate a reformist attitude toward freedom of expression.

In March 2018, the government passed Law Number 9, which established specialized courts for criminal cases related to information and communication technologies. Judges on these courts will be specially trained to handle technology issues, although the results of this training on human rights conditions are yet to be seen. The lack of judicial independence in Syria has led to concerns that the new law could be used to suppress freedom of expression and criminalize critics of the regime even further.

Despite relative improvements to access, Syria remains one of the most dangerous places to use the internet in the world. According to Reporters Without Borders, 12 citizen journalists were killed in 2017. In August 2017, it was confirmed that digital activist Bassel Khartabil Safadi was executed by the regime's security forces in 2015. He had been detained in 2012 for his democratic activism.

Obstacles to Access:

Mobile phone penetration increased in 2017, the cost of access became more affordable across regions in the past year. There were fewer restrictions on cybercafés, particularly in IS-held territories. Nonetheless, internet access was still subject to regular shutdowns both in areas controlled by the regime and rebel-held territories.

Availability and Ease of Access

Syria's telecommunications infrastructure is one of the least developed in the Middle East, with broadband connections among the most difficult and expensive to acquire.¹ This worsened after 2011, as electricity outages increased dramatically following public protests and the government's corresponding crackdown. Damage to the communications infrastructure is particularly severe in cities where the government is no longer in control, largely due to bombing and other damage caused by the civil war. As a result, a decentralized telecommunications infrastructure has developed, with each part of the country finding different sources of connectivity.

According to latest available estimates by the International Telecommunication Union, nearly 30 percent of Syrians had access to the internet, up from 21 percent in 2010.² The estimated number of fixed broadband subscribers also increased, but remained low at just over 3.14 subscriptions per 100 inhabitants. The number of mobile phone subscriptions increased from 72 percent in 2016 to 86 percent in 2017.³

Around two-thirds of the country is disconnected from Syrian ISP networks. Syrians have turned to WiMax connections, internet cables, or Turkish Wi-Fi operators for connectivity, which feed local distributors, who in turn provide subscriptions to local residents. In addition, many rely on mobile phone connections from Turkish operators in rebel-controlled areas in northern Syria, or Jordanian operators in border areas with Jordan in southern Syria, as well as lines from Israeli operators in border areas with occupied Palestinian territories in southwestern Syria. Others use satellite communication systems (VSAT) that serve internet cafés and some organizations. The monthly subscription fees for 40 GB of 3G and 4G data via Jordanian operators in southern Syria reached US\$13 in 2017. Many telephone centers in rebel-controlled areas in northern Syria install ADSL lines for landline subscribers using Turkish ISPs.⁴

The price, speed, and availability of internet access varies across regions. In a positive development, the cost of access decreased across regions in the past year. Prices decreased in areas served by Turkish internet as the strength of the Turkish lira dropped. Government-controlled areas also saw price decreases with the declining value of the Syrian lira. According to a price list published by the Syrian Computer Society Network, the monthly cost for a 1 Mbps ADSL connection was SYP 2400 (US\$5) as of mid-2017.⁵ The monthly fees for a 1 Mbps internet subscription were approximately US\$11 in rebel-controlled areas in northern Syria; the average monthly per capita income is SYP 33,000 (around \$75).⁶

Restrictions on Connectivity

The government has carried out extensive and repeated internet shutdowns since 2011. Damage to the telecommunications infrastructure led to a disconnection in Aleppo from March to November 2015.⁷ When Turkey initiated Operation Olive Branch, a military operation in the Afrin area, north of Aleppo, against Kurdish People Protection Units (YPG), Turkish authorities cut off internet service in most areas of northern Syria.⁸ Moreover, Hay'at Tahrir al-Sham (formerly Jabhat al-Nusra), a jihadist militant group that has fought in the civil war, also cut off the internet in many Idlib cities and towns, in response to the protest movement against its presence in the city of Idlib, which was accompanied by a campaign on social media launched by many activists and residents.⁹

Internet connections to Aleppo are now routed through Syrian networks, rather than Turkish networks. Researchers speculated that the move reflected recent gains made by the Syrian army over rebel forces in the areas surrounding Aleppo, once Syria's most populous city. Researchers noted the city was reconnected in 2016 using a "high capacity microwave link to the coastal city of Latakia, Syria."¹⁰ However, users in Aleppo have suffered from connection interruptions and slow connectivity, likely due to limited bandwidth.¹¹

In areas controlled by the government, the Syrian Telecommunications Establishment (STE) serves as both an ISP and the telecommunications regulator, providing the government with tight control over the internet infrastructure.¹² 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).¹³

ICT Market

There are currently around 20 ISPs in Syria, three of them government-owned: 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 martyrs and veterans.¹⁴ Independent VSAT connections are prohibited, although they are still heavily employed due to the damage that government ICT infrastructure has sustained as a result of the conflict.¹⁵ ISPs and cybercafés operating in government-controlled areas must obtain a permit from the STE and another security permit from the Ministry of the Interior.¹⁶ Moreover, cybercafé owners are required to monitor visitors and record their activities. There were fewer restrictions observed on cybercafés in IS-controlled territories in the past year.

There are two main mobile phone providers: Syriatel, owned by Rami Makhlof, a cousin of President Bashar al-Assad, and MTN Syria, a subsidiary of the South African company. During the 60th cycle of the Damascus International Exhibition in August 2017, the two companies announced the launch of 4G high-speed internet service.¹⁷

Regulatory Bodies

Syria's ICT market and internet policy is 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 Telecommunications and Technology.¹⁸ Domain name registration is handled by the Syrian Computer Society.¹⁹

Limits on Content:

The government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. In a positive development, authorities had unblocked a number of websites by the end of 2017. However, self-censorship heightened in the past year amid growing threats and violent reprisals for online activities, particularly in areas under government control.

Blocking and Filtering

Authorities block a variety of internet content. Since the beginning of the civil war, a number of websites have been employed to mobilize people to protest or resist the regime, including the websites linked to the Local Coordination Committees (LCCs) network. Many of these sites have been subject to blocking, in addition to opposition websites and the websites of human rights organizations, content critical of the regime's political, cultural, social or economic policies, criticism of high-level government officials, and sites that expose official corruption.

In a positive development, authorities had unblocked a number of regional and Lebanese media websites by the end of 2017, including Al Jazeera, Al Arabiya, *Asharq al-Awsat*, the Qatari *Al-Arab* newspaper, and *Al-Hayat*,²⁰ in addition to the Syrian websites the *New Syrian*, *Enab Baladi*, and Sourialli Radio. Many nonpolitical websites were unblocked as well, such as Wikipedia and the WordPress blogosphere. Notably, the block on the Israeli domain (.il) was also lifted. No formal rationale was provided for the unblocking decision, though analysts think that as the government has gained ground in the civil war, it may be trying to demonstrate a reformist attitude toward freedom of expression.

Nonetheless, a number of websites remained blocked, including *Al-Quds Al-Arabi* and the Kuwaiti newspaper *Al-Seyassah*, as well as the websites of human rights groups such as the Syrian Observatory for Human Rights, the Syrian Human Rights Committee, and *Souriatna*, a magazine that offers the perspectives of young Syrians.

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. As of 2018, both were among the top-three most visited websites in the country. Other social media platforms such as Twitter are also available.²¹

Skype, on the other hand, has suffered frequent disruptions, either due to low speeds or intermittent blocking by authorities. In February 2012, the government also began restricting access to some applications on mobile phones that activists had been using to circumvent other blocks. Antivirus software and updates to operating systems remain blocked due to U.S. sanctions, to the dismay of many U.S.-based activists.²²

The government continues to block circumvention tools, internet security software, and applications that enable anonymous communications. By enabling deep packet inspection (DPI) filtering on the Syrian network, authorities were able to block secure communications tools such as OpenVPN, Later 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPsec) in August 2011.²³

In addition to blocking websites, authorities forced the owners of a number of websites to shut them down, including the news sites *Syrian Mirror* and *An-Nazaha* ("Integrity"), whose owner was arrested by the Information Branch of the General Intelligence Directorate that forced the website's closure.²⁴

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."²⁵ Authorities have also used technology provided by the Italian company Area SpA to improve their censorship and surveillance capabilities, according to evidence from 2011. The contract with Area SpA included software and hardware manufactured by companies such as Blue Coat Systems, NetApp, and Sophos. Blue Coat had reportedly sold 14 devices to an intermediary in Dubai, which then sent them to Area SpA, with Blue Coat apparently believing that the equipment would be given to the Iraqi government. However, logs obtained by the hacktivist group Telecomix in August 2011 revealed evidence of their use in Syria instead.²⁶ In October of that year, Blue Coat acknowledged that 13 of the 14 devices had been redirected to the Syrian government, an inadvertent violation of a U.S. trade embargo, and that the company was cooperating with the relevant investigations.²⁷ Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.²⁸ The *Wall Street Journal* identified efforts to block or monitor tens of thousands of opposition websites or online forums covering the uprising.²⁹

The government has also allegedly filtered text messages since 2011, especially around the dates of planned protests. In February 2012, Bloomberg, using evidence from a series of interviews and leaked documents, reported that a special government unit known as Branch 225 had ordered Syriatel and MTN Syria to block text messages containing key words like "revolution" or "demonstration." The providers reportedly implemented the directives with the help of technology originally purchased from two Irish firms to restrict spam.³⁰

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 online censorship. When a user seeks access to a blocked website, an error message appears implying a technical problem rather than deliberate government restriction. The entity (STE) that implements blocking is known, but it is unclear which security apparatus makes the decisions. Following a request to unblock the *Al-Nazaha* news site in 2008, the Ministry of Communications and Technology informed the court that "The website was blocked under the direction of Branch 225,"³¹ one of the security branches of the Military Intelligence Directorate.

Content Removal

According to digital security organization SecDev, the Facebook pages of dozens of opposition groups, media outlets, and independent nongovernmental organizations (NGOs) have been suspended by the social network over the years.³² The Facebook pages of LCCs and the London-based Syrian Network for Human Rights have been banned, as well. Activists believe that Facebook users sympathetic to President Assad may be reporting the pages en masse for violating user guidelines. Razan Zeitouneh of the Violations Documentation Center shared a letter urging Facebook to keep the 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." Representatives from Facebook have cited the difficulties in discerning between objective reporting and propaganda, 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 the YouTube platform in mid-2017, after YouTube applied a "machine learning" algorithm that tracks any content that could violate the platform's rules. YouTube has since restored a number of channels and reposted thousands of clips that were mistakenly removed.

Media, Diversity, and Content Manipulation

With the onset of the civil war, citizen journalism and social media provided the Syrian public with an alternative view of domestic events,³³ especially as the perception of independence and credibility of state media outlets declined.³⁴ In an environment of violence and arbitrary "red lines," self-censorship is widespread online and increased in recent years amid growing threats and violent reprisals for critical content online (see Intimidation and Violence). Sensitive topics include criticism of President Assad, his late father, the military, the ruling Ba'ath party, the military, the ruling Ba'ath party, covering religious and ethnic tensions or corruption allegations related to the ruling family are also off limits. Most users are careful not only to avoid such sensitive topics, but also to refrain from visiting blocked websites.³⁵ Since 2014, users living in areas controlled by the Islamic State (IS) or other extremist groups have also stepped up their self-censorship.

Proregime forces 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 government. The Syrian Electronic Army (SEA), a progovernment hacktivist group, targets the websites of opposition forces, human rights groups, and foreign media outlets (see Technical Attacks). Journalists with domestic outlets sometimes receive phone calls from government officials offering "directions" on how to cover particular events.³⁶ The government also supports and promotes websites that provide progovernment coverage. These sites typically cite the reporting of SANA, the official state news agency, with the same wording often evident across multiple websites. Since early 2011, this approach has also been used to promote the government's view of the uprising and subsequent military campaign.³⁷ Interestingly, in 2012, the progovernment website *Aksalser* changed its stance to support the opposition and was subsequently blocked by the government.³⁸ The government has since unblocked the website, likely at the end of 2017.

U.S. sanctions have resulted in the blocking of paid online services, making it difficult for Syrians to purchase a domain or host their websites in the U.S. Restrictions on importing funds into Syria has made publishing content difficult. For instance, the magazine *Syrian Oxygen* was unable to obtain SSL certificates for its website from U.S. providers, apparently because the domain syrianooxygen.com contains the word "Syria."

Digital Activism

Online tools have proven crucial for Syrians inside and outside the country seeking to document human rights abuses, campaign for the release of imprisoned activists, and disseminate news from the front lines of the conflict. Communication apps 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.³⁹ The U.S.-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.⁴⁰ Activists have also established the Syria Observatory, a group of channels on social media networks linked to other observatories inside of Syria, which 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.⁴¹

Syrians are active on Facebook, using it as a platform to share news, discuss events, release statements, and coordinate both online and offline activities.⁴²

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.⁴³ Indeed, as the Syrian government shifted to the use of heavy arms and missiles against opposition fighters, the role of citizen journalists has 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 ensure coverage of remote areas and conflict zones. “Local Media Offices” ensure that local journalists cover limited geographic areas, and then use a social network as a platform to collect, verify, and publish news stories. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, rebel groups, and civil society groups, mostly documenting attacks. A group that categorized YouTube videos and shared them via the platform OnSyria posted almost 200,000 videos in 2013.⁴⁴

Violations of User Rights:

Law Number 9, passed in March 2018, establishes specialized courts for criminal cases related to communication and technology; critics worry the courts could be used to further suppress freedom of expression online. Citizen journalists, bloggers, and activists were detained and often tortured while in detention. Netizens were confirmed killed during the coverage period.

Legal Environment

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 language such as “threatening national unity” or “publishing false news that may weaken national sentiment.”⁴⁵ Defamation offenses are punishable by up to one year in prison if comments target the president and up to six months in prison for libel against other government officials, including judges, the military, or civil servants.⁴⁶ The cybercrime law allows prison sentences of up to three years and fines of up to SYP 250,000 (US\$600) for anyone who incites or promotes crime through computer networks.⁴⁷ 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 establishes specialized courts for criminal cases related to communication and technology.⁴⁸ Some analysts view the creation of such courts as a positive step. Judges on these courts will be specially trained to handle technology issues. However, the lack of judicial independence in Syria has led to concerns that the new law could be used to suppress freedom of expression and criminalize critics of the regime.

Prosecutions and Detentions for Online Activities

Since antigovernment protests broke out in 2011, the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. While it is difficult to obtain information on recent arrests, at least 15 netizens remain in prison according to Reporters Without Borders, an international NGO.⁴⁹ Bassel Khartabil, an open source activist and recipient of the 2013 Index on Censorship Digital Freedom Award, was detained by the authorities in March 2012 and subsequently executed (see Intimidation and Violence).⁵⁰

Human rights activists who work online are also targeted by the government and rebels. Four members of the Violations Documentation Center (VDC) were kidnapped by an unknown group from a rebel-controlled area in December 2013.⁵¹ Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in February 2012, arresting 14 employees.⁵² One SCM member and civil rights blogger, Razan Ghazzawi,⁵³ was detained for 22 days.⁵⁴ The other members were released in August 2015 after three years in pretrial detention.⁵

The Hay'at Tahrir al-Sham arrested a number of digital activists in the governorate of Idlib on various charges, such as “media work against HTS,” which is the charge that media activists Amjad Al-Maleh, Hussam Mahmoud, Hassan Yunis, and Bakr Yunis faced when they were arrested in December 2017. Activists launched a media campaign for their release, under the slogan “Free Madaya Activists,” and a number of organizations signed a statement demanding their release. Many media activists have left Syria for Turkey after receiving threats or being arrested.

Surveillance, Privacy, and Anonymity

Surveillance is rampant on domestic ISPs, which are tightly aligned with government security forces. Activists and bloggers released from custody have reportedly been pressured by security agents to provide the passwords of their Facebook, Gmail, Skype, and other online accounts.⁵⁵ Meanwhile, in IS-controlled territory, militants have allegedly conducted unannounced raids at cybercafés to monitor customers’ browsing history and social media accounts.⁵⁶

The Law for the Regulation of Network Communication against Cyber Crime, passed in February 2012, requires websites to clearly publish the names and details of the owners and administrators.⁵⁷ 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.⁵⁸ Failure to comply may cause the website to be blocked and is punishable by a fine of SYP 100,000 to 500,000 (US\$230 to \$1,100). If the violation is found to have been deliberate, the website owner or administrator may face punishment of three months to two years imprisonment as well as a fine of SYP 200,000 to 1 million (US\$450 to \$2,300).⁵⁹

Reports of sophisticated phishing and malware attacks targeting online activists emerged in February 2012.⁶⁰ The U.S.-based Electronic Frontier Foundation (EFF) reported that malware called Darkcomet RAT (remote access tool) and Xtreme RAT had been found on activists’ computers and were capable of capturing webcam activity, 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 instant messaging programs.⁶¹ Later, EFF reported the appearance of a fake YouTube channel carrying opposition videos that requested users’ login 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.⁶² Due to the prevailing need for circumvention and encryption tools among activists and other opposition members, authorities have developed fake Skype encryption tools and a fake VPN application, both containing harmful Trojans.⁶³

A 2014 report by Kaspersky Labs 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.⁶⁴ 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.

A 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 Kurdish militia. Since January 2018, the YPG have been targeted by the Turkish air and ground forces as part of Operation Olive Branch.

Anonymous communication is possible online, but is increasingly restricted. Registration is required to purchase a mobile phone, though in recent years, activists have used the SIM cards of friends and colleagues killed in clashes with security forces to shield their identities. Mobile phones from neighboring countries like Turkey and Lebanon have been widely used since 2012, notably by Free Syrian Army fighters and, increasingly, civilians.

Intimidation and Violence

Once in custody, citizen journalists, bloggers, and other detainees frequently endure beatings and torture at the hands of government authorities. According to Reporters Without Borders, 12 citizen journalists were killed in 2017.⁶⁵

- In August 2017, it was confirmed that digital activist Bassel Khartabil Safadi was executed by the regime’s security forces in 2015. He had been detained in 2012 for his democratic activism.⁶⁶
- In March 2017, Mohamed Abadzed, also known as George Samara, was killed during an airstrike by the Russian and Syrian militaries in the city of Daraa. Shortly before his death, Abadzed had posted a live video of the airstrike on his Facebook page.⁶⁷
- In September 2015, it was revealed that *Al-Fida* newspaper’s cartoonist Akram Raslan, who had shared antigovernment cartoons on Arabic news sites and social media, had died in state custody in 2013.⁶⁸ He had been arrested in October 2012 and was allegedly tortured to death.⁶⁹

Separately, in a video recording published by IS on June 26, 2016, five journalists—many of whom worked primarily online—were murdered. In at least two cases, IS militants had rigged the individuals’ computers or cameras with explosives.⁷⁰ Citizen journalists have also been targeted by IS militants while in Turkey. Ibrahim Abdul Kader of the human rights organization Raqqa is Being Slaughtered Silently (RBSS) was killed by IS militants in the city of Urfa, Turkey along with his friend Fares Hammadi in October 2015.⁷¹ Naji Jaraf, editor in chief of the opposition *Hentah Magazine* and an activist with RBSS, was shot and killed in the Turkish city of Gaziantep in December 2015.⁷² Hundreds of activists have gone into hiding or fled Syria.⁷³ Blogger Assad Hanna left Syria following online threats stemming from his criticism of the regime, but was badly injured by knife-wielding assailants at his apartment in Turkey in April 2015.⁷⁴

In a move some observers called unprecedented, IS executed a female journalist in September 2015. Ruqia Hassan, also known as Nissan Ibrahim, was blogging about daily life in the city of Raqqa.⁷⁵ She was accused of being a spy for the Free Syrian Army. Shortly before her death, she reportedly complained of death threats allegedly sent by IS. International journalists, including those whose work is mainly featured online, were also killed by Syrian militant groups in previous years.⁷⁶

Technical Attacks

While the Syrian Electronic Army (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 cyber operations. In 2016, Citizen Lab published research on Group 5, a new hacker collective noted for its use of “Iranian Persian dialect tools and Iranian hosting companies.”⁷⁷ Hackers established websites with names such as AssadCrimes while executing more elaborate social engineering schemes.⁷⁸ 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. Hackers created email addresses and social media profiles linking to the fake publications in order to communicate with government opponents and human rights defenders and map out their social networks. Once trust was established, the hackers targeted victims with so-called remote access Trojan (RAT) programs and gained access to their devices.

Numerous reports have detailed the spillover of the conflict into the online sphere. According to the cybersecurity group FireEye, Russia’s intelligence agency, the FSB, stepped up technical attacks against Syrian human rights organizations and opposition groups in a major campaign to glean intelligence and disrupt reporting on Russian human rights violations.⁷⁹ In December 2014, Citizen Lab released a report entitled “Malware Attack Targeting Syrian ISIS Critics,” focusing on groups such as RBSS, which documents human rights abuses committed by IS. Citizen Lab believes that the malware was developed by IS or pro-IS hackers in order to collect information about the group.⁸⁰

In March 2016, the FBI added three SEA members to its “Cyber Most Wanted” list.⁸¹ In May 2016, Syrian national Peter Romar was extradited from Germany to the U.S. on charges of conspiracy linked to a hacking associated with his alleged membership in the SEA. He pled guilty that September.⁸²

The SEA made headlines after hacking major western media outlets and organizations, including the websites of the *New York Times*,⁸³ the U.S. Marines,⁸⁴ Facebook,⁸⁵ and many others. Most of the attacks occurred at the DNS level, which involved redirecting requests for the domain name to another server. In 2013, the Twitter account of Barack Obama, run by staff from Organizing for Action (OFA), was briefly hacked by the SEA.

resulting in the account posting shortened links to SEA sites.⁸⁶ The hackers had gained access to the Gmail account of an OFA staffer. Also in 2013, the SEA hacked the website and Twitter feed of Human Rights Watch, redirecting visitors to the SEA homepage.⁸⁷ These tactics continued with the high-profile hacking of *Forbes* in 2014⁸⁸ and the *Washington Post* in 2015.⁸⁹

Though the hacktivist group's precise relationship to the regime is unclear, evidence exists of government links or at least tacit support. The SEA registered its domain in 2011 on servers maintained by the Assad-linked Syrian Computer Society.⁹⁰ In a 2011 speech, President Assad explicitly praised the SEA and its members,⁹¹ and state-run media has given positive coverage of the group's actions.⁹

Notes:

- 1 Kyle Wansink, *Syria - Telecoms, Mobile, Broadband and Forecasts*, BuddeComm, <http://bit.ly/1OdyCSD>.
- 2 International Telecommunication Union, "Statistics," 2016, <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.
- 3 International Telecommunication Union, "Statistics," 2017, <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.
- 4 "Syrian company provides "Internet" service in the town of Sarmin Idleb", 12 January 2017, Smartnews-Agency, [In Arabic], <https://bit.ly/2HU7TOc>
- 5 Syrian Computer Society Network, "ADSL Services and price" [In Arabic], accessed May 17, 2017, <http://bit.ly/250BUqt>.
- 6 Labor Observatory for Studies and Research, "The Syrian's living costs are 7 times higher than his income". [Arabic] June 6, 2017, http://syriasteps.com/?d=126&id=151984&in_main_page=1.
- 7 Doug Madory, "Internet Returns to Aleppo, Syria," Dyn Research, November 11, 2015, <http://research.dyn.com/2015/11/internet-returns-to-aleppo-syria/>.
- 8 "Turkish Internet service disconnected from Northern Syria", 21 Jan 2018 Smartnews-Agency, <https://smartnews-agency.com/en/wires/256293/turkish-internet-service-disconnected-from-northern-syria>.
- 9 "Tahreer Al sham" breaks off the Internet services form the cities and towns in Idlib, 26 February 2018, Smartnews-Agency, [In Arabic], <https://bit.ly/2FakvCQ>
- 10 Doug Madory, "War-torn Syrian city gets new fiber link," Dyn Research, October 12, 2016, <http://research.dyn.com/2016/10/war-torn-syrian-city-gets-new-fiber-link/>.
- 11 Aleppo News network, "Internet disconnection is deliberate, and these are the reasons", May 1, 2017, <https://www.nfac-sy.net/news/10413>
- 12 Syrian Telecom, "Intelligent Network Project," http://www.in-ste.gov.sy/inindex_en.html.
- 13 Jaber Baker, "Internet in Syria: experimental goods and a field of a new control," White and Black Magazine, posted on Marmarita website, August 10, 2008, <http://www.dai3tna.com/nuke/modules.php?name=News&file=article&sid=6019>. (no longer available)
- 14 "Opening Internet Service Provider ISP the private with military establishment "Ibaa"", 15 August 2016, <https://bit.ly/2qSSc7m>
- 15 "Online Syria, Offline Syrians," *One Social Network with a Rebellious Message*, The Initiative or an Open Arab Internet, accessed March 8, 2012, <http://bit.ly/INSCAHO>.
- 16 Ayham Saleh, "Internet, Media and Future in Syria" [In Arabic], The Syrian Center for Media and Free Expression, November 14, 2006, <http://bit.ly/1hfdwWl>.
- 17 Launch of 4G service at Damascus International Fair. Al Watan newspaper. [Arabic], August 22, 2017. <http://alwatan.sy/archives/116132>
- 18 Ministry of Communication and Technology, "Overview," [In Arabic], <http://www.moct.gov.sy/moct/?q=ar/node/21>.
- 19 Sean Gallagher, "Network Solutions seizes over 700 domains registered to Syrians," Ars Technica, May 8, 2013, <http://arstechnica.com/tech-policy/2013/05/network-solutions-seized-over-700-domains-registered-to-syrians/>.
- 20 "Damascus reconcile the hostile media", Almodon.com, 15 Septmber 2017, [In Arabic], <https://bit.ly/2yzY1eO>
- 21 Alexa, "Top Sites in SY," accessed October 25, 2016, <http://www.alexa.com/topsites/countries/SY>.
- 22 Mike Rispoli, "Access joins open letter to tech industry addressing overcompliance with U.S. sanctions," Access, June 28, 2012, <http://bit.ly/1iOXdDM>.
- 23 Dlashad Othman, "Bypassing censorship by using obsproxy and openVPN, SSH Tunnel," *Dlshad*, June 22, 2013, <http://bit.ly/1KH3KJz>.
- 24 Syrian center for media and freedom expression, "Taming the Internet", [In Arabic], <https://bit.ly/2JIEqBf>
- 25 Reporters Without Borders, "Syria," *Enemies of the Internet: Countries under surveillance*, March 12, 2010, <http://bit.ly/1OCZ0cS>, and Platinum, Inc., "ThunderCache Overview," accessed August 14, 2012, <http://www.platinum.sy/index.php?m=91>.
- 26 Andy Greenberg, "Meet Telecomix, The Hackers Bent on Exposing Those Who Censor and Surveil The Internet," *Forbes*, December 26, 2011, <http://onforb.es/1BuItQx>.
- 27 Blue Coat, "Update on Blue Coat Devices in Syria," news release, December 15, 2011, <http://bit.ly/1FzFd8X>.
- 28 "Blue Coat device logs indicate the levels of censorship in Syria," *Arturo Filasto*, accessed August 14, 2012, <http://bit.ly/1LZDZJ3>.
- 29 Jennifer Valentino-Devries, Paul Sonne, and Nour Malas, "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web," *Wall Street Journal*, October 29, 2011, <http://on.wsj.com/16Y13W>.
- 30 Ben Elgin and Vernon Silver, "Syria Disrupts Text Messages of Protesters With Dublin-Made Equipment," *BloombergBusiness*, February 14, 2012, <http://bloom.bg/1i0TOEU>.
- 31 Violations of freedom of expression in the time between 4/5/2007 to 3/5/2008, Syrian Center for Media and Freedom of Expression, [In Arabic], <https://bit.ly/2qZGXcT>
- 32 Michael Pizzi, "The Syrian Opposition Is Disappearing From Facebook," *The Atlantic*, February 4, 2014, <http://theatltn.tc/1aoJZAQ>.
- 33 Amr Alhamad, "Holding on to Seafoam: Insights on the Reality of Radio and Web Publishing in Syria" Weedoo, November, 2016, <https://weedoo.tech/our-studies-en/holding-on-to-seafoam-insights-on-the-reality-of-radio-and-web-publishing-in-syria/>.
- 34 Nasir Al-Sahli, "The Schizophrenia of the Syrian media 'Terrorists are bombing Aleppo'" Alaraby, May 4, 2016, <http://bit.ly/2fT2L9q>, and Hanin Al-Nukri, Enabbaladi "What changed in the Syrian government media outlets after seven years?" March 19, 2016, <https://www.enabbaladi.net/archives/137788>.
- 35 Email communication from a Syrian blogger. Name was hidden.
- 36 Guy Taylor, "After the Damascus Spring: Syrians search for freedom online," *Reason*, February 2007, <http://theatltn.tc/1aoJZAQ>.
- 37 Guy Taylor, "After the Damascus Spring: Syrians search for freedom online," *Reason*, February 2007, <http://theatltn.tc/1aoJZAQ>.
- 38 The Syrian "Aksalser website with the revolution," [In Arabic] *the-syrian*, August 28, 2012, <http://the-syrian.com/archives/86170>.
- 39 Maya Gebeily, "Secret Syria network warns of air raids over WhatsApp," *The Times of Israel*, January 21, 2016, <http://www.timesofisrael.com/secret-syria-network-warns-of-air-raids-over-whatsapp/>.
- 40 Avi Asher-Schapiro, "The Virtual Surgeons of Syria," *The Atlantic*, August 24, 2016, <http://www.theatlantic.com/international/archive/2016/08/syria-madaya-doctors-whatsapp-facebook-surgery-assad/496958/>.
- 41 Facebook page "the observatory" and the user guide, <https://bit.ly/2qUydFq>
- 42 Judith Dublin, "Syrian Fight Fire with Facebook," *Vocativ*, September 23, 2013, <http://voc.tv/1UJqclP>.
- 43 Christophe Koettl, "The YouTube War: Citizen Videos Revolutionize Human Rights Monitoring in Syria," *Mediashift* (blog), PBS, February 18, 2014, <http://bit.ly/1Nkfnw9>.
- 44 The platform, <http://onsyria.org/>, is now offline and the related Facebook page has not been updated since 2013: Onsyria, Facebook Page, <http://on.fb.me/1GnVymR>.
- 45 Syrian Penal Code, art. 285, 286, 287
- 46 Syrian Penal Code, art. 378.
- 47 Global Resource and Information Directory, "Legislation," in "Syria," <http://www.fosigrid.org/middle-east/syria>.
- 48 "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>
- 49 See Reporters Without Borders, "Violations of Press Freedom Barometer," 2017, https://rsf.org/en/barometer?year=2017&type_id=233#list-barometre.
- 50 "Renewed calls for Bassel Khartabil's release on 4th anniversary of detention," Reporters Without Borders, March 17, 2016, <https://rsf.org/en/news/renewed-calls-bassel-khartabils-release-4th-anniversary-detention>.
- 51 Hania Mourtada, "She Was My Mandela" – Famous Syrian Activist Gets Abducted," Time, December 11, 2013, <http://ti.me/1KcXrTc>.
- 52 Maha Assabalani, "My colleagues are in prison for fighting for free expression," UNCut - Index on Censorship, May 11, 2012, <http://bit.ly/1EYHMX9>.
- 53 Jared Malsin, "Portrait of an Activist: Razan Ghazzawi, the Syrian Blogger Turned Exile," Time, April 2, 2013, <http://ti.me/1Q46vKl>.
- 54 An interview with Syrian blogger, February 2013, Skype.
- 55 Interviews with released bloggers, names were hidden.
- 56 Interview with Abu Ibrahim Raqqawi of Raqqa Is Being Slaughtered Silently, Skype.

- 57 "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-law-on-Internet-regulation.html>.
- 58 "Law of the rulers to communicate on the network and the fight against cyber crime" art. art. 2.
- 59 "Law of the rulers to communicate on the network and the fight against cyber crime" art. art. 8.
- 60 Ben Brumfield, "Computer spyware is newest weapon in Syrian conflict," CNN, February 17, 2012, <http://cnn.it/1LZPOXn>.
- 61 Eva Galperin and Morgan Marquis-Boire, "How to Find and Protect Yourself Against the Pro-Syrian-Government Malware on Your Computer," Electronic Frontier Foundation, March 5, 2012, <http://bit.ly/xsbmXy>.
- 62 Eva Galperin and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, <http://bit.ly/1XQhHzX>.
- 63 "Syrian Malware" Up-to-date website collecting the malware <http://syrianmalware.com/>.
- 64 Kaspersky Lab Global Research and Analysis Team, *Syrian Malware, the evolving threat*, August 2014, <http://bit.ly/1pCJ0gK>.
- 65 See Reporters Without Borders, "Violations of Press Freedom Barometer," for 2016 and 2017, https://rsf.org/en/barometer?year=2017&type_id=233#list-barometre.
- 66 Liz Sly, "One of Syria's best-known democracy activists has been executed," *Washington Post*, August 2, 2017, https://www.washingtonpost.com/world/middle_east/one-of-syrias-best-known-democracy-activists-has-been-executed/2017/08/02/483f4ca0-778a-11e7-8c17-533c52b2f014_story.html.
- 67 Committee to Protect Journalists, "Syrian journalist killed by airstrike in Daraa," March 13, 2017, <https://cpj.org/2017/03/syrian-journalist-killed-by-an-airstrike-in-daraa.php>.
- 68 "Well-known Syrian cartoonist died in detention after being tortured," *Reporters Without Borders*, September 22, 2015, <https://rsf.org/en/news/well-known-syrian-cartoonist-died-detention-after-being-tortured>.
- 69 Ibrahim Naffee, "Cartoonist Raslan arrested in Syria," *Arab News*, October 16, 2012, <http://www.arabnews.com/cartoonist-raslan-arrested-syria>.
- 70 Enab Baladi Online, "ISIS Executes Five Journalists in Deir-ez-Zor," *The Syrian Observer*, June 27, 2016, http://syrianobserver.com/EN/News/31250/ISIS_Executes_Five_Journalists_Deir_Zor.
- 71 Lizzie Dearden, "Isis beheads 'Raqqa is Being Slaughtered Silently' activist and friend in Turkey," *Independent*, October 30, 2015, <http://ind.pn/1Wm9dAh>.
- 72 AP, "Reporters Without Borders urges Turkey to protect exiled Syrian journalists," *US News and World Report*, December 29, 2015, <http://www.usnews.com/news/world/articles/2015-12-29/journalism-group-calls-on-turkey-to-protect-syrian-reporters>.
- 73 Interviews with two photographers who have taken refuge in Turkey, December 2011.
- 74 Amira al Hussaini, "Syrian Blogger Stabbed in His Istanbul Home After Receiving Threats Online," *Global Voices Advocacy*, April 21, 2015, <http://bit.ly/1JS03fb>.
- 75 Aisha Gani and Kareem Shaheen, "Journalist Ruqia Hassan murdered by Isis after writing on life in Raqqa," *The Guardian*, January 5, 2016, <http://bit.ly/1O8Gqbb>.
- 76 See Committee to Protect Journalists, "James Foley," *Journalists Killed/Syria*, 2014, <https://cpj.org/killed/2014/james-foley.php>, Committee to Protect Journalists, "Steven Sotloff," *Journalists Killed/Syria*, 2014, <https://cpj.org/killed/2014/steven-sotloff.php>, and Committee to Protect Journalists, "Kenji Goto," *Journalists Killed/Syria*, 2015, <https://cpj.org/killed/2015/kenji-goto.php>; I-fan Lin, "Hate Is Not What Humans Should Do: Slain Journalist Kenji Goto's Words Live On Online," *Global Voices*, February 7, 2015, <http://bit.ly/1MyBtll>.
- 77 "Group5: Syria and the Iranian Connection" citizenlab, August 2, 2016 <https://citizenlab.org/2016/08/group5-syria/>
- 78 "Group5: Syria and the Iranian Connection" citizenlab, August 2, 2016 <https://citizenlab.org/2016/08/group5-syria/>
- 79 Sam Jones, "Russia steps up Syria cyber assault," *Financial Times*, February 19, 2016, <https://www.ft.com/content/1e97a43e-d726-11e5-829b-8564e7528e54>.
- 80 John Scott-Railton and Seth Hardy, *Malware Attack Targeting Syrian ISIS Critics*, CitizenLab, December 18, 2014, <http://bit.ly/1JbRwMW>.
- 81 James Temperton, "FBI adds Syrian Electronic Army hackers to most wanted list," *Wired*, March 23, 2016, <http://www.wired.co.uk/article/syrian-electronic-army-fbi-most-wanted>.
- 82 "Syrian Electronic Army Hacker Pleads Guilty" Department of justice, September 28, 2016, <https://www.justice.gov/opa/pr/syrian-electronic-army-hacker-pleads-guilty>
- 83 Christine Haughney and Nicole Perloth, "Times Site Is Disrupted in Attack by Hackers," *New York Times*, August 27, 2013, <http://nyti.ms/17krXEO>.
- 84 Julian E. Barnes, "Syrian Electronic Army Hacks Marines Website," *The Wall Street Journal*, September 2, 2013, <http://on.wsj.com/1KGVnFf>.
- 85 Adario Strange, "Syrian Electronic Army Hacks Facebook's Domain Record," *Mashable*, February 5, 2014, <http://on.mash.to/1EQuHPY>.
- 86 Gregory Ferenstein, "The Syrian Electronic Army Hacked Obama's Twitter Links And Campaign Emails," *Tech Crunch*, October 28, 2013, <http://tcrn.ch/1Xi62bV>.
- 87 Max Fisher, "Syria's pro-Assad hackers infiltrate Human Rights Watch Web site and Twitter feed," *Washington Post*, March 17, 2013, <http://wapo.st/1eU9nKl>.
- 88 Andy Greenberg, "How the Syrian Electronic Army Hacked Us: A Detailed Timeline," *Forbes*, February 20, 2014, <http://onforb.es/MEWYiq>.
- 89 Brian Fung, "The Syrian Electronic Army just hacked the Washington Post (again)," *Washington Post*, May 14, 2015, <http://wapo.st/1JS0eY7>.
- 90 The Syrian Electronic Army, <http://sea.sy/index/en>.
- 91 Haroon Siddique and Paul Owen, "Syria: Army retakes Damascus suburbs-Monday 30 January," *The Guardian*, January 30, 2012, <http://bit.ly/1LZSDQA>; Voltaire Network, "Speech by President Bashar al-Assad at Damascus University on the situation in Syria," June 20, 2011, <http://bit.ly/1FzOUEp>.
- 92 "The Syrian Electronic Army Fights Rumors and Gives the True Picture of the Incident," [in Arabic], *Wehda*, May 17, 2011, <http://bit.ly/1Of0sCp>.