SYRIA

	2011	2012
INTERNET FREEDOM STATUS	**n/a**	**Not Free**
Obstacles to Access (0-25)	n/a	23
Limits on Content (0-35)	n/a	25
Violations of User Rights (0-40)	n/a	35
Total (0-100)	**n/a**	**83**

* 0=most free, 100=least free

POPULATION: 23 million
INTERNET PENETRATION 2011: 23 percent
WEB 2.0 APPLICATIONS BLOCKED: Yes
NOTABLE POLITICAL CENSORSHIP: Yes
BLOGGERS/I USERS ARRESTED: Yes
PRESS FREEDOM STATUS: Not Free

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 al-Assad's rule and which by early 2012 had turned into a full-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, the 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.

OBSTACLES TO ACCESS

Syria's telecommunications infrastructure is one of the least developed in the Middle East, with broadband connections being among the most difficult and expensive to acquire.[1] This dynamic only worsened in 2011 and 2012, as inflation and electricity outages increased dramatically following public protests and the government's corresponding repression. The communications infrastructure was badly damaged, especially in cities like Homs that were subject to particularly severe shelling by the Syrian armed forces. By the end of 2011, the International Telecommunications Union (ITU) estimated that 22.5 percent of the population—around five million people—had used the internet.[2] However, the number of broadband subscribers was only 121,300.[3] Mobile phone penetration was notably higher, reaching about 63 percent of the population at the end of 2011.[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 (almost US$25 for 4 MB or US$200 for unlimited data usage).[5] In addition, MTN, one of two main providers, only offers the service in large cities. Most other users connect to the internet via a dial-up connection and a fixed-line telephone subscription. Most internet users are restricted to 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 for two reasons: a lack of necessary 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 US$30) as of May 2012, in a country where the average monthly per capita income does not exceed US$200.[7]

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

[2] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.

[3] Ibid.

[4] International Telecommunication Union (ITU), "Mobile-cellular telephone subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.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://www.surf.sy/Sitemap/Home/Prices/tabid/214/language/ar-SY/default.aspx.

[6] "Internet Enemies," Reporters Without Borders, March 2011, http://www.reporter-ohne-grenzen.de/fileadmin/rte/docs/2011/110311_Internetbericht_engl.pdf.

[7] "Services and price" [in Arabic], Syrian Computer Society Network (SCS-NET), accessed March 8, 2012 http://www.scs-net.org/portal/OurConnection/OurConnections/SCSADSL/PlansPrices/tabid/493/Default.aspx.

At least eleven internet service providers (ISPs) have entered the market since the end of 2005, raising the total number of ISPs to 14.[8] In practice, however, 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 infrastructure. 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.[9] Independent satellite connections are prohibited.[10] This centralization has also contributed to connectivity problems, as the weak and overburdened infrastructure often results in slow speeds and periodic outages.

An ISP can begin operating after procuring a license from the Telecommunications Department and obtaining approval from the security services.[11] Opening a cybercafe has become very difficult, as owners must first obtain approval from the STE and pass security vetting by the Ministry of Interior. Moreover, owners are required to monitor visitors and record their activities. There are two main mobile phone providers in Syria—Syriatel (which is owned by Rami Makhlouf, a cousin of President Bashar al-Assad) and MTN (a subsidiary of the South African company MTN).

Since early 2011, the Syrian government has repeatedly used its centralized control over the internet infrastructure to obstruct connectivity, at times shutting down the internet and mobile phone networks entirely (either nationwide or at particularly sites of unrest). A nationwide shut down was imposed in June 2011 and lasted one day.[12] More localized, but longer lasting cut-offs were reported in Kurdish regions in September 2011, in Aleppo in November, in Daraa and parts of Damascus in December, and in Homs in January 2012.[13] According to activists, every time pro-regime forces begin to besiege a city, the broadband bandwidth is simultaneously reduced to a crawl and 3G services are shut off.[14] In other

[8] "STE is shifting into company in June" [in Arabic], Alwatan, June 12, 2012, http://www.alwatan.sy/dindex.php?idn=124296.
[9] 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.
[10] "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.
[11] Ayham Saleh, "Internet, Media and Future in Syria" [in Arabic], The Syrian Center for Media and Free Expression, November 14, 2006, http://alayham.com/%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA/%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA%D8%8C-%D8%A5%D8%B9%D9%84%D8%A7%D9%85-%D8%A7%D9%84%D9%85%D8%B3%D8%AA%D9%82%D8%A8%D9%84-%D9%8A%D9%88%D8%A1%D8%AF-%D9%81%D9%8A-%D8%B3%D9%88%D8%B1%D9%8A%D8%A7.
[12] Christopher Rhoads, "Syria's Internet Blockage Brings Risk of Backfire," Wall Street Journal, June 3, 2011, http://online.wsj.com/article/SB10001424052702304563104576363763722080144.html?mod=googlenews_wsj.
[13] "News From the Ground," [in Arabic], Telecomix: Syria, December 9, 2011, http://syria.telecomix.org/f689d2faa8c9a5ce29216c00152c8c7b
[14] Interviews with several activists in Syria wishing to remain anonymous, August 2011to March 2012.

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."[15] It was widely believed that such steps aimed at preventing citizen journalists from charging communication devices or transmitting updates to the outside world.[16]

The Syrian government regulates and controls the internet via the state-owned Syrian Telecommunication Establishment (STE), which owns all telecommunications infrastructure.[17] The STE is a government body established in 1975 as a part of the Ministry of Telecommunications and Technology.[18] In addition to its regulatory role, the STE also serves as an ISP.[19]

LIMITS ON CONTENT

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs, and such censorship has expanded in recent years. Tests conducted by the OpenNet Initiative (ONI) in 2008-2009 found pervasive blocking of websites related to opposition to the Assad regime, human rights groups, the Muslim Brotherhood, and activism on behalf of the Kurdish minority.[20] A range of websites related to regional politics were also found to be blocked, including several Lebanese newspapers and the websites of groups campaigning to end Syrian influence in Lebanon, as well as the prominent London-based Arabic newspapers *Al-Quds al-Arabi* and *Al-Sharq al-Awesat*. Access to the entire Israeli domain name ".il" was also restricted.

Internet censorship continued to worsen in 2011 and early 2012. Activists and average users consistently complained about the extensive and unprecedented blocking of circumvention tools, internet security software, and applications that enable anonymous communications. Websites used to mobilize people for protests or resistance against the regime, including

[15] "Leaked Syrian document shows how Assad banned internet access and satellite phones," The Telegraph, June 27, 2011. http://blogs.telegraph.co.uk/news/michaelweiss/100093908/leaked-syrian-document-shows-how-assad-banned-internet-access-and-satellite-phones/.
[16] "Syria - a country that can no longer communicate," Bambuser (blog), March, 1, 2012, http://blog.bambuser.com/2012/03/syria-country-that-cannot-longer.html.
[17] "Syria," OpenNet Initiative, August 7, 2009, http://opennet.net/research/profiles/syria.
[18] See the Ministry of Telecommunications and Technology's website (in Arabic) at: http://www.moct.gov.sy/moct/?q=ar/node/58.
[19] See STE's website at: http://www.in-ste.gov.sy/inindex_en.html.
[20] "Syria," OpenNet Initiative; Guy Taylor, "After the Damascus Spring: Syrians search for freedom online," Reason, February 2007, http://www.reason.com/news/show/118380.html.

those of the network of Local Coordination Committees (LCCs) that emerged as the uprising progressed, were blocked.[21] Online initiatives to gather information and raise public awareness, such as the Mondaseh website, were blocked as well.[22] 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."[23] 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, thinking they were to be given to the Iraqi government, but logs obtained by the activist hacking group Telecomix in August revealed evidence of their use in Syria instead. In October, 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.[24] Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.[25] The *Wall Street Journal* identified efforts to block or monitor tens of thousands of attempts to access 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.[26]

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 other mobile phone providers to block text messages containing key words like "revolution" or "demonstration." The providers reportedly implemented the directives with

[21] Email communication with activists in Syria, wishing to remain anonymous, December 2011. Local coordination committees of Syria: http://www.lccsyria.org/.
[22] Email communication with activists in Syria, wishing to remain anonymous, December 2011. The Mondaseh: http://the-syrian.com/.
[23] 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.
[24] Blue Coat, "Update on Blue Coat Devices in Syria," news statement, December 15, 2011, http://www.bluecoat.com/company/news/statement-syria.
[25] "Blue Coat device logs indicated the levels of censorship in Syria," Hellias.github.com, accessed August 14, 2012, http://hellais.github.com/syria-censorship/.
[26] 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.

the help of technology purchased from two Irish firms several years earlier for the alleged purpose of restricting spam.[27]

In an unexpected turn of events, the Syrian government lifted a four-year block on the social-networking site Facebook in February 2011, resulting in a doubling of the number of users within three months.[28] The video-sharing website YouTube was also unblocked, though it was not usable from mobile phone devices.[29] By March 2012, both were within the top-five most visited websites in the country.[30] Some activists suspected, however, that rather than a sign of openness, the regime's motive for unblocking the sites was to be able to more easily track citizens' online activities and identities. Other social media platforms like Twitter are freely available but Syrian users have a minimal presence on them.

Despite the renewed access to Facebook and YouTube, a range of Web 2.0 applications remain inaccessible in Syria, including the blog-hosting platform Blogger and the VoIP service Skype. The Arabic blog-hosting service Maktoob has also been sporadically blocked, but was available as of May 2012. 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. Among the 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 Ebuddy, Nimbuzz, and MiG-33 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 the 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 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

[27] 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.

[28] Jennifer Preston, "Seeking to Disrupt Protesters, Syria Cracks Down on Social Media," New York Times, May 22, 2011, http://www.nytimes.com/2011/05/23/world/middleeast/23facebook.html.

[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://blog.bambuser.com/2012/02/live-video-streaming-service-bambuser.html.

[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.

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 father, the military, or the ruling Baath party. Publicizing problems faced by religious and ethnic minorities or corruption allegations related to Rami Makhlouf, the president's cousin, 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] Those who do choose to use circumvention tools typically do so at cybercafes rather than at their home or workplace out of a belief that surveillance and tracking of their browsing is easier for authorities at the latter.[35]

For news websites and other online forums based in the country, it is common 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 official version of events. These sites typically cite the reporting of the official 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 their primary utility has been information sharing rather than planning street protests. The "Syrian Revolution 2011" Facebook page, which by June 2012 had over 500,000 members from both inside and outside the country, has been a vital source of information for dissidents.[38] What has especially stood out in the Syrian context has been citizen journalists' creative and courageous use of mobile phone devices and video-sharing websites to document both demonstrations and human rights abuses—including regime security forces firing on unarmed civilians—and disseminate them to the outside world after most foreign correspondents were forced to leave the country.[39] For example, by March 2012, activists and citizen journalists had posted over 40,000 video clips to YouTube, many of which were

[34] Email communication from a Syrian blogger. Name was hidden.
[35] "Syria," OpenNet Initiative.
[36] Guy Taylor, "After the Damascus Spring: Syrians search for freedom online."
[37] Ibid.
[38] "The Syrian Revolution 2011 Facebook Statistics," Socialbakers.com, accessed August 14, 2012, http://www.socialbakers.com/facebook-pages/420796315726-the-syrian-revolution-2011.
[39] "Iranians were creative in using Twitter, Egyptians preferred Facebook, and Syrians are the masters of You Tube," Interview with Dr. Radwan Ziadeh, Director of the Damascus Center for Human Rights Studies, Washington, D.C., February 2012.

subsequently rebroadcast by leading news outlets like Al-Jazeera, the CNN, and the BBC, reaching tens of millions of viewers.[40]

Responding to the growing circulation of such footage and first-hand accounts, pro-regime forces have employed a range of tactics to manipulate online content and discredit the reports or those posting them, though a direct link between those carrying out these activities and the government is not always evident. Most notable has been the emergence of the Syrian Electronic Army (SEA) since April 2011, a pro-government activist and hacking group operating with at least tacit regime approval.[41] Among the tactics used by the SEA is to spam popular Facebook pages—like those of U.S. President Barack Obama or French President Nicolas Sarkozy—with highly orchestrated pro-Assad comments.[42] In other instances, misinformation is the tactic of choice. For example, in early 2012, a fake Twitter account was launched in the name of British-Syrian activist Danny Abdel Dayem, whose reports on a massacre in Homs had drawn international attention. The fake account's tweets combined plausible criticism of the Assad regime with comments seeming to incite sectarian hatred or ask for Israeli intervention; once discovered, Twitter closed the account.[43]

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. Laws such as the penal code, the 1963 State of Emergency Law, and the 2001 Press Law are used to control traditional media and arrest journalists or internet users based on vaguely worded violations such as threatening "national unity" or "publishing false news that may weaken national sentiment."[44] Defamation can carry criminal penalties if comments target the president (punishable by up to one year in prison) or other government officials, including judges, the military, or civil servants (punishable by up to six months in prison).[45] The judiciary lacks independence and its decisions are often arbitrary. 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. The reasons for someone's arrest are often unclear and among those targeted have been

[40] Robert Mackey, "Syria's Losing Battle to Control the News," The Lede (blog), *New York Times*, March 13, 2012, http://thelede.blogs.nytimes.com/2012/03/13/syrias-losing-battle-to-control-the-news/.
[41] 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.
[42] "Assad's Shadow Army," Al Jazeera, September 7, 2011, http://www.stream.aljazeera.com/story/assads-shadow-army.
[43] Robert Mackey, "Syria's Losing Battle to Control the News."
[44] Articles 285, 286, 287 of the Syrian Penal Code.
[45] Article 378 of the Syrian Penal Code.

individuals not known for their political activism. 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. For example, veteran blogger Ahmad Abu al-Khair was taken into custody in February 2011 while traveling from Damascus to Banias. [46] He was released one week later, but arrested again the following month on charges of "inciting demonstrations." He was held in custody for 24 days without being brought before a judge. Shortly after his release, he went into hiding. Security forces subsequently detained his brother twice—the second time for 60 days—in an effort to pressure al-Khair to turn himself in; as of May 2012, he remained in hiding.[47] In July, prominent tech blogger Anas Maarawi was detained and held for 59 days until his release after an online campaign on his behalf.[48] In February 2012, civil rights blogger Razan Ghazzawi and Mazen Darwich, the head of the Syrian Center for Media and Freedom of Expression, along with 12 others were arrested in a raid on the organization.[49] Gazzawi and six other female detainees were released after several days though they continue to face charges.[50] Darwich was still under incommunicado detention as of May 2012.[51]

Very few detainees have been brought before a judge. However, in a high-profile decision in February 2011, the Damascus State Security Court convicted 19-year-old student and blogger Tal al-Mallouhi to five years in prison for allegedly "divulging information to a foreign state," a charge she denied and for which no evidence was presented; al-Mallhouhi was not known to be politically active, but had posted poetry and commentary on political and social issues to her blog.[52]

Once in custody, citizen journalists, bloggers, and other detainees reportedly suffered severe torture. Though the precise number is unknown, it is estimated that dozens of individuals have been tortured to death after being caught filming protests or abuses and

[46] 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/.
[47] Email communication with activist in Syria who wished to remain anonymous, April 2012.
[48] "Syria: Bloggers Rally for Anas Maarawi," Censorship in America, July 10, 2011, http://censorshipinamerica.com/2011/07/10/syria-bloggers-rally-for-anas-maarawi/; "Anas Maarawi is Free! Thank you all for your support!" Freeanas.pen.io, accessed August 14, 2012, http://freeanas.pen.io/.
[49] "Syria arrests iconic blogger Razan Ghazzawi and leading activists," The Telegraph, February 16, 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9086741/Syria-arrests-iconic-blogger-Razan-Ghazzawi-and-leading-activists.html.
[50] Email communication from Razan Gazzawi. See also: Syrian Blogger Razan Gazzawi denies the charges against him and confirm that his activity is 'guaranteed by the Syrian Constitution" [in Arabic], Asharq Al-Awsat, accessed June 15, 2012, http://www.aawsat.com/details.asp?section=4&article=654226&issueno=12069.
[51] "Syrian activist Razan Ghazzawi is freed by authorities for a second time," Al Arabiya News, February 20, 2012, http://english.alarabiya.net/articles/2012/02/20/195939.html.
[52] "Syria: Tal Al-Mallouhi," PEN, accessed August 14, 2012, http://www.pen.org/viewmedia.php/prmMID/5499/prmID/174.

then uploading them to YouTube.[53] In one high-profile case from November 2011, freelance journalist and photographer Ferzat Jarban from Homs was arrested and killed by security forces after filming a demonstration in al-Qasir; his body was mutilated and his eyes gouged out.[54] In some cases, the Syrian army appeared to deliberately target online activists and photographers in Homs, using the signal from their satellite phones to track their location. During the bombardment of Bab Amr in Homs in February 2012, government forces fired on a team of photographers who were live-streaming the assault using a satellite internet connection. Rami al-Sayed, who had run the live stream and previously uploaded over 800 videos to YouTube, was injured during the shelling and died several hours later.[55] 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.[56]

Anonymous communication is possible but increasingly restricted. Registration is required upon purchasing a cell phone, though over the past year, activists have begun using the SIM cards of friends killed in clashes with security forces in order to shield their identities. Meanwhile, activists and bloggers released from custody reported being systematically asked or forced by security agents to provide the passwords for their Facebook, Gmail, Skype, and other online accounts.[57]

A new "Law for the Regulation of Network Communication against Cyber Crime" was passed in February 2012 and 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 100,000 and 500,000 SYP (US$1,700 to US$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 and a fine of 200,000 to 1 million SYP (US$3,400

[53] Interview via Skype with A.A, Human Rights Lawyer in Damascus, December 12, 2011. Name is hidden.
[54] "Ferzat Jarban," Committee to Protect Journalists, November 19 or 20, 2011, http://cpj.org/killed/2011/ferzat-jarban.php.
[55] Ahmed Al Omran, "Rami Al-Sayed, Syrian Citizen Journalist, Is Killed During Attack On Homs," The Two-Way (blog), NPR, February 21, 2012, http://www.npr.org/blogs/thetwo-way/2012/02/21/147224200/rami-al-sayed-syrian-citizen-journalist-is-killed-in-attack-on-homs.
[56] Interviews with two photographers who have taken refuge in Turkey, December 2011.
[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.

to US$17,000).[60] As of May 2012, 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 the Syrian government had contracted Area SpA, an Italian surveillance company, in 2009 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 begun setting up the system that, when complete, would include flat-screen workstations displaying user communications in near real-time alongside graphics mapping users' contacts.[61] The exposé sparked protests in Italy and, at the end of November, Area SpA announced that it would not be completing the project.[62] As of May 2012, it remained unclear what the project's status was or whether any of the equipment was 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 and their account information. Though it was impossible to trace the attacks back to the Syrian government, it was widely believed that the regime or those linked to it were behind them. 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 and more. Both sent the data back to the same IP address in Syria and were circulated via email and instant message programs.[63] A few weeks 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]

[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.

[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, https://www.eff.org/deeplinks/2012/03/how-find-syrian-government-malware-your-computer-and-remove-it.

[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.

Though present previously, cyberattacks have become increasingly common in Syria since February 2011, with many carried out by the Syrian Electronic Army (SEA). 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] Among other means of communication, the SEA has itself used Facebook to share information, coordinate attacks, and publicize their results. It has opened several Facebook pages, where it repeatedly issued calls to hack the emails of activists and to provide the obtained information to the security apparatus; most pages used to post such calls have subsequently been closed by Facebook for violating its terms of use. In other instances, the SEA has endangered anti-government activists by making public their phone numbers and addresses.[70] In April 2012, the personal email and Facebook accounts of Burhan Ghalioun, then-President of the opposition Syrian National Council were hacked. Two weeks later, his personal email communications began being published in the pro-Syrian Lebanese newspaper *al-Akhbar* in an effort termed "Ghalioun leaks."[71]

Activist-hacker groups in Syria and elsewhere have responded by hacking and defacing government websites. In August and September 2011, Anonymous and RevoluSec hacked at least 12 Syrian government websites replacing their content with interactive maps and statements detailing violence by security forces against peaceful protesters.[72] In another

[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."
[70] 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.
[71] "Pipe Lex," Al-Akhbar, accessed June 14, 2012, http://al-akhbar.com/taxonomy/term/3858.
[72] Zeina Karam, "Syrian Electronic Army: Cyber Warfare From Pro-Assad Hackers"; Amir Ahmed, "Apparently hacked, Syrian government website condemns president," CNN, August 8, 2011, http://articles.cnn.com/2011-08-08/world/syria.ministry.site.hacked_1_bashar-al-assad-syrian-people-syrian-flag?_s=PM:WORLD.

reaction, in November 2011, three members of the SEA were added to the European Union's list of individuals subject to financial sanctions.[73]

[73] "Consolidated List of Financial Sanctions Targets in the UK," Department of Treasury of UK, July 24, 2012, http://www.hm-treasury.gov.uk/d/syria.htm.