SYRIA

	2012	2013
INTERNET FREEDOM STATUS	**NOT FREE**	**NOT FREE**
Obstacles to Access (0-25)	23	24
Limits on Content (0-35)	25	25
Violations of User Rights (0-40)	35	36
Total (0-100)	**83**	**85**

* 0=most free, 100=least free

POPULATION: 22.5 million
INTERNET PENETRATION 2012: 24 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Not Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Telecommunications infrastructure has deteriorated as a result of the armed conflict and authorities periodically shut down internet service to thwart citizen journalism and communications among rebel fighters (see **OBSTACLES TO ACCESS**).
- Several users remained in prison for expressing anti-regime views or documenting human rights violations online (see **VIOLATIONS OF USER RIGHTS**).
- Extralegal attacks have escalated, as several online activists and citizen journalists were attacked or killed by military units (see **VIOLATIONS OF USER RIGHTS**).
- Several users were targeted with surveillance malware, and hacktivism against human rights organizations, particularly by the Syrian Electronic Army, was prominent (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

The regime of President Bashar al-Assad has maintained tight control over information and communication technologies (ICTs) in Syria for many years, dominating key networks via government-linked service providers and engaging in extensive blocking of websites. The internet was first introduced to Syria in 2000, reaching only 30,000 users that year. By the end of 2010, more than one-fifth of the population was online. It is in the context of such growing access that the internet and social media have played an important role in a civic protest movement, which began in February 2011, calling for the end of President Bashar al-Assad's undemocratic rule and which, by early 2012, had turned into a fully-fledged armed conflict.

Amidst deadly repression and barred entry to foreign correspondents, citizen journalists using mobile phone devices and video-sharing websites have been a critical channel for informing Syrians and the international community about events in the country. In response, government censorship and retaliation against internet users dramatically intensified. Among the tactics employed have been periodic shutdowns of the internet and mobile phone networks, intensified filtering of websites, and various sophisticated means of monitoring and tracking internet users' online activities. In addition, Syria has emerged as one of the most dangerous countries in the world for citizen journalists and bloggers, with an untold number arrested and several killed.

The role of citizen journalists has lessened, however, as the popular uprising has deteriorated into an armed conflict. The infrastructure in at least seven major cities and provinces has been badly damaged, with many lacking internet access and power. Traditional journalists and human rights groups have slowly returned to northern areas of the country, which are now controlled by rebel groups, although disparate attacks against by radical fighters have been documented. Still, areas controlled by the opposition do enjoy a greater degree of freedom than those controlled by the Syrian government, even if a lack of working infrastructure has limited many individuals to using more expensive options, such as satellite internet. As the country's internet capacity has dwindled over the past year, the situation has become even more difficult for activists and bloggers.

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.[1] This dynamic only worsened after 2011, as inflation and electricity outages increased dramatically following public protests and the government's corresponding crackdown. Damage to the country's communications infrastructure has been 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 2012, the International Telecommunications Union (ITU) estimated that 24 percent of the population had

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

access to the internet.[2] However, the number of broadband subscribers tripled from last year, reaching 378,000.[3] Mobile phone penetration was notably higher, at about 61 percent of the population at the end of 2012.[4]

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 of almost $25 for 4 MB and $200 for unlimited data usage.[5] In addition, the service is primarily only offered in large cities. Most users connect to the internet through a fixed dial-up connection at speeds of only 256 Kbps, which severely limits their ability to download or view multimedia content. During peak times, the speed is even slower.[6] Broadband ADSL service remains limited due to the inadequate infrastructure in rural areas and relatively high 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 $30) as of May 2012,[7] in a country where gross domestic product per capita, when taken on a monthly basis, is only $274.[8]

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.[9] This centralization has also 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.[10] Private ISPs like Aya, as well as mobile phone internet providers, are required to sign a memorandum of understanding to connect via the gateways controlled by the SIO.[11]

At least 11 internet service providers (ISPs) have entered the market since the end of 2005, raising the total number of ISPs to 14.[12] Independent satellite connections are prohibited.[13] ISPs and

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2012, accessed August 1, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[3] Ibid.
[4] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2012, accessed August 1, 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[5] "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.
[6] "Internet Enemies," Reporters Without Borders, March 2011, http://bit.ly/eLXGvi.
[7] "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.
[8] "GDP per capita (current US$)," The World Bank, 2008-12, accessed August 1, 2013, http://data.worldbank.org/indicator/NY.GDP.PCAP.CD.
[9] See the Ministry of Telecommunications and Technology's website (in Arabic) at: http://www.moct.gov.sy/moct/?q=ar/node/58.
[10] See STE's website at: http://www.in-ste.gov.sy/inindex_en.html.
[11] 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.
[12] "STE is shifting into company in June" [in Arabic], Alwatan, June 12, 2012, http://www.alwatan.sy/dindex.php?idn=124296.

cybercafés must obtain approval from the STE and pass security vetting by the Ministry of Interior and other security services.[14] Moreover, cybercafé 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 2012 and early 2013, the Syrian government has continued to obstruct connectivity through its control of key infrastructure, at times shutting down the internet and mobile phone networks entirely or at particularly sites of unrest. A nationwide shutdown was imposed on November 29, 2012, lasting two and a half days.[15] Another nationwide shutdown was imposed in December 11, 2012.[16] 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.[17] According to activists, broadband is often throttled and 3G services shut off as pro-regime forces prepare to besiege a city.[18] In other instances—such as in Daraa in March 2012—the entire electrical grid has been shut down for hours at a time. The government's deliberate use of such measures was evident from a leaked document issued by the General Head of the National Security Office in May 2011 explicitly ordering that "the internet is to be completely disconnected in Daraa, Homs, and the eastern provinces starting on Wednesday at 14:00."[19]

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.[20] 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 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.

---

[13] "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.

[14] 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.

[15] 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/

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

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

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

[19] "Leaked Syrian document shows how Assad banned internet access and satellite phones," The Telegraph, June 27, 2011. http://bit.ly/mLaugR.

[20] 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. .

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 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."[21] In 2011, evidence emerged that the Syrian authorities were also using censorship and surveillance software manufactured by the U.S. firm Blue Coat Systems. Blue Coat had reportedly sold 14 devices to an intermediary in Dubai, 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.[22] In October of that year, Blue Coat acknowledged that 13 of the above 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.[23] Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.[24] 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.[25]

The Syrian government also engages in filtering of 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.[26]

The government continues to block circumvention tools, internet security software, and applications that enable anonymous communications. Websites used to mobilize people for protests

[21] 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.

[22] 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/.

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

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

[25] 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.

[26] 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.

or resistance against the regime, including pages linked to the network of Local Coordination Committees (LCCs) that have emerged, continued to be blocked as of May 2013.[27] An online initiative to gather information and raise public awareness, the Mondaseh website, also remains blocked. [28]

Facebook remained accessible in Syria after the government lifted a four-year block on the social-networking site in February 2011. The video-sharing website YouTube was also unblocked, although it was not usable from mobile phone devices due to limits on data speeds.[29] As of March 2012, both were within the top-five most visited websites in the country (more recent data is not available).[30] 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. 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 Web 2.0 applications remain inaccessible in Syria, including the blog-hosting platform Blogger and the VoIP service Skype. 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[31] and WhatsApp, an application that allows users to send mobile phone text messages via the internet.[32] Instant messenger services such as eBuddy, Nimbuzz, and mig33 have been blocked as well. 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.[33]

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 the abovementioned 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

[27] LCCs website: http://www.lccsyria.org/en/
[28] The Syrian, the English page is available at: http://english.the-syrian.com/
[29] Interview with activist in Syria wishing to remain anonymous, December 2011.
[30] "Top Sites in SY," Alexa.com, accessed August 14, 2012, http://www.alexa.com/topsites/countries/SY.
[31] "Bambuser now blocked in Syria," Bambuser (blog), February 17, 2012, http://bit.ly/xu2Hpl.
[32] Stuart Thomas, "Syrian government blocks access to WhatsApp," Memeburn.com, March 3, 2012, http://memeburn.com/2012/03/syrian-government-blocks-access-to-whatsapp/.
[33] 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.

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.[34] 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.[35]

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) since April 2011, a pro-government hacktivist group that targets the websites of opposition forces and human rights websites, often shutting them down (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" for how to cover particular events.[36] The Syrian government also pursues a policy of supporting and promoting websites that publish pro-government 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. Since early 2011, this approach has also been used to promote the government's perspective about the uprising and subsequent military campaign.[37]

Social media has played a crucial role in the Syrian uprising, though its primary utility has been information sharing rather than planning street protests. The "Syrian Revolution 2011" Facebook page, which by March 2013 had over 750,000 members from both inside and outside the country, has been a vital source of information for dissidents.[38] 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 an attack. Several YouTube channels belong to armed rebels, particularly Islamist groups. Both Facebook and YouTube have removed content related to the Syrian uprising, mainly due to content that promotes violence or contains graphic content, such as videos of torture or killing. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, mostly documenting attacks. A Syrian group working on categorizing YouTube videos and sharing them via a platform called "OnSyria" had posted almost 200,000 videos as of April 2013.[39]

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

[34] Email communication from a Syrian blogger. Name was hidden.
[35] Interview, via Skype, with a Syrian activist. Damascus. November 2012. Name is hidden.
[36] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."
[37] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."
[38] "The Syrian Revolution 2011 Facebook Statistics," Socialbakers.com, accessed March 31, 2013, http://www.socialbakers.com/facebook-pages/420796315726-the-syrian-revolution-2011.
[39] See http://onsyria.org/

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."[40] 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.[41] The judiciary lacks independence and its decisions are often arbitrary. Furthermore, some civilians have been tried before military courts.

Since anti-government 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, making the reasons behind their arrest 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 to released, though he has remained in hiding.[42] 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.[43] 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.[44]

Human rights activists who work online are also targeted by the government. Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in February 2012, arresting 14 employees.[45] SCM member and civil rights blogger Razan Ghazzawi[46] was released after 22 days in detention and fled to Sweden.[47] Five members remain in prison and face up to 15 years for "publicizing terrorist acts" over their role in documenting human rights violations by the

[40] Articles 285, 286, 287 of the Syrian Penal Code.
[41] Article 378 of the Syrian Penal Code.
[42] 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/.
[43] Email communication with activist in Syria who wished to remain anonymous, April 2012.
[44] 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.
[45] 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/.
[46] 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/.
[47] An interview with Syrian blogger via Skype. February 2013, name is hidden.

Syrian regime.[48] The organization's founder and director, Mazen Darwich, remained in incommunicado detention as of March 2013. [49]

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.[50] In some cases, the Syrian army appeared to deliberately target online activists and photographers all across the country. In one high-profile case from February 2012, Anas al-Tarsha, a videographer who documented unrest in the besieged city of Homs, was killed by a mortar round while filming the bombardment of the city's Qarabees District.[51] At least five of the citizen journalists who worked for the Damascus-based Shaam News Network, whose videos have been used extensively by international news organizations, were killed during 2012 and early 2013. Among them were Ghaith Abd al-Jawad and Amr Badir al-Deen Junaid, both from Qaboun Media Center, a group of opposition citizen journalists who film clashes in the neighborhood of Qaboun and publish the unattributed videos online.[52] In response to such brutality, hundreds of activists have gone into hiding and dozens have fled the country, fearing that arrest may not only mean prison, but also death under torture.[53]

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.[54] Further, "Al Nusra Front" (*Jabhat al Nusra*), a group of armed extremists, have arrested tens of young citizen journalists for weeks, and in one incident, opened fire on them for filming a protest in Bostan al Qaser in Aleppo.[55]

Competition among activists has also led to violations against each other. In one case, a citizen journalist used armed thugs to kidnap the administrator of a competing Facebook page for 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.[56]

Anonymous communication is possible online but increasingly restricted. Registration is required upon purchasing a cell phone, though over the past year, activists have begun using the SIM cards of

[48] "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/.
[49] Skype interview with Syrian activist, March 2013. The name is hidden.
[50] Interview via Skype with A.A, Human Rights Lawyer in Damascus, December 12, 2011. Name is hidden.
[51] Committee to Protect Journalists, Anas al-Tarsha, February 24, 2012. http://www.cpj.org/killed/2012/anas-al-tarsha.php , visited on December 2012.
[52] Committee to Protect Journalists, Ghaith Abd al-Jawad, March 10, 2013, available at http://www.cpj.org/killed/2013/ghaith-abd-al-jawad.php, visited March 31, 2013.
[53] Interviews with two photographers who have taken refuge in Turkey, December 2011.
[54] Interview with activist from Aleppo, via Skype, January 2013. Name is hidden.
[55] Interview with lawyer from Aleppo. Istanbul, Turkey. January 2013. Name is hidden.
[56] The author helped mediate this case, which occurred in the Damascus suburban area in February 2013. Names are hidden.

friends and colleagues killed in clashes with security forces in order to shield their identities. Cell phones of neighboring countries like Turkey and Lebanon have been widely used during 2012 and 2013, notably by Free Syrian Army fighters. Meanwhile, activists and bloggers released from custody reported being pressured by security agents to provide the passwords of their Facebook, Gmail, Skype, and other online accounts.[57]

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.[58] 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.[59] Failure to comply may cause the website to be blocked and is punishable by a fine of between SYP 100,000 and 500,000 ($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 ($3,400 to $17,000).[60] As of April 2013, 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, an Italian surveillance company, to equip them with an upgraded system that would enable interception, scanning, and cataloging of all e-mail, 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.[61] The exposé sparked protests in Italy and, a few weeks after the revelations, Area SpA announced that it would not be completing the project.[62] No update is available on the project's status or whether any of the equipment is now operational.

In a potential indication that the Syrian authorities were seeking an alternative to the incomplete Italian-made surveillance system, in March 2012 reports emerged of sophisticated phishing and malware attacks targeting online activists. The U.S.-based Electronic Frontier Foundation (EFF) reported that malware called "Darkcomet RAT" and "Xtreme RAT" had been found on activists' computers and were capable of capturing webcam activity, logging keystrokes, stealing passwords,

[57] Interviews with released bloggers, names were hidden.
[58] "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.
[59] "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.
[60] "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.
[61] 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.
[62] 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.

and more. Both applications sent the data back to the same IP address in Syria and were circulated via e-mail and instant messaging programs.[63] Later, EFF reported the appearance of a fake YouTube channel carrying Syrian opposition videos that requested users' login information and urged them to download an update to Adobe Flash, which was in fact a malware program that enabled the stealing of data from their computer. Upon its discovery, the fake site was taken down.[64]

Cyberattacks have become increasingly common in Syria since February 2011, responding 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[65] in May 2011 on servers maintained by the Assad-linked Syrian Computer Society,[66] a June 2011 speech in which the president explicitly praised the SEA and its members,[67] and positive coverage of the group's actions in state-run media.[68]

The SEA's key 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.[69] On March 17, 2013, the SEA hacked the website and Twitter feed of Human Rights Watch, redirecting to the SEA homepage.[70] The Mondaseh website was also hacked by the SEA in early January 2012.[71] The SEA is known to post private information, such as the phone numbers and addresses of anti-government activists, onto its Facebook pages.[72] Most of these pages have subsequently been closed by Facebook for violating its terms of use. However, pro-government media outlets continued to publish hacked e-mails from opposition figures.

---

[63] 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.
[64] 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.
[65] The Syrian Electronic Army, http://syrian-es.com/.
[66] 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.
[67] "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.
[68] 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=182170880201105161220 43; Wehda.alwedha.gov.sy, May 17, 2011, http://wehda.alwehda.gov.sy/_archive.asp?FileName=18235523420110517121437.
[69] 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.
[70] Max Fisher, "Syria's pro-Assad hackers infiltrate Human Rights Watch Web site and Twitter feed", The Washington Post, March 17, 2013. http://wapo.st/1eU9nKI.
[71] See YouTube video by SEA celebrating the hacking: http://www.youtube.com/watch?v=48q34HlIBOk.
[72] 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.