Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**654**
Land:	Syrien
Kilde:	Freedom House
Titel:	Freedom on the Net 2016 – Syria
Udgivet:	november 2016
Optaget på baggrundsmaterialet:	16. januar 2017

EN | DE

- **Source:**
  Freedom House
- **Title:**
  Freedom on the Net 2016 - Syria
- **Publication date:**
  November 2016
- **ecoi.net summary:** Report on digital media and internet freedom (covering June 2015 - May 2016) [ID 332102]
- **Countries:**
  Syrian Arab Republic
- Original link https://freedomhouse.org/print/48931

Recommended citation:
Freedom House: Freedom on the Net 2016 - Syria, November 2016 (available at ecoi.net)
http://www.ecoi.net/local_link/332102/460047_en.html (accessed 06 January 2017)

Freedom on the Net 2016 - Syria

Country:
Syria
Year:
2016
Status:
Not Free
Total Score:
87
(0 = Best, 100 = Worst)
Obstacles to Access:
24
(0 = Best, 25 = Worst)
Limits on Content:
26
(0 = Best, 35 = Worst)
Violations of User Rights:
37
(0 = Best, 40 = Worst)
Population:
18.5 million
Internet Penetration:
30 percent
Social Media/ICT Apps Blocked:
No
Political/Social Content Blocked:
Yes
Bloggers/ICT Users Arrested:
Yes
Press Freedom Status:
Not Free
Key Developments:

June 2015–May 2016

- The so-called Islamic State (IS) issued strict regulations on the provision of internet access at cybercafes, requiring business to obtain licenses for setting up operations in Raqqa and Deir al-Zor (see **Availability and Ease of Access**).
- The internet was reportedly restored to parts of Aleppo, which had been shut off from access for seven months due to damage to telecommunications infrastructure. Authorities continue to shut down internet access in preparation for military offensives (See **Restrictions on Connectivity**).
- At least 17 netizens and citizen journalists remain imprisoned by the regime on charges related to their digital activism. It was confirmed in September 2015 that cartoonist Akram Raslan died while in state custody, likely as a result of torture (see **Prosecutions and Detentions for Online Activities**).
- Several activists and bloggers were murdered by IS militants both in IS-controlled territory and neighboring Turkey, including two members of Raqqa is Being Slaughtered Silently and a female blogger who wrote about daily life in Raqqa (see **Intimidation and Violence**).
- Russia stepped up cyberattacks against Syrian human rights organizations and opposition groups in a bid to disrupt reporting on human rights violations and obtain intelligence (see **Technical Attacks**).

Introduction:

Syria remained one of the most repressive and dangerous environments for users in 2015-16, marked by the first execution of a female blogger by extremists and the arbitrary detention of tech activists by the regime.

Syrian cyberspace remains fraught with conflict, often mirroring the brutality of the war on the ground and its complex geopolitics. Citizen journalists were killed during air raids, regime opponents were tortured in state prisons, and the so-called Islamic State (IS) murdered individuals for chronicling the hardships of life under the religious extremists. Pro-regime hackers in the Syrian Electronic Army conducted spear-phishing other cyberattacks, joined by Russian hackers who have increasingly targeted human rights organizations and opposition groups.

Syria's telecommunications infrastructure is highly decentralized. In areas controlled by the regime, the state-owned service provider employs sophisticated technologies to filter political, social, and religious websites. Meanwhile, individuals in rebel-controlled areas often rely on Turkish mobile internet beamed in from across the border, or in many cases, expensive satellite connections. Authorities regularly shut down internet access to prevent the dissemination of information, particularly before and during military operations. Shelling and sabotage have led to heavy damage to infrastructure, affecting internet and power connections in several provinces.

The internet has played a significant role in documenting popular protests against the Syrian regime and its heavy-handed response against civilians. Authorities prevented foreign media from accessing the country, prompting many ordinary Syrians to take up mobile phones and small cameras to cover the deteriorating situation and post videos of the conflict on social media. These citizen journalists have become vital in the quest to document flagrant human rights abuses by all parties to the conflict.

Obstacles to Access:

The war has devastated telecommunications infrastructure and disconnected around two-thirds of the country from Syrian internet service providers (ISPs). As a result, internet access has become highly decentralized with some relying on microwave links from Turkish cities or pooled satellite connections serving cybercafes. Internet access is regularly shutdown in areas controlled by the regime and disparate rebel groups alike.

Availability and Ease of Access

Syria's telecommunications infrastructure is one of the least developed in the Middle East, with broadband connections among the most difficult and expensive to acquire.[1] This worsened after 2011, as inflation and electricity outages increased dramatically following public protests and the government's corresponding crackdown. Damage to the communications infrastructure is particularly bad in cities where the government is no longer in control, due to shelling by both the Syrian armed forces and opposition fighters. This has led to a decentralized telecommunications infrastructure, whereby each and every part of the country has a different internet gateway.

According to estimates by the International Telecommunication Union, some 30 percent of Syrians had access to the internet at the end of 2015, up from 21 percent in 2010.[2] The estimated number of fixed broadband subscribers also increased, but remained low at just over 3 subscriptions per 100 inhabitants. The number of mobile phone subscriptions decreased slightly over the past year, with 62 subscriptions per 100 inhabitants.

The price, speed, and availability of internet access vary depending on the region of the country. According to a pricelist published by the Syrian Computer Society Network, the monthly cost for a 1 Mbps ADSL connection was SYP 1950 (approximately US$6) as of March 2016,[3] in a country where monthly gross domestic product per capita was US$274[4] in 2012 and has since dropped.[5] While the Syrian lira (SYP) has lost a large amount of its value, prices have not changed dramatically during the conflict.

Around two-thirds of the country is disconnected from Syrian ISP networks, instead relying on a WiMax or WiFi microwave links from Turkish cities[6] or satellite connections (VSAT).[7] The former is particularly prominent in Kurdish areas along the Turkish border, such as Qamishli, where Wi-Fi connections are around US$50 per month. Prices are reportedly lower in the city than last year, with cybercafes reportedly available in every neighborhood.[8]

In areas controlled by the so-called Islamic State (IS), such as Deir al-Zor and Raqqa, internet access is subject to many regulations and often depend on military developments on the ground. For example, IS authorities reportedly banned the internet from the village of al-Boukamal in the province of Deir al-Zor in September 2015 in preparation for a military operation against regime forces in a nearby village.[9] Due to the prohibitive cost of VSAT connections, businesses in IS-controlled areas have established cybercafes where users split the cost of satellite infrastructure and purchase separate Wi-Fi connectivity. Based on Skype interviews with Syrians living under IS-controlled areas, the cost of Internet access inside the Internet cafes is 100 SYP (US$ 0.50) for 1 hour connection, while for smartphone users, 15 MB of data transactions costs 100 SYP.

In mid-2015, IS released a statement requiring these cybercafes to “remove Wi-Fi boosters in internet cafes as well as private wireless adapters, even for soldiers of the Islamic State.”[10] The move is an attempt to limit private internet access in Raqqa and Deir al-Zor to public locations[11] that can be policed by the extremists in order to restrict reporting by activists as well as GPS-tracking of militants using the services.[12] Licenses are only provided to “loyal” businesses and require cafe owners to restrict WiFi availability to the physical space of the cybercafé, to log all customers using their IDs, and to separate men from women.[13] IS has allowed only four cybercafes in Deir al-Zor city (one each in the neighborhoods of Hamidiyeh, al-Ommal, Ghassan Aboud, and al-Sheikh Yassin) and all are under heavy surveillance by authorities.[14] Recent airstrikes targeting IS militants have also damaged telecommunications infrastructure in IS-held areas.[15]

Restrictions on Connectivity

The Syrian government has engaged in extensive and repeated internet shutdowns since 2011. Damage to telecommunications infrastructure disconnected the war-torn city of Aleppo from March to November 2015.[16] In a change from pre-March, internet connections to Aleppo were being routed through Syrian networks, rather than Turkish networks. Researchers speculated the move reflected recent gains made by the Syrian government army over rebel forces in the areas surrounding Aleppo, once Syria’s most populous city. Researchers noted the city was reconnected using a “high capacity microwave link to the coastal city of Latakia, Syria.”[17]

In areas controlled by the Syrian government, the Syrian Telecommunications Establishment (STE) serves as both an internet service provider (ISP) and the telecommunications regulator, providing the government with tight control over internet infrastructure.[18] In addition, private fixed-line and mobile ISPs are required to sign a memorandum of understanding to connect to the international internet via gateways controlled by the Syrian Information Organization (SIO).[19]

ICT Market

As of 2012, some 14 ISPs operated in Syria. Independent VSAT connections are prohibited, although in reality they are heavily employed due to the damage that government ICT infrastructure has sustained as a result of the conflict.[20] ISPs and cybercafes must obtain approval from the STE and pass security vetting by the Ministry of Interior and other security services.[21] 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.

Regulatory Bodies

Syria’s ICT market and internet policy is regulated by the SIO and the state-owned 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.[22] Domain name registration is handled by the Syrian Computer Society, which was once headed by Bashar al-Assad prior to his appointment as president in 2000.[23]

Limits on Content:

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. Self-censorship is highly prevalent, particularly in areas under government control. Despite these limitations, activists make use of communication apps to save lives in rebel-controlled areas and 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.

Blocking and Filtering

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

The Syrian government also engages in filtering SMS messages. Beginning in February 2011, such censorship was periodically reported around dates of planned protests. In February 2012, Bloomberg reported in a series of interviews and leaked documents 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.[30]

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.[31] Websites used to mobilize people to protest or resist the regime, including pages linked to the network of Local Coordination Committees (LCCs)—groups that have formed since the revolution to organize the opposition—continue to be blocked.[32] Websites that document human rights violations, such as the Violations Documentation Center, remain blocked,[33] as does the Mondaseh website, an online initiative to gather information and raise public awareness.[34] Authorities have repeatedly blocked the website and key search terms of *SouriaLi,* an internet radio station started by a group of pluralistic young Syrians.[35]

Facebook remains 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. Some activists suspected that the regime unblocked the sites to track citizens' online activities and identities. As of 2016, both were within the top-three most visited websites in the country.[36] Other social media platforms like Twitter are freely available, although they are not as popular and do not figure within the top 25 most visited sites in the country.

The Voice-over-Internet-Protocol (VoIP) service Skype often has suffered 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. Anti-virus software and updates to operating systems remain blocked due to U.S. sanctions, to the dismay of many U.S.-based activists.[37]

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.

Content Removal

According to digital security organization SecDev, dozens of opposition pages, media centers, and independent NGOs have been closed by Facebook.[38] These include numerous pages of local coordination committees (LCCs) and the London-based Syrian Network for Human Rights. Activists believe that Facebook users sympathetic to President Assad may be reporting the pages en masse as violating user guidelines, thereby provoking Facebook into action. 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.

Media, Diversity, and Content Manipulation

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.[39] 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.[40] In 2014, users living in areas under control of IS or other extremist groups have stepped up their self-censorship in order to avoid criticizing the militants or Islam in general.

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 "Technical Attacks"). 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.[41] 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. Since early 2011, this approach has also been used to promote the government's perspective about the uprising and subsequent military campaign.[42]Interestingly, in 2012, the progovernment website Aksalser changed its stance to support the opposition and was subsequently blocked by the government.[43]

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

Digital Activism

Online tools have proven crucial for Syrians inside and outside the country seeking to document human rights abuses, campaign for the release of imprisoned activists, and disseminate news from the front lines of the conflict. Communication apps have become particularly important in saving lives during the conflict. A WhatsApp group called "The Monitors" was created by individuals based in regime-controlled areas to warn individuals living in rebel-controlled areas of impending Syrian and Russian air raids.[44] The U.S.-based Syrian American Medical Society has used WhatsApp for telemedicine, in one instance guiding a veterinarian who delivered twin babies by caesarean section in the besieged town of Madaya.[45]

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 the conflict in 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 and missiles against opposition fighters, the role of citizen journalists has shifted from live event coverage to documenting the bloody aftermath of an attack. Although many obstacles stand in the way of media coverage, citizen journalists have designed techniques to ensure media coverage of remote and conflict areas. “Local Media Offices” ensure that local journalists cover limited geographic areas, and then use a social network as a platform to collect, verify, and publish news stories. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, rebel groups, and civil society groups, mostly documenting attacks. A Syrian group categorizing YouTube videos and sharing them via the platform OnSyria had posted almost 200,000 videos in 2013.[51]

Violations of User Rights:

Syria remains one of the most dangerous places to use the internet in the world. Citizen journalists, bloggers, and activists are detained and often tortured by both government forces and, increasingly, fighters linked to extremist groups like the so-called Islamic State (IS). Several netizens were killed during the coverage period, including a female blogger who wrote of daily life in the IS stronghold of Raqqa.

Legal Environment

Laws such as the penal code, the 1963 State of Emergency Law, and the 2001 Press Law are used to control traditional media and arrest journalists or internet users based on vaguely worded terms such as threatening “national unity” or “publishing false news that may weaken national sentiment.”[52] 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.[53] 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 computer networks.[54] The judiciary lacks independence and its decisions are often arbitrary. Some civilians have been tried before military courts.

Prosecutions and Detentions for Online Activities

Since antigovernment protests broke out in February 2011, the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. While it is very difficult to obtain information on recent arrests, 17 netizens remain in prison according to Reporters Without Borders. [55] 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 remains 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 Darwish, was reportedly released in August 2015 after three years in pretrial detention and recently moved to Germany.[64]

Surveillance, Privacy, and Anonymity

Surveillance is rampant on Syrian internet service providers, which are tightly aligned with security forces. Meanwhile, in IS-controlled territory, there are reports that militants have conducted unannounced raids at cybercafes in which they force users to leave their machines, going through their open web browsing sessions and social media accounts to ensure users are not viewing or writing impermissible content.[65]

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.[66] 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.[67] Failure to comply may cause the website to be blocked and is punishable by a fine of SYP 100,000 to 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).[68] In early 2014, however, the authorities were not vigorously enforcing these regulations.

In early November 2011, Bloomberg reported that the Syrian government had contracted Area SpA 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 began setting up the system to monitor user communications in near real-time, alongside graphics mapping users' contacts.[69] The exposé sparked protests in Italy and, a few weeks after the revelations, Area SpA announced that it would not be completing the project.[70] 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.[71] 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.[72] 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 its discovery, the fake site was taken down.[73] 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.[74]

A report from Kaspersky Labs, published in August 2014, revealed that some 10,000 victims' computers had been infected with RATs in Syria, as well as in other Middle Eastern countries and the United States. [75] 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.

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.[76]

Intimidation and Violence

Once in custody, citizen journalists, bloggers, and other detainees reportedly suffered severe torture at the hands 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.[77] In September 2015, it was confirmed that *al-Fida* newspaper's cartoonist Akram Raslan had died in state custody in 2013 due to sharing antigovernment cartoons on Arabic news sites and social media.[78] He had been arrested in October 2012 and it is believed he was tortured to death.[79]

According to Reporters Without Borders, seven "netizens" were killed during the coverage period, mostly for work as citizen journalists. Separately, in a video recording published by IS on June 26, 2016, five journalists—many of them whose work was primarily online—were brutally murdered. In at least two cases, IS militants had rigged the individuals' computers or cameras with explosives.[80] Citizen journalists have also been targeted by IS militants while in Turkey. Ibrahim Adul Kader of the human rights organization Raqqa is Being Slaughtered Silently (RBSS) was killed by IS militants in the city of Urfa, Turkey along with his friend Fares Hammadi in October 2015.[81] Naji Jaraf, editor-in-chief- of the opposition Hentah Magazine and an activist with RBSS, was shot and killed in the Turkish city of Gaziantep in December 2015.[82] Hundreds of activists have gone into hiding or fled the country, fearing that arrest may not only mean prison, but also death under torture.[83] Blogger Assad Hanna left Syria following online threats stemming from his criticism of the regime, but was badly injured by knife-wielding assailants at his apartment in Turkey in April 2015.[84]

In a move some observers called unprecedented, IS executed a female journalist in September 2015. Ruqia Hassan, also known as Nissan Ibrahim, was blogging about daily life in the city of Raqqa.[85] She was accused of being a spy for the Free Syrian Army. Shortly before her death, she reportedly complained of death threats stemming from IS. International journalists, including those whose work is mainly featured online, have also been killed by Syrian militant groups in previous years.[86]

Technical Attacks

Numerous reports from the past year have detailed the spillover of the country's conflict to the online sphere. According to the cybersecurity group FireEye, Russia's intelligence agency, the FSB, has stepped up technical attacks against Syrian human rights organizations and opposition groups in a major campaign to glean intelligence and disrupt reporting on Russian human rights violations.[87] In December 2014, the University of Toronto's Citizen Lab released a report entitled, "Malware Attack Targeting Syrian ISIS Critics," focusing on groups such as Raqqa is Being Slaughtered Silently (RSS), which documents human rights abuses committed by IS. Citizen Lab believes the malware was developed by IS or pro-IS hackers in order to discover more information about the nonviolent group.[88]

The Syrian Electronic Army (SEA) continues to target Syrian opposition websites and Facebook accounts, as well as Western or other news websites perceived as hostile to the regime. In March 2016, the FBI added three SEA members to its "Cyber Most Wanted" list.[89] The SEA made headlines after hacking major Western media outlets and organizations, including the websites of the *New York Times*,[90] the U.S. Marines,[91] Facebook,[92] 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 (OFA), was briefly hacked by the SEA, resulting in the account posting shortened links to SEA sites.[93] 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.[94] These tactics continued with the high-profile hacking of *Forbes* in February 2014[95] and the *Washington Post* in May 2015.[96]

Though the hacktivist 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;[97] a June 2011 speech in which the president explicitly praised the SEA and its members;[98] and positive coverage of the group's actions in state-run media.[99]

Notes:

[1] Kyle Wansink, *Syria - Telecoms, Mobile, Broadband and Forecasts*, BuddeComm, accessed March 8, 2012, http://bit.ly/1OdycSD.

[2] International Telecommunication Union, "Statistics," 2015, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[3] Syrian Computer Society Network, "ADSL Services and price" [in Arabic], accessed March 3, 2016, http://bit.ly/250BUqt.

[4] World Bank Databank, "GDP per capita (current US$)," 2008-12, accessed March 12, 2014, http://bit.ly/1eRbn2E.

[5] Democratic Arabic Center, "Reports: Syrian conflict losses of $ 80 billion and 11 percent of the population were killed or injured," [Arabic] February 11, 2016, http://democraticac.de/?p=27360.

[6] "Northern Syria, Internet cafes are everywhere in the North, Chatting, Smoking and Porn," [in Arabic], *Hunasaotak*, http://bit.ly/1Q4ieIU.

[7] "Internet through satellite and Turkish providers as an alternative of Al-Assad network in the countryside of Idlib," [in Arabic] *Orient News*, August 10, 2014, http://bit.ly/1PEllt8.

[8] Interview with the Amjad Othman, journalist from Qamishli city via Skype.

[9] Zainah Alsamman, "ISIS Bans the Internet in al-Boukamal, Deir Ezzor," SecDev Foundation, September 25, 2015, https://secdev-foundation.org/isis-bans-the-internet-in-al-boukamal-deir-ezzor/.

[10] Erika Solomon, "Isis to cut private internet access in parts of Syria," *Financial Times*, July 20, 2015, http://on.ft.com/1M4z2ff.

[11] ISIS is allowing the Internet but under surveillance, (Arabic), Alrai media, May 22nd , 2016 http://www.alraimedia.com/ar/article/others/2015/05/22/591978/nr/iraq

[12] “ISIL is shutting down Internet Cafes around Deir ez-Zor Airport,” [in Arabic] *Al-Arabiya*, December 8, 2014, http://ara.tv/mhf43.

[13] “The Islamic state to prevent Internet in Abu Kamal,” (Arabic), The Syrian Observatory for Human Rights, September 19, 2015, http://www.syriahr.com/?p=136555.

[14] Skype Call with Samer Al-Deri.

[15] Firas Alhakar “Hello.. Al-Raqa is offline,” *Al-Akbar*, July 24, 2015, https://al-akhbar.com/node/238429.

[16] Doug Madory, “Internet Returns to Aleppo, Syria,” Dyn Research, November 11, 2015, http://research.dyn.com/2015/11/internet-returns-to-aleppo-syria/.

[17] Doug Madory, “War-torn Syrian city gets new fiber link,” Dyn Research, October 12, 2016, http://research.dyn.com/2016/10/war-torn-syrian-city-gets-new-fiber-link/.

[18] Syrian Telecom, “Intelligent Network Project,” http://www.in-ste.gov.sy/inindex_en.html.

[19] Jaber Baker, “Internet in Syria: experimental goods and a field of a new control,” White and Black Magazine, posted on Marmarita website, August 10, 2008, http://www.dai3tna.com/nuke/modules.php?name=News&file=article&sid=6019. (no longer available)

[20] “Online Syria, Offline Syrians,” *One Social Network with a Rebellious Message,* The Initiative or an Open Arab Internet, accessed March 8, 2012, http://bit.ly/1NSCAHQ.

[21] 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.

[22] Ministry of Communication and Technology, “Overview,” [in Arabic], http://www.moct.gov.sy/moct/?q=ar/node/21.

[23] Sean Gallagher, “Network Solutions seizes over 700 domains registered to Syrians,” Ars Technica, May 8, 2013, http://arstechnica.com/tech-policy/2013/05/network-solutions-seized-over-700-domains-registered-to-syrians/.

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

[25] Reporters Without Borders, “Syria,” *Enemies of the Internet: Countries under surveillance*, March 12, 2010, http://bit.ly/1OCZ0cS.

Platinum, Inc., “ThunderCache Overview,” accessed August 14, 2012, http://www.platinum.sy/index.php?m=91.

[26] Andy Greenberg, “Meet Telecomix, The Hackers Bent on Exposing Those Who Censor and Surveil The Internet,” *Forbes*, December 26, 2011, http://onforb.es/1Bu1tQx.

[27] Blue Coat, “Update on Blue Coat Devices in Syria,” news release, December 15, 2011, http://bit.ly/1FzFd8X.

[28] “Blue Coat device logs indicate the levels of censorship in Syria,” *Arturo Filasto*, accessed August 14, 2012, http://bit.ly/1LZDZJ3.

[29] Jennifer Valentino-Devries, Paul Sonne, and Nour Malas, “U.S. Firm Acknowledges Syria Uses Its Gear to Block Web,” *Wall Street Journal*, October 29, 2011, http://on.wsj.com/t6YI3W.

[30] Ben Elgin and Vernon Silver, “Syria Disrupts Text Messages of Protesters With Dublin-Made Equipment,” *BloombergBusiness*, February 14, 2012, http://bloom.bg/1i0TOEU.

[31] Dlshad Othman, “Bypassing censorship by using obfsproxy and openVPN, SSH Tunnel,” *Dlshad,* June 22, 2013, http://bit.ly/1KH3KjZ.

[32] Local Coordination Committees, “Home,”: http://www.lccsyria.org/en/.

[33] “Leaked list of all blocked websites in Syria,” Arab Crunch, May 19, 2013, http://bit.ly/1KGFPBm.

[34]“Home,” *the-syrian,* http://english.the-syrian.com/.

[35] Syria Untold, “Syrian Creativity: Radio SouriaLi Broadcasts over the Internet,” *Global Voices*, June 7, 2013, http://bit.ly/1EQl2ZS.

[36] Alexa, “Top Sites in SY,” accessed October 25, 2016, http://www.alexa.com/topsites/countries/SY.

[37] Mike Rispoli, “Access joins open letter to tech industry addressing overcompliance with U.S. sanctions,” Access, June 28, 2012, http://bit.ly/1i0XdDM.

[38] Michael Pizzi, “The Syrian Opposition Is Disappearing From Facebook,” *The Atlantic*, February 4, 2014, http://theatln.tc/1aojZAO.

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

[40] Interview with a Syrian activist, November 2012, Damascus, November 2012.

[41] Guy Taylor, “After the Damascus Spring: Syrians search for freedom online,” *Reason,* February 2007, http://theatln.tc/1aojZAO.

[42] Guy Taylor, “After the Damascus Spring: Syrians search for freedom online,” *Reason,* February 2007, http://theatln.tc/1aojZAO.

[43] The Syrian “Aksalser website with the revolution,“ [in Arabic] *the-syrian*, August 28, 2012, http://the-syrian.com/archives/86170.

[44] Maya Gebeily, “Secret Syria network warns of air raids over WhatsApp,” *The Times of Israel*, January 21, 2016, http://www.timesofisrael.com/secret-syria-network-warns-of-air-raids-over-whatsapp/.

[45] Avi Asher-Schapiro, “The Virtual Surgeons of Syria,” *The Atlantic*, August 24, 2016, http://www.theatlantic.com/international/archive/2016/08/syria-madaya-doctors-whatsapp-facebook-surgery-assad/496958/.

[46] Judith Dublin, “Syrian Fight Fire with Facebook,” *Vocativ*, September 23, 2013, http://voc.tv/1UJqcIP.

[47] Clara Olshansky, “The Web Petitions to Free Syrian Artist Youssef Abdelke,” *Artfcity*, August 1, 2013, http://bit.ly/1VQezSS.

[48] “Déclaration pour Syrie democratique” [Declaration for a Democratic Syria], *Babelmed*, accessed March 14, 2014, http://bit.ly/1izKKHU.

[49] Khalil Sweileh and Omar al-Sheikh,“Syria: Youssef Abdelke Free, Resolved to Stay in Damascus,” *Al-Akhbar,* August 23, 2013, http://bit.ly/1XQaLmi.

[50] Christophe Koettl, “The YouTube War: Citizen Videos Revolutionize Human Rights Monitoring in Syria,” *Mediashift* (blog), *PBS,* February 18, 2014, http://bit.ly/1Nkfnw9.

[51] The platform, http://onsyria.org/, is now offline and the related Facebook page has not been updated since 2013: Onsyria, Facebook Page, http://on.fb.me/1GnVymR.

[52] Syrian Penal Code, art. 285, 286, 287.

[53] Syrian Penal Code, art. 378.

[54] Global Resource and Information Directory, “Legislation,” in “Syria*,”* http://www.fosigrid.org/middle-east/syria.

[55] Reporters Without Borders, “Netizens Imprisoned,” 2016, https://rsf.org/en/barometer?year=2016&type_id=237#list-barometre.

[56] Anas Qtiesh, “Syrian Blogger Ahmad Abu al-Khair Arrested This Morning,” *Global Voice Advocacy*, February 20, 2011, http://bit.ly/1vxJk5g.

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

[58] “Renewed calls for Bassel Khartabil’s release on 4th anniversary of detention,” Reporters Without Borders, March 17, 2016, https://rsf.org/en/news/renewed-calls-bassel-khartabils-release-4th-anniversary-detention.

[59] Hania Mourtada, "'She Was My Mandela' – Famous Syrian Activist Gets Abducted," *Time*, December 11, 2013, http://ti.me/1KcXrTc.

[60] Maha Assabalani, "My colleagues are in prison for fighting for free expression," UNCUT - Index on Censorship, May 11, 2012, http://bit.ly/1EYHMX9.

[61] Jared Malsin, "Portrait of an Activist: Razan Ghazzawi, the Syrian Blogger Turned Exile," *Time*, April 2, 2013, http://ti.me/1Q46vKi.

[62] An interview with Syrian blogger, February 2013, Skype.

[63] Sara Yasin,"Syrian free speech advocates face terror charges," Index on Censorship, May 17, 2013, http://bit.ly/1VQg2IL.

[64] Prominent Syrian activist Mazen Darwish freed" SKeyes, August 10, 2015, http://bit.ly/1GgvGK5.

[65] Interview with Abu Ibrahim Raqqawi of Raqqa Is Being Slaughtered Silently, Skype.

[66] "Law of the rulers to communicate on the network and the fight against cyber crime" art. 5-12. Informal English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.

[67] "Law of the rulers to communicate on the network and the fight against cyber crime" art. art. 2.

[68] "Law of the rulers to communicate on the network and the fight against cyber crime" art. art. 8.

[69] Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," *Bloomberg Business*, November 3, 2011, http://bloom.bg/1VQij6R.

[70] Vernon Silver, "Italian Firm Said Exits Syrian Monitoring Project, Repubblica Says," *Bloomberg Business*, November 28, 2011, http://bloom.bg/1igDnoL.

[71] Ben Brumfield, "Computer spyware is newest weapon in Syrian conflict," CNN, February 17, 2012, http://cnn.it/1LZPQXn.

[72] 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.

[73] Eva Galperin and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, http://bit.ly/1XQhHzX.

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

[75] Kaspersky Lab Global Research and Analysis Team, *Syrian Malware, the evolving threat*, August 2014, http://bit.ly/1pCJ0gK.

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

[77] Interview A.A, Human Rights Lawyer, December 12, 2011, Damascus, Skype.

[78] "Well-known Syrian cartoonist died in detention after being tortured," *Reporters Without Borders*, September 22, 2015, https://rsf.org/en/news/well-known-syrian-cartoonist-died-detention-after-being-tortured.

[79] Ibrahim Naffee, "Cartoonist Raslan arrested in Syria," *Arab News*, October 16, 2012, http://www.arabnews.com/cartoonist-raslan-arrested-syria.

[80] Enab Baladi Online, "ISIS Executes Five Journalists in Deir-ez-Zor," The Syrian Observer, June 27, 2016, http://syrianobserver.com/EN/News/31250/ISIS_Executes_Five_Journalists_Deir_Zor.

[81] Lizzie Dearden, "Isis beheads 'Raqqa is Being Slaughtered Silently' activist and friend in Turkey," *Independent*, October 30, 2015, http://ind.pn/1Wm9dAh.

[82] AP, "Reporters Without Borders urges Turkey to protect exiled Syrian journalists," US News and World Report, December 29, 2015, http://www.usnews.com/news/world/articles/2015-12-29/journalism-group-calls-on-turkey-to-protect-syrian-reporters.

83 Interviews with two photographers who have taken refuge in Turkey, December 2011.

84 Amira al Hussaini, “Syrian Blogger Stabbed in His Istanbul Home After Receiving Threats Online,” *Global Voices Advocacy*, April 21, 2015, http://bit.ly/1jS03fb.

85 Aisha Gani and Kareem Shaheen, “Journalist Ruqia Hassan murdered by Isis after writing on life in Raqqa,” *The Guardian*, January 5, 2016, http://bit.ly/1O8Gqbh.

86 See Committee to Protect Journalists, “James Foley,” *Journalists Killed/Syria*, 2014, https://cpj.org/killed/2014/james-foley.php, Committee to Protect Journalists, “Steven Sotloff,” *Journalists Killed/Syria*, 2014, https://cpj.org/killed/2014/steven-sotloff.php, and Committee to Protect Journalists, “Kenji Goto,” *Journalists Killed/Syria*, 2015, https://cpj.org/killed/2015/kenji-goto.php; I-fan Lin, “Hate Is Not What Humans Should Do: Slain Journalist Kenji Goto’s Words Live On Online,” *Global Voices*, February 7, 2015, http://bit.ly/1MyBlt1.

87 Sam Jones, “Russia steps up Syria cyber assault,” *Financial Times*, February 19, 2016, https://www.ft.com/content/1e97a43e-d726-11e5-829b-8564e7528e54.

88 John Scott-Railton and Seth Hardy, *Malware Attack Targeting Syrian ISIS Critics*, CitizenLab, December 18, 2014, http://bit.ly/1JbRwMW.

89 James Temperton, “FBI adds Syrian Electronic Army hackers to most wanted list,” *Wired*, March 23, 2016, http://www.wired.co.uk/article/syrian-electronic-army-fbi-most-wanted.

90 Christine Haughney and Nicole Perlroth, “Times Site Is Disrupted in Attack by Hackers,” *New York Times*, August 27, 2013, http://nyti.ms/17krXEO.

91 Julian E. Barnes, “Syrian Electronic Army Hacks Marines Website,” *The Wall Street Journal*, September 2, 2013, http://on.wsj.com/1KGVnFf.

92 Adario Strange, “Syrian Electronic Army Hacks Facebook's Domain Record,” *Mashable*, February 5, 2014, http://on.mash.to/1EQuHPY.

93 Gregory Ferenstein, “The Syrian Electronic Army Hacked Obama’s Twitter Links And Campaign Emails,” *Tech Crunch*, October 28, 2013, http://tcrn.ch/1Xi62bV.

94 Max Fisher, “Syria’s pro-Assad hackers infiltrate Human Rights Watch Web site and Twitter feed,” *Washington Post*, March 17, 2013. http://wapo.st/1eU9nKl.

95 Andy Greenberg, “How the Syrian Electronic Army Hacked Us: A Detailed Timeline,” *Forbes*, February 20, 2014, http://onforb.es/MEWYiq.

96 Brian Fung, “The Syrian Electronic Army just hacked the Washington Post (again),” *Washington Post*, May 14, 2015, http://wapo.st/1jS0eY7.

97 The Syrian Electronic Army, http://sea.sy/index/en.

98 Haroon Siddique and Paul Owen, “Syria: Army retakes Damascus suburbs-Monday 30 January,” *The Guardian*, January 30, 2012, http://bit.ly/1LZSDQA; Voltaire Network, “Speech by President Bashar al-Assad at Damascus University on the situation in Syria,” June 20, 2011, http://bit.ly/1FzOUEp.

99 “The Syrian Electronic Army Fights Rumors and Gives the True Picture of the Incident,” [in Arabic], *Wehda*, May 17, 2011, http://bit.ly/1OfOsCp.

Source URL: https://freedomhouse.org/report/freedom-net/2016/syria

published on