FREEDOM
ON THE NET
2014

Freedom
House

Syria

	2013	2014
Internet Freedom Status	**Not Free**	**Not Free**
Obstacles to Access (0-25)	24	25
Limits on Content (0-35)	25	26
Violations of User Rights (0-40)	36	37
TOTAL* (0-100)	**85**	**88**

* 0=most free, 100=least free

Population:	21.9 million
Internet Penetration 2013:	26 percent
Social Media/ICT Apps Blocked:	Yes
Political/Social Content Blocked:	Yes
Bloggers/ICT Users Arrested:	Yes
Press Freedom 2014 Status:	Not Free

Key Developments: May 2013 – May 2014

- With the telecommunications infrastructure in a dire state, government agencies and rebel forces continued to periodically shut down internet service to thwart citizen journalism and communications among fighters (see **Obstacles to Access**).

- Websites that express criticism of the government or opposition viewpoints are blocked (see **Limits on Content**).

- Activists, bloggers, and citizen journalists that document human rights violations online faced arrest and kidnapping by both the regime and rebel forces such as the Free Syrian Army, al-Nusra Front, and Islamic State of Iraq and the Levant (ISIL). Syrian journalist Abdulwahab Mulla, known for his satirical show on YouTube, was abducted by masked men in October 2013 while in a rebel-held area of Aleppo (See **Violations of User Rights**).

- Authorities still supply progovernment hackers with servers and data to target online activists with surveillance malware. The Syrian Electronic Army continued to target foreign media outlets for their coverage of the conflict (see **Violations of User Rights**).

Introduction

Syria remains one of the most repressive and dangerous environments for internet users in 2014. Authorities employ sophisticated technologies to filter political, social, and religious websites, and to conduct surveillance on citizens. Phishing, spear-phishing, and other cyberattacks have grown dramatically over the past year. Progovernment hackers have infected over 10,000 computers with surveillance malware, which can then be used to gain sensitive information about opposition networks or ordinary citizens. Individuals are regularly detained and tortured for their online posts or digital activism, either by the Syrian government or by armed extremists such as the Islamic State of Iraq and the Levant (ISIL), whose power has increased over the past year. The situation for bloggers, journalists, and citizen journalists has only grown worse as a result; Syria recorded the highest number of deaths of citizen journalists in the world. Nonetheless, despite weak infrastructure, online restrictions, and harsh punishments for online activities, Syrians have made extensive use of social networks and online tools to document human rights abuses and mobilize protests.

The internet was first introduced to Syria in 2000, immediately after the transfer of power from Hafez al-Assad to his son, current president Bashar al-Assad. The internet came to portray the new president's ostensible emphasis on modernity and evolution, with more than one-fifth of the population online by 2010. However, the regime has maintained tight control over information and communication technologies (ICTs) for many years by dominating key networks via government-linked service providers and engaging in extensive blocking of websites. Syrian users had limited access to secure connections; the Secure Sockets Layer (SSL) protocol necessary for browsing "https" sites was blocked until 2004, when foreign email providers were finally allowed into the country.

Inspired by regional events, a civic protest movement began in February 2011, calling for political reforms, the end of emergency rule, and basic freedoms. By early 2012, after brutal crackdowns on demonstrations in several cities, events descended into armed conflict. Authorities prevented foreign media from accessing the situation on the ground, prompting many ordinary Syrians to take up mobile phones and small cameras to cover the deteriorating situation and post videos on social media. These citizen journalists have become vital in the quest to document flagrant human rights abuses by all parties to the conflict.

Since the start of the conflict, government censorship and retaliation against internet users has intensified. Tactics have included periodic shutdowns of internet and mobile phone service, increased filtering of websites, sophisticated monitoring of users' online activities, as well as the confiscation of laptops, mobile phones, and other equipment used by citizen journalists. Shelling and sabotage have led to heavy damage to infrastructure, affecting internet and power connections in seven provinces. The poor state of internet service has led many opposition activists to use satellite connections, which can be tracked easily and have resulted in targeted bombings against media centers, as occurred in the 2012 death of journalist Marie Colvin.[1] Combined, these developments make Syria one of the worst countries for internet freedom in 2014.

[1] Trevor Timm and Jillian C. York, "Satphones, Syria, and Surveillance," EFF, February 23, 2012, https://www.eff.org/deeplinks/2012/02/satphones-syria-and-surveillance.

Obstacles to 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.[2] This worsened after 2011, as inflation and electricity outages increased dramatically following public protests and the government's corresponding crackdown. Damage to the communications infrastructure was particularly bad in the cities of Homs, Daraa, and Aleppo, as they were subject to severe shelling by the Syrian armed forces. By the end of 2013, the International Telecommunications Union (ITU) estimated that 26.2 percent of the population had access to the internet.[3] The number of fixed broadband subscribers increased to 346,000, a ten-fold increase from 2009 but still representing only 1.58 subscriptions per 100 inhabitants. Mobile phone penetration was at about 56 percent.

In 2009, mobile phone companies began providing 3G services in Syria, though the number of subscribers had reached only 80,000 by late 2010 due to the relatively high prices, almost US$25 for 4 GB and US$200 for unlimited data usage.[4] In addition, the service is primarily available in large cities. Most users connect to the internet through a fixed dial-up connection at speeds of only 56 Kbps, which severely limits their ability to download or view multimedia content. During peak times, the speed is even slower.[5] Broadband ADSL service remains limited due to the inadequate infrastructure in rural areas at prices which remain beyond the reach of most Syrians. For example, according to a price list published by the Syrian Computer Society, the monthly cost for a connection speed of 1 Mbps was SYP 1650 (approximately US$15) as of May 2012,[6] in a country where gross domestic product per capita, when taken on a monthly basis, is only $274.[7] As two-thirds of the country is disconnected from Syrian internet service providers (ISP) networks, access has declined with the average Syrian unable to afford satellite internet, the most popular alternative.

The country's connection to the international internet remains centralized and tightly controlled by the government. This is done under the purview of the Syrian Information Organization (SIO) and the state-owned Syrian Telecommunications Establishment (STE), which owns all fixed-line infrastructures. The STE is a government body established in 1975 as part of the Ministry of Telecommunications and Technology.[8] This centralization has contributed to connectivity problems, as the weak and overburdened infrastructure often results in slow speeds and periodic outages. In addition to its regulatory role, the STE also serves as an ISP.[9] Private ISPs like Aya, as well as mobile

[2] "Syria - Telecoms, Mobile, Broadband and Forecasts," BuddeComm, accessed March 8, 2012, http://www.budde.com.au/Research/Syria-Telecoms-Mobile-Broadband.html.

[3] International Telecommunication Union (ITU), "Percentage of individuals using the Internet," "Fixed (wired)-broadband subscriptions," "Mobile-cellular subscriptions," 2013, accessed August 1, 2015, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[4] "Projects to transform Syria into a regional anchor point in the communication" [in Arabic], Alhayat, September 1, 2010, http://international.daralhayat.com/internationalarticle/177606; "What are SURF Postpaid Packages?" [in Arabic], SURF Wireless Broadband, accessed March 8, 2012, http://bit.ly/15EHXWb.

[5] "Internet Enemies," Reporters Without Borders, March 2011, http://bit.ly/eLXGvi.

[6] "Services and price" [in Arabic], Syrian Computer Society Network (SCS-NET), accessed March 31, 2013 http://www.scs-net.org/portal/OurConnection/OurConnections/SCSADSL/PlansPrices/tabid/493/Default.aspx.

[7] "GDP per capita (current US$)," The World Bank, 2008-12, accessed March 12, 2014, http://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

[8] See the Ministry of Telecommunications and Technology's website (in Arabic) at: http://www.moct.gov.sy/moct/?q=ar/node/58.

[9] See STE's website at: http://www.in-ste.gov.sy/inindex_en.html.

phone internet providers, are required to sign a memorandum of understanding to connect via the gateways controlled by the SIO.[10]

At least 11 ISPs have entered the market since the end of 2005, raising the total number of ISPs to 14.[11] Independent satellite connections are prohibited, although in reality, they are heavily employed due to the unreliability of government ICT infrastructure.[12] ISPs and cybercafes must obtain approval from the STE and pass security vetting by the Ministry of Interior and other security services.[13] Moreover, cybercafe owners are required to monitor visitors and record their activities. There are two main mobile phone providers in Syria: Syriatel—owned by Rami Makhlouf, a cousin of President Bashar al-Assad—and MTN Syria, a subsidiary of the South African company.

During late 2013 and early 2014, the Syrian government continued to obstruct connectivity through its control of key infrastructure, at times shutting down the internet and mobile phone networks entirely or at particular sites of unrest. Syrians faced a 19-hour internet blackout from May 7 to 8, and an 11-hour shutdown on May 15, 2013.[14] State sources blamed the outages on technical failures, although many speculated that the outages were timed to coincide with a specific political or military purpose.[15] Two shutdowns also occurred in November[16] and December 2012.[17] More localized, but longer lasting cut-offs were reported in seven provinces all across the country. This includes, for example, a full shutdown in Aleppo on August 11, 2012.[18]

As a result of the devastating conflict, most of the northern and eastern parts of the country have experienced heavy damage to telecommunications infrastructure. Exchange centers have been shelled or deliberately sabotaged by both rebel and progovernment fighters, often to disable the telecommunications network of the other party. This occurred in the cities of Der el Zor, al-Hassaka, and Qamishli, where inhabitants have been offline since May 2013. The government has claimed this is due to technical problems, but reporters believe it is for political reasons.[19] According to activists, broadband is often throttled and 3G services shut off as pro-regime forces prepare to besiege a city.[20] From opposition activists to jihadists, rebel fighters to the Syrian army, all players in the conflict rely heavily on the internet, whether for its use as a propaganda tool or for standard

[10] 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.

[11] "STE is shifting into company in June" [in Arabic], Alwatan, June 12, 2012, http://www.alwatan.sy/dindex.php?idn=124296.

[12] "Online Syria, Offline Syrians," The Initiative For an Open Arab Internet, accessed March 8, 2012; "One Social Network With A Rebellious Message," The Initiative For an Open Arab Internet, accessed March 8, 2012, http://old.openarab.net/en/node/1625.

[13] 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.

[14] "Syria cut off from the internet," BBC News, May 8, 2013, http://www.bbc.co.uk/news/world-middle-east-22446041.

[15] Lorenzo Franceschi-Bicchierai, "Syria Suffers Yet Another Internet Blackout," Mashable, May 15, 2013, http://mashable.com/2013/05/15/syria-internet-outage/.

[16] Darren Anstee, "Syria goes dark," DDoS and Security Reports: The Arbor Networks Security Blog, November 29th, 2012, http://ddos.arbornetworks.com/2012/11/syria-goes-dark/

[17] Darren Anstee, "Snapshot: Syria's Internet drops, returns," DDoS and Security Reports: The Arbor Networks Security Blog, December 12, 2012, http://ddos.arbornetworks.com/2012/12/snapshot-syrias-internet-drops-returns/

[18] "News From the Ground," [in Arabic], Telecomix: Syria, August 13, 2012, http://syria.telecomix.org/

[19] Skynews Arabia, "Internet disconnection in all of Syria," May 8, 2013, http://bit.ly/1xTJ8wt.

[20] Interviews with several activists in Syria wishing to remain anonymous, August 2011to March 2012.

communication. As such, many have taken to satellite technology to ensure that blackouts, sabotage, and destruction do not impede their ability to connect.[21]

Limits on Content

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. In recent years, censorship has expanded; the blocking of websites related to government opposition, human rights groups, the Muslim Brotherhood, and activism on behalf of the Kurdish minority is very common.[22] The Syrian government is suspected of possessing sophisticated technologies for filtering and surveillance, and self-censorship is highly prevalent, particularly in areas under government control. Despite these limitations, citizen journalists continue to make use of video-uploading sites and social networks to spread information about human rights abuses and the atrocities of war. Their role has become particularly important at a time when traditional journalists operate in highly unsafe conditions and foreign press visas are difficult to obtain. Many websites have also been blocked more recently, such as the magazine *Syria Oxygen* and the site SyriaStocks.[23]

A range of websites related to regional politics are also inaccessible, including the prominent London-based news outlets *Al-Quds al-Arabi* and *Asharq al-Awsat*, as well as several Lebanese online newspapers and other websites campaigning to end Syrian influence in Lebanon. Access to the entire Israeli top-level domain ".il" was also restricted. However, the websites of most international news sources and human rights groups have remained accessible.

Censorship is implemented by the STE and private ISPs with the use of 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."[24] In 2011, evidence emerged that the Syrian authorities were also using technology provided by the Italian company Area SpA to improve their censorship and surveillance abilities. The contract with Area 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, that was then sent to Area SpA, believing the equipment would be given to the Iraqi government, but logs obtained by the hacktivist group Telecomix in August 2011 revealed evidence of their use in Syria instead.[25] 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

[21] Amy Chozick, "For Syria's Rebel Movement, Skype Is a Useful and Increasingly Dangerous Tool," New York Times, November 30, 2012, http://www.nytimes.com/2012/12/01/world/middleeast/syrian-rebels-turn-to-skype-for-communications.html?_r=0.

[22] Internet Enemies, Reporters Without Borders, March 2011, http://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/2011/110311_Internetbericht_engl.pdf, visited on May 1, 2013. .

[23] See https://syria-stocks.com/forum/showthread.php?p=290187.

[24] Syria," OpenNet Initiative; Reporters Without Borders, "Syria," *Internet Enemies 2010* (Paris: Reporters Without Borders, March 18, 2010), http://www.unhcr.org/refworld/publisher,RSF,,SYR,4c21f66e28,0.html; "ThunderCache Overview," Platinum, Inc., accessed August 14, 2012, http://www.platinum.sy/index.php?m=91.

[25] Andy Greenberg, "Meet Telecomix, The Hackers Bent on Exposing Those Who Censor and Surveil The Internet," Forbes, December 26, 2011, http://www.forbes.com/sites/andygreenberg/2011/12/26/meet-telecomix-the-hackers-bent-on-exposing-those-who-censor-and-surveil-the-internet/.

the relevant investigations.[26] Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.[27] The *Wall Street Journal* identified efforts to block or monitor tens of thousands of opposition websites or online forums covering the uprising. Out of a sample of 2,500 attempts to visit Facebook, the logs revealed that three-fifths were blocked and two-fifths were permitted but recorded.[28]

The Syrian government also engages in filtering mobile phone text messages. Beginning in February 2011, such censorship was periodically reported around dates of planned protests. In February 2012, the news service Bloomberg reported that a series of interviews and leaked documents revealed 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 purchased from two separate Irish firms several years earlier for the alleged purpose of restricting spam.[29]

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.[30] Websites used to mobilize people for protests or resistance against the regime, including pages linked to the network of Local Coordination Committees (LCCs) that have emerged, continue to be blocked.[31] An online initiative to gather information and raise public awareness, the Mondaseh website, also remains blocked, [32] Websites that document human rights violations, such as the Violations Documentation Center, remain blocked.[33] Authorities have repeatedly blocked the website and key search terms of "SouriaLi" an internet radio station started by a group of pluralistic young Syrians.[34]

Facebook remains accessible in Syria after the government lifted a four-year block on the social-networking site in February 2011. Nonetheless, according to one Damascus-based activist, Facebook pages sometimes do not load correctly and show a TCP error. The video-sharing website YouTube was also unblocked, although it was not usable from mobile phone devices due to limits on data speeds.[35] Some activists suspected, however, that rather than a sign of openness, the regime's motive for unblocking the sites was to track citizens' online activities and identities. As of March 2012, both were within the top-five most visited websites in the country. More recently, neither of

[26] Blue Coat, "Update on Blue Coat Devices in Syria," news statement, December 15, 2011, http://www.bluecoat.com/company/news/statement-syria.

[27] "Blue Coat device logs indicated the levels of censorship in Syria," Hellias.github.com, accessed August 14, 2012, http://hellais.github.com/syria-censorship/.

[28] 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://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.

[29] Ben Elgin and Vernon Silver, "Syria Disrupts Text Messaging of Protesters With Made-in-Dublin Equipment," Bloomberg, February 14, 2012, http://www.bloomberg.com/news/2012-02-15/syria-blocks-texts-with-dublin-made-gear.html.

[30] Syria News / Hacktivist blog "Settings up Syria censorship-proof OpenVPN server" 4th June, 2012 https://syria.hacktivist.me/?p=148

[31] LCCs website: http://www.lccsyria.org/en/

[32] The Syrian, the English page is available at: http://english.the-syrian.com/

[33] "Leaked list of all blocked websites in Syria," Arab Crunch, May 10, 2013, http://arabcrunch.com/2013/05/leaked-list-of-all-blocked-web-sites-in-syria.html.

[34] Syria Untold, "Syrian Creativity: Radio SouriaLi Broadcasts over the Internet," GlobalVoices, June 7, 2013, http://globalvoicesonline.org/2013/06/07/syrian-creativity-radio-souriali-broadcasts-over-the-internet/.

[35] Interview with activist in Syria wishing to remain anonymous, December 2011.

the sites appear in the Top 25, perhaps due to users employing proxies that change their IP address to another country.[36] Other social media platforms like Twitter are freely available, although the presence of Syrian users on them is minimal.

Despite the free access to Facebook and YouTube, a range of other social media applications remain inaccessible in Syria. The Voice over Internet Protocol (VoIP) service Skype often suffers from disruptions either due to low speeds or intermittent blocking by the authorities. In February 2012, the government also began restricting access to certain applications for mobile phone devices that activists had been using to circumvent other blocks. Additionally, other applications reportedly blocked were the live video-streaming service Bambuser,[37] and WhatsApp, an application that allows users to send mobile phone text messages via the internet.[38] Instant messenger services such as eBuddy, Nimbuzz, and mig33 have been disabled by blocking the SMS that users must receive in order to activate their accounts. In other cases, certain online services—such as Google Maps or the photo-sharing tool Picasa—have been rendered inaccessible from Syria by their U.S.-based service providers due to restrictions related to economic sanctions against the country.[39] More applications, such as anti-virus software and updates to operating systems, remain blocked by sanctions, pushing many U.S.-based activists to ask for a "reboot" of the sanctions strategy.[40]

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 engaging in internet censorship. When a user seeks to access a blocked website, an error message appears implying a technical problem rather than deliberate government restriction. Decisions on which websites or keywords should be censored are made by parts of the security apparatus, including Branch 225, or by the executive branch.

In an environment of extreme violence and arbitrary "red lines," self-censorship is widespread. Sensitive topics include criticizing President Assad, his late father, the military, or the ruling Baath party. Publicizing problems faced by religious and ethnic minorities or corruption allegations related to the ruling family, such as those of Assad's cousin Rami Makhlouf, are also off limits. Most Syrian users are careful not only to avoid such sensitive topics when writing online, but also to avoid visiting blocked websites.[41] However, the period of May 2012 to April 2013 witnessed a large number of local Syrian users expressing opposition to Assad, his father, Makhlouf, the Baath party, and certain ethnic or sectarian groups.[42] In 2014, users living in areas under control of ISIL or other extremist groups have stepped up their self-censorship in order to avoid criticizing the militants or Islam.

[36] "Top Sites in SY," Alexa.com, accessed August 14, 2012, http://www.alexa.com/topsites/countries/SY.

[37] "Bambuser now blocked in Syria," Bambuser (blog), February 17, 2012, http://bit.ly/xu2HpI.

[38] Stuart Thomas, "Syrian government blocks access to WhatsApp," Memeburn.com, March 3, 2012, http://memeburn.com/2012/03/syrian-government-blocks-access-to-whatsapp/.

[39] On May 23, 2012, Google announced that it made Google Earth, Picasa and Chrome available for download in Syria. Yet, Google said that "As a U.S. company, we remain committed to full compliance with U.S. export controls and sanctions." Activists and internet users in Syria describe Google's step as insufficient, saying that there are tens of Google services still blocked in Syria including the entire Google Play App store on Android phones. See, "Software downloads in Syria," Official Google Blog, May 23, 2012, http://googleblog.blogspot.com/2012/05/software-downloads-in-syria.html?m=1.

[40] The New America Foundation "Do we need to reboot our sanctions strategy?" December 5, 2013, http://weeklywonk.newamerica.net/articles/do-we-need-to-reboot-our-sanctions-strategy/.

[41] Email communication from a Syrian blogger. Name was hidden.

[42] Interview, via Skype, with a Syrian activist. Damascus. November 2012. Name is hidden.

Pro-regime forces have employed a range of tactics to manipulate online content and discredit news reports or those posting them, though it is often difficult to directly link those who are carrying out these activities with the government. Most notable has been the emergence of the Syrian Electronic Army (SEA), a progovernment hacktivist group that targets the websites of opposition forces, human rights websites, and even Western media outlets (see "Violations of User Rights"). For news websites and other online forums based in the country, it is common for writers to receive phone calls from government officials offering "directions" on how to cover particular events.[43] The Syrian government also pursues a policy of supporting and promoting websites that publish progovernment materials in an attempt to popularize the state's version of events. These sites typically cite the reporting of the official state news agency SANA, with the same exact wording often evident across multiple websites. Interestingly, in 2012, the progovernment website Aksalser changed its stance to support the opposition and was subsequently blocked by the government.[44] Since early 2011, this approach has also been used to promote the government's perspective about the uprising and subsequent military campaign.[45]

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 places like the U.S. or Europe. Restrictions on importing funds into Syria have had a significant impact on the ability to publish content. For instance, recently, the website of the Syrian magazine *Syrian Oxygen* attempted to buy SSL certificates for their website. However, they were not able to obtain the certificates from U.S. providers as the domain syrianoxygen.com has the word Syria in it.

Online tools have proven crucial for Syrians in 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. Syrians are very active on Facebook, using it as a platform to share news, discuss events, release statements, and coordinate both online and offline activities.[46] A Facebook petition for the release of Youssef Abdelke, initiated by a group of Syrian intellectuals and artists, was signed by over 2,500 users.[47] Abdelke, an illustrator and painter who has often expressed political dissent through his art, was arrested in July 2013 after he signed a declaration, posted online, which called for a democratic transition and the stepping down of President Assad.[48] He was released one month later.[49]

In addition, one observer has called Syria the first "YouTube War" due to the extraordinarily high coverage of human rights violations, military battles, and post-conflict devastation that is contained in videos posted to the site.[50] Indeed, as the Syrian government shifted to the use of heavy arms

[43] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."

[44] The Syrian "Aksalser website with the revolution," August 28, 2012, http://the-syrian.com/archives/86170.

[45] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."

[46] Vocativ, "Syrian fight Fire with Facebook" September 23, 2013, http://www.vocativ.com/09-2013/fight-fire-with-facebook-how-syrian-rebels-are-waging-real-war-one-status-update-at-a-time/.

[47] See https://www.facebook.com/events/258608904264261/, accessed March 14, 2014.

[48] "Déclaration pour Syrie democratique" (Declaration for a Democratic Syria), Babelmed, http://www.babelmed.net/cultura-e-societa/48-syria/13391-declaration-pour-syrie-democratique.html, accessed March 14, 2014.

[49] Syria: web campaign to free jailed artist Youssef Abdelke, France 24, July 24, 2013, http://www.france24.com/en/20130723-syria-youssef-abdelke-internet/.

[50] Christophe Koettl, "The YouTube War: Citizen Videos Revolutionze Human Rights Monitoring in Syria," PBS Mediashift, February 18, 2014, http://www.pbs.org/mediashift/2014/02/the-youtube-war-citizen-videos-revolutionize-human-rights-monitoring-in-syria/.

and missiles against opposition fighters, the role of citizen journalists has shifted from live event coverage to documenting the bloody aftermath of an attack. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, rebel groups, and civil society groups, mostly documenting attacks. A Syrian group categorizing YouTube videos and sharing them via the platform OnSyria had posted almost 200,000 videos in 2013.[51] Since full media coverage throughout the country is very difficult, citizen journalists have designed a technique to ensure full media coverage of the entire country. "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.

Controversially, both Facebook and YouTube have removed content related to the Syrian uprising under the justification that content posted to the accounts promotes violence or contains graphic content. According to digital security NGO SecDev, dozens of opposition pages, media centers, and independent NGOs have been closed by Facebook. These include numerous pages of Local Coordination Councils, or LCCs, and the London-based Syrian Network for Human Rights. Activists believe that Facebook users sympathetic to President Assad may be reporting the pages as violating user guidelines en masse, thereby provoking Facebook into action. One activist, Razan Zaitouneh of the Violations Documentation Center, shared a letter urging Facebook to keep the sites 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 have taken to using the site.[52]

Violations of User Rights

Syria's constitution provides for freedom of opinion and expression, but these are severely restricted in practice, both online and offline. Furthermore, a handful of laws are used to prosecute online users who express their opposition to the government. Citizen journalists and YouTube users are detained and often tortured by both government forces and, at times, rebel fighters. Surveillance tools are used to identify and harass those who oppose the Assad government, often through targeted malware attacks against their computer systems and online accounts. Finally, the websites of opposition groups and human rights organizations are consistently targeted with cyberattacks from hackers linked to the government.

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 terms such as threatening "national unity" or "publishing false news that may weaken national sentiment."[53] 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.[54] In addition, Syria's cybercrime law allows prison sentences of up to three years and fines of up to SYP 250,000 (US$ 1,500) for anyone who incites or promotes crime through

[51] See http://onsyria.org/

[52] Michael Pizzi, "The Syrian Opposition Is Disappearing From Facebook," Atlantic, February 4, 2014, http://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/.

[53] Articles 285, 286, 287 of the Syrian Penal Code.

[54] Article 378 of the Syrian Penal Code.

computer networks.[55] The judiciary lacks independence and its decisions are often arbitrary. Some civilians have been tried before military courts.

Since antigovernment protests broke out in February 2011, the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. However, many of those targeted are not known for their political activism, so the reason for their arrest is often unclear. This arbitrariness has raised fears that users could be arrested at any time for even the simplest online activities—posting on a blog, tweeting, commenting on Facebook, sharing a photo, or uploading a video—if it is perceived to threaten the regime's control. Veteran blogger Ahmad Abu al-Khair was taken into custody in February 2011 while traveling from Damascus to Banias and was later released, though he has remained in hiding.[56] More recently, in an effort to pressure al-Khair to turn himself in, security forces have twice detained his brother, once for a period of 60 days.[57] Bassel Khartabil, an open source activist and recipient of the 2013 Index on Censorship Digital Freedom Award, remains in prison after he was taken by authorities without explanation in March 2012.[58]

Human rights activists who work online are also targeted by the government and the rebels. Four members of the Violations Documentation Center (VDC) were kidnapped by an unknown group from a rebel-controlled area in December 2013.[59] Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in February 2012, arresting 14 employees.[60] One SCM member and civil rights blogger, Razan Ghazzawi,[61] was detained for 22 days.[62] Three others remain in prison and face up to 15 years for "publicizing terrorist acts" due to their role in documenting human rights violations by the Syrian regime.[63] The organization's founder and director, Mazen Darwich, has been held incommunicado since his arrest. [64]

Once in custody, citizen journalists, bloggers, and other detainees reportedly suffered severe torture on behalf of government authorities. Although the precise number is unknown, it is estimated that dozens of individuals have been tortured to death for filming protests or abuses and then uploading them to YouTube.[65] In some cases around the country, the Syrian army appeared to deliberately target online activists and photographers. In response to such brutality, hundreds of activists have

[55] http://www.fosigrid.org/middle-east/syria

[56] Anas Qtiesh, "Syrian Blogger Ahmad Abu al-Khair Arrested This Morning," Global Voices Online, February 20, 2011, http://advocacy.globalvoicesonline.org/2011/02/20/syrian-blogger-ahmad-abu-al-khair-arrested-this-morning/.

[57] Email communication with activist in Syria who wished to remain anonymous, April 2012.

[58] William Echikson, "Supporting freedom of expression in all forms," Google – Europe Blog, March 23, 2013, http://googlepolicyeurope.blogspot.co.uk/2013/03/supporting-freedom-of-expression-in-all.html.

[59] Hania Mourtada, "'She Was My Mandela' – Famous Syrian Activist Gets Abducted," Time, December 11, 2013, http://world.time.com/2013/12/11/she-was-my-mandela-famous-syrian-activist-gets-abducted/.

[60] Maha Assabalani, "My colleagues are in prison for fighting for free expression," UNCUT - Index on Censorship, May 11, 2012, http://uncut.indexoncensorship.org/2012/05/my-colleagues-are-in-prison-for-fighting-for-free-expression/.

[61] Jared Malsin, "Portrait of an Activist: Razan Ghazzawi, the Syrian Blogger Turned Exile," Time, April 2, 2013, http://world.time.com/2013/04/02/portrait-of-an-activist-meet-razan-ghazzawi-the-syrian-blogger-turned-exile/.

[62] An interview with Syrian blogger via Skype. February 2013, name is hidden.

[63] "Syrian free speech advocates face terrorism charges," Index on Censorship, May 17, 2013, http://www.indexoncensorship.org/2013/05/syria-there-are-not-enough-prisons-for-the-free-word/.

[64] Skype interview with Syrian activist, March 2013. The name is hidden.

[65] Interview via Skype with A.A, Human Rights Lawyer in Damascus, December 12, 2011. Name is hidden.

gone into hiding and dozens have fled the country, fearing that arrest may not only mean prison, but also death under torture.[66]

Attacks on activists and citizen journalists were not limited to Syrian government forces. The Free Syrian Army (FSA), the opposition armed movement, have committed many attacks on videographers and citizen journalists, mainly in the suburbs of Aleppo. Since the "liberation" of Aleppo province, activists and photographers were targeted by FSA fighters more than they were targeted by the Syrian government.[67] Further, the "Al Nusra Front" (*Jabhat al Nusra*), a group of armed extremists, have arrested tens of young citizen journalists for weeks at a time, and in one incident, opened fire on them for filming a protest in Bostan al Qaser in Aleppo.[68]

According to Reporters Without Border, at least 51 netizens and citizen journalists were killed between May 2013 and May 2014. In one case from December 2013, the "Islamic State of Iraq and the Levant" (ISIL), an armed extremist group, killed 50 prisoners, including many journalists and media activists such as Syrian journalist Sultan al-Shami.[69] Abdulwahab Mulla, a Syrian journalist known for his satirical YouTube comedy show "3-Star Revolution," was kidnapped by masked gunmen on October 8, 2013. He was taken from his home in rebel-controlled areas of Aleppo. Many have hypothesized that extremist militants, such as ISIL, are behind the kidnappings.[70] Many citizen journalists have lost their lives while documenting clashes. On May 21, 2013, 14-year-old citizen journalist Omar Qatifaan was killed while covering a battle between government forces and the Free Syrian Army near the city of Daraa in southern Syria, near the Jordanian border.[71]

Competition among activists has also led to violations against each other. In one 2013 case, a citizen journalist used armed thugs to kidnap the administrator of a Facebook page for a competing media groups, aiming to shut it down. The victim sought help from another armed group, who, in turn, abducted the first individual. Both of the kidnapped group administrators were beaten to provide passwords of their Facebook accounts. Eventually, both men were released.[72]

Anonymous communication is possible online but increasingly restricted. Registration is required to purchase a cell phone, though over the past years, activists have begun using the SIM cards of friends and colleagues killed in clashes with security forces in order to shield their identities. Cell phones from neighboring countries like Turkey and Lebanon have been widely used since 2012, notably by Free Syrian Army fighters. However, civilians in Syria are now also using these foreign cell phones due to the lack of cell service in the country. Meanwhile, activists and bloggers released from custody report being pressured by security agents to provide the passwords of their Facebook, Gmail, Skype, and other online accounts.[73]

[66] Interviews with two photographers who have taken refuge in Turkey, December 2011.

[67] Interview with activist from Aleppo, via Skype, January 2013. Name is hidden.

[68] Interview with lawyer from Aleppo. Istanbul, Turkey. January 2013. Name is hidden.

[69] Zaman Alwasel " Al Qaeda Affiliate ISIL kills 50 hostages including media activists," January 7, 2014, http://www.zamanalwsl.net/en/news/3173.html.

[70] Nour Al-Ali, "Syrian Journalist Abdulwahab Mulla Kidnapped in Liberated Aleppo," Global Voices, November 10, 2013, http://globalvoicesonline.org/2013/11/10/syrian-journalist-abdulwahab-mulla-kidnapped-in-liberated-aleppo/.

[71] Rami Alhames, "14-year-old Citizen Journalist Killed Covering Clashes in Syria," GlobalVoices, May 22, 2013, http://globalvoicesonline.org/2013/05/22/teen-citizen-journalist-killed-in-syria/.

[72] The author helped mediate this case, which occurred in the Damascus suburban area in February 2013. Names are hidden.

[73] Interviews with released bloggers, names were hidden.

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.[74] 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.[75] Failure to comply may cause the website to be blocked and is punishable by a fine of between SYP 100,000 and 500,000 (US$1,700 to $8,600). 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$1,500 to $7,500).[76] In early 2014, however, the authorities were not vigorously enforcing these regulations.

Surveillance is widespread in Syria, as the government capitalizes on the centralized internet connection to intercept user communications. In early November 2011, Bloomberg reported that in 2009 the Syrian government had contracted Area SpA to equip them with an upgraded system that would enable interception, scanning, and cataloging of all email, internet, and mobile phone communication flowing in and out of the country. According to the report, throughout 2011, employees of Area SpA had visited Syria and began setting up the system to monitor user communications in near real-time, alongside graphics mapping users' contacts.[77] The exposé sparked protests in Italy and, a few weeks after the revelations, Area SpA announced that it would not be completing the project.[78] No update is available on the project's status or whether any of the equipment is now operational.

One indication that the Syrian authorities were potentially seeking an alternative to the incomplete Italian-made surveillance system were reports of sophisticated phishing and malware attacks targeting online activists that emerged in February 2012.[79] 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.[80] Later, EFF reported the appearance of a fake YouTube channel carrying Syrian 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

[74] "Law of the rulers to communicate on the network and the fight against cyber crime" [in Arabic], Articles 5-12, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm (site discontinued). Informal English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.

[75] "Law of communicating on the network and fighting against cyber crime" [in Arabic], Article 2, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm.

[76] "Law of communicating on the network and fighting against cyber crime" [in Arabic], Article 8, accessed March 8, 2012, http://www.sana.sy/ara/2/2012/02/10/pr-399498.htm. English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.

[77] Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," Bloomberg, November 3, 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.

[78] Vernon Silver, "Italian Firm Said To Exit Syrian Monitoring Project," Bloomberg, November 28, 2011, http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html.

[79] "Computer spyware is newest weapon in Syrian conflict," CNN, February 17, 2012 http://www.cnn.com/2012/02/17/tech/web/computer-virus-syria. /

[80] 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.

its discovery, the fake site was taken down.[81] Due to the prevailing need for circumvention and encryption tools among activists and other opposition members, Syrian authorities have developed fake Skype encryption tools and a fake VPN application, both containing harmful Trojans.[82]

A report from Kaspersky Labs, published in August 2014, revealed that some 10,000 victims' computers had been infected with RATs some 10,000 victims in Syria, as well as in other Middle Eastern countries and the United States. [83] The attackers sent messages via Skype, Facebook, and YouTube to dupe victims into downloading surveillance malware. One file was disguised as a spreadsheet listing names of activists and "wanted" individuals.

Cyberattacks have become increasingly common in Syria since February 2011, in response to the growing circulation of anti-Assad videos and other content online. Most notable has been the Syrian Electronic Army (SEA), a hacktivist group that emerged in April 2011. Though the group's precise relationship to the regime is unclear, evidence exists of government links or at least tacit support. These include the SEA registering its domain in May 2011 on servers maintained by the Assad-linked Syrian Computer Society;[84] a June 2011 speech in which the president explicitly praised the SEA and its members;[85] and positive coverage of the group's actions in state-run media.[86] The SEA's main activities include hacking and defacing Syrian opposition websites and Facebook accounts, as well as targeting Western or other news websites perceived as hostile to the regime. However, some foreign websites from the academic, tourism, or online marketing sectors have also been targeted.[87]

A huge shift in the level of hacking operations happened at the end of 2013, when the SEA was able to hack the *New York Times* website,[88] the U.S. Marines website,[89] Facebook,[90] and many others. Most of the attacks occurred on the DNS level, which involved redirecting requests for the domain name to another server. The Twitter account of Barack Obama, run by staff from Organizing for Action

[81] Eva Galperin and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware.

[82] "Syrian Malware" Up-to-date website collecting the malware http://syrianmalware.com/

[83] For the full report, see "Syrian Malware, the evolving threat," Kaspersky Lab Global Research and Analysis Team," August 2014, https://securelist.com/files/2014/08/KL_report_syrian_malware.pdf.

[84] The Syrian Electronic Army, http://syrian-es.com/.

[85] Haroon Siddique and Paul Owen, "Syria: Army retakes Damascus suburbs," Middle East Live (blog), *The Guardian*, January 30, 2012, http://www.guardian.co.uk/world/middle-east-live/2012/jan/30/syria-army-retakes-damascus-suburbs; "Speech of H.E. President Bashar al-Assad at Damascus University on the situation in Syria," official Syrian news agency (SANA), June 21, 2011, http://www.sana.sy/eng/337/2011/06/21/353686.htm.

[86] See positive coverage on state-run websites [in Arabic]: Thawra.alwedha.gov.sy, May 15, 2011, http://thawra.alwehda.gov.sy/_print_veiw.asp?FileName=18217088020110516122043; Wehda.alwedha.gov.sy, May 17, 2011, http://wehda.alwehda.gov.sy/_archive.asp?FileName=18235523420110517121437.

[87] Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," OpenNet Initiative, accessed August 14, 2012, http://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army.

[88] Christine Haughney and Nicole Perlroth, "Times Site Is Disrupted in Attack by Hackers," New York Times, August 27, 2013, http://www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html.

[89] Wall Street Journal, "Syrian Electronic Army Hacks Marines Website," September 2, 2013, http://blogs.wsj.com/washwire/2013/09/02/syrian-electronic-army-hacks-marines-website/.

[90] "Syrian Electronic Army Hacks Facebook's Domain Record," Mashable, February 6, 2014, http://mashable.com/2014/02/05/syrian-electronic-army-hacks-facebook-domain/.

(OFA), was briefly hacked by the SEA, resulting in the account posting shortened links to SEA sites.[91] The hackers had gained access to the Gmail account of an OFA staffer.

On March 17, 2013, the SEA hacked the website and Twitter feed of Human Rights Watch, redirecting visitors to the SEA homepage.[92] The Mondaseh website was also hacked by the SEA in early January 2012.[93] The SEA is known to post private information, such as the phone numbers and addresses of antigovernment activists, on Facebook.[94] Most of its pages have been closed by Facebook for violating terms of use. However, progovernment media outlets continue to publish hacked emails from opposition figures. These tactics continued in 2014 with the high-profile hacking of *Forbes* in February.[95]

[91] "The Syrian Electronic Army Hacked Obama's Twitter Links And Campaign Emails," Tech Crunch, October 28, 2013, http://techcrunch.com/2013/10/28/obamas-twitter-links-and-campaign-emails-were-hacked-by-the-syrian-electronic-army/.

[92] Max Fisher, "Syria's pro-Assad hackers infiltrate Human Rights Watch Web site and Twitter feed," Washington Post, March 17, 2013. http://wapo.st/1eU9nKI.

[93] See YouTube video by SEA celebrating the hacking: http://www.youtube.com/watch?v=48q34HlIBOk.

[94] Zeina Karam, "Syrian Electronic Army: Cyber Warfare From Pro-Assad Hackers," Huffington Post, September 27, 2011, http://www.huffingtonpost.com/2011/09/27/syrian-electronic-army_n_983750.html.

[95] Andy Greenberg, "How the Syrian Electronic Army Hacked Us: A Detailed Timeline," Forbes, February 20, 2014, http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/.