The Canadian Connection: An investigation of Syrian government and Hezbullah web hosting in Canada

November 17, 2011

Citizen Lab and Canada Centre for Global Security Studies
Munk School of Global Affairs
University of Toronto

Web version: http://citizenlab.org/the-canadian-connection/
Contact: info@citizenlab.org

Summary of Main Findings

- Websites of the Syrian government, including the Ministries of Culture, Transport, and others, are hosted on Canada-based web servers through intermediary companies, one of which, called “Platinum Incorporated,” advertises that it has co-location servers in Canada.

- The Syrian TV station Addounia TV, which is sanctioned by Canada and the European Union for inciting violence against Syrian citizens, uses Canada-based web servers to host its website.

- The website for Al-Manar -- the official media arm of the Lebanese political party, Hezbullah -- is hosted on Canada- and US-based web servers and employs Canada-based web servers to stream its TV broadcast globally. Al-Manar satellite broadcasts have been banned by the US, France, Spain, and Germany as well as the European Union. The United States includes Al-Manar on its Specially Designated Nationals List, a list of entities with which U.S. persons are generally prohibited from dealing, and the assets of which are blocked. Canada currently classifies Hezbullah as a terrorist organization.

- There are legal questions concerning the provision of web hosting services to each of these organizations. As the Syrian government, Addounia TV, and Hezbullah are all subject to Canadian sanctions, services provided by Canada-based hosting providers to these entities may fall within the scope of the sanctions.

- Any consideration of the removal of an organization’s website from web hosting services, however, must be treated as a potential infringement on freedom of speech and access to information, with due process and proper accountability mechanisms clearly articulated and followed.

Background and Overview

There has been increasing attention and concern around the provision of information and communication technologies, products, and services to repressive regimes. For example, recent reports, including several of our own,[1] have spotlighted the sale of commercial filtering and surveillance technologies to Internet service providers (ISPs) and / or governments who use those technologies to engage in national-level censorship of political, human rights, cultural, and religious content, and / or surveillance of citizens.[2] In November 2011, Citizen Lab and a number of other groups documented the presence of technology produced by California-based Blue Coat Systems to filter Internet content in Syria.[3] In our report *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma*, we also identified Blue Coat devices operating in Burma. The cases of Syria and Burma are especially noteworthy because Blue Coat is a U.S.-based company, and both Syria and Burma are subject to U.S. export restrictions.

In the case of Syria, the government is responsible for an ongoing and often brutal crackdown against democratic protesters that has been subject to widespread condemnation. A recent report by Human Rights Watch asserts that the Syrian regime has committed "crimes against humanity" in its violence committed against protesters in the city of Homs.[4] The Arab League has condemned the Syrian government for its mistreatment of its citizens, and has suspended Syria from its meetings.[5] The United Nations Office of the High Commissioner for Human Rights has estimated that over 3,500 Syrian citizens have been killed since demonstrations began in March 2011.[6]

[1] OpenNet Initiative, "West censoring East: The use of western technologies by Middle East censors," March 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

OpenNet Initiative, "When a Canadian company decides what citizens in the Middle East can access online," May 16, 2011, http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online

[2] In November 2011, Bloomberg reported on Italian firm Area SpA, who are installing a comprehensive web and mobile phone monitoring system in Syria. See Ben Elgin and V. 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

[3] Citizen Lab, "Behind Blue Coat: Investigations of commercial filtering in Syria and Burma," November 9, 2011, http://citizenlab.org/2011/11/behind-blue-coat/

[4] Human Rights Watch, "Syria: Crimes against humanity in Homs," November 11, 2011, http://www.hrw.org/news/2011/11/11/syria-crimes-against-humanity-homs

[5] BBC News, "Arab League sanctions for Syria" November 12, 2011, http://www.bbc.co.uk/news/world-middle-east-15706851

[6] United Nations News Centre, "Death toll passes 3,500 as Syrian Crackdown continues, says UN human rights office," November 8, 2011, http://www.un.org/apps/news/story.asp?NewsID=40326&Cr=Syria&Cr1=

This report continues Citizen Lab research into the intersection of the private sector, authoritarianism, and cyberspace regulation, turning our attention to a component of the Internet that does not typically receive the same amount of attention as filtering, surveillance, and computer network attack products and services: *web hosting services*.

Web hosting is a central element of Internet communications and commerce. Thousands of companies, large and small, operate servers on which content (including their organization's web presence) is stored and served to Internet users through a global market place. With the shift to cloud computing and social networking, the politics of web hosting have become more pronounced and complex.

Web hosting is an internationalized market. Given the global nature of Internet communications, web hosting can be purchased from nearly any political jurisdiction on the planet. Content that is associated with one region or country might very well be physically situated and served from computers that are based in an entirely different region or country. For that reason, web hosting can be used to circumvent legal and technical restrictions in one jurisdiction by hosting that content in another -- in effect using "safe havens" as a basis for strategic web hosting decisions.

Web hosting can also be politically controversial. Most of the controversy to date has centered on the conditions under which content is removed from hosting services. There have been numerous cases of content being dropped from web hosting services because of its politically controversial nature, and as a result of pressures being brought to bear on the web hosting providers by lobby groups and special interests without due process. Takedown vigilantism can have as strong an effect as any government regulations when it comes to creating chilling effects around politically controversial speech online.[7]

There are, however, many political jurisdictions in which certain content categories are considered illegal and web hosting services are prohibited from offering their services in these areas. Depending on the country concerned, there can be enormous variation. In China, entire blog-hosting services have been closed because of concerns over the content produced by their uses, and OpenNet Initiative (ONI)[8] research has documented other Chinese blogging providers

[7] Nart Villeneuve, "Free speech or hate speech," Nart Villeneuve: Malware Explorer, March 28, 2005, http://www.nartv.org/2005/03/28/free-speech-or-hate-speech/ ; Ethan Zuckerman, "Bluehost censors Zimbabwean bloggers", My Heart's in Accra, February 13, 2009, http://www.ethanzuckerman.com/blog/2009/02/13/bluehost-censors-zimbabwean-bloggers/

[8] The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa). Our aim is to investigate, expose, and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion. See OpenNet Initiative, http://opennet.net

using lists of sensitive keywords to prevent controversial material from being posted.[9] In Canada and other liberal democratic countries, on the other hand, restrictions on web hosting are limited primarily to hate speech and content related to the sexual exploitation of children, although even among liberal democratic countries there are variations.[10]

Web hosting is, therefore, categorically different than filtering and surveillance, and involves a different set of considerations when evaluating the market for web hosting services for repressive and authoritarian regimes and with respect to objectionable content in general. Filtering technologies are used to restrict speech and access to information whereas web hosting is designed to facilitate them. Whether and to what extent web hosting should be subject to restrictions of various sorts involves the same sort of reasoning as that applied to speech in general. In liberal democratic countries, infringements on freedom of speech are considered to be highly exceptional and need to be justified in explicit ways that follow due process and clearly specified laws.

In the course of Citizen Lab research, we have discovered that a significant number of Syrian government websites are hosted by Canada-based web servers, including the Ministry of Culture, Ministry of Transport, Ministry of Electricity, and Syrian Patent Office. We have also found that the Syrian TV station Addounia TV, which is sanctioned by Canada and the European Union for inciting violence against Syrian citizens, uses Canada-based web servers to host its website addounia.tv.

Outside of Syria, we found that the website for Al-Manar -- the official media arm of the Lebanese political party, Hezbullah -- is hosted on Canada- and US-based web servers and employs Canada-based web servers to stream its TV broadcast globally. Al-Manar satellite broadcasts have been banned by the US, France, Spain, and Germany as well as the European Union. The United States includes Al-Manar on its Specially Designated Nationals List, a list of entities with which U.S. persons are generally prohibited from dealing, and the assets of which are blocked. Canada currently classifies Hezbullah as a terrorist organization. In 2006 and 2008

[9] Ethan Zuckerman, ”Intermediary Censorship,” in Deibert, R., Palfrey, J., Rohozinski, R. and J. Zittrain (Eds), *Access Controlled: The shaping of power, rights and rule in cyberspace*, MIT Press 2010. http://www.access-controlled.net/wp-content/PDFs/chapter-5.pdf

[10] Canadian Human Rights Act (R.S.C. , 1985, c.H-6), Section 13, http://laws-lois.justice.gc.ca/eng/acts/H-6/FullText.html; Canadian Human Rights Commission, “Section 13 - Overview,” http://www.chrc-ccdp.ca/proactive_initiatives/hoi_hsi/qa_qr/page1-eng.aspx; OpenNet Initiative, “United States and Canada,” 2010, http://opennet.net/research/regions/united-states-and-canada OpenNet Initiative, “Europe” 2010, http://opennet.net/research/regions/europe.

there were reports of separate incidences of the Al-Manar website found hosted on Canadian providers.[11]

Each of these cases presents a variety of ethical, practical, and legal issues with significant human rights implications. We conclude this report with a discussion of the relevant ethical considerations and legal issues that arise from our research, and an open discussion of the challenges these cases pose for academia, civil society, the private sector, and policy makers.

Syrian government websites hosted on Canadian web servers

In 2009, the ONI reported that Syria was implementing Internet filtering with a product called ThunderCache, produced by a firm called Platinum Incorporated.[12] Reporters Without Borders has identified the Syrian Telecommunications Establishment (STE) and Syrian Information Organization (SIO) as clients who use the ThunderCache system.[13]

Platinum Inc. is a software development and network application developer currently based in Damascus, Syria. Founded in 1991, the company has worked in a variety of markets, including the provision of hosting services, and claims to have used co-located servers in Vancouver, Canada.[14] We found that the company has registered an IP block through Rackforce, a Kelowna, B.C.-based co-location provider.[15] Platinum Inc. is either owned by or affiliated with another company[16], The Kernel, which is headquartered at the following address:

Dubai Airport Free Zone
Building 6EA,
Office #209
Dubai - United Arab Emirates
Phone: +971 4 7017 260[17]

[11] CBC News, "Hezbollah hijacks Montreal firm's web server" August 11, 2006, http://www.cbc.ca/news/canada/montreal/story/2006/08/11/hezbollah-website.html; iWeb blog, "Information ou Désinformation? Hébergement de Al-Manar (Relié au Hezbollah)", August 11, 2006, http://blog.iweb.com/fr/2006/08/information-ou-desinformation-hebergement-de-al-manar-relie-au-hezbollah/427.html; Nart Villeneuve, "CBC takes down Hamas, Hezbullah websites." Nart Villeneuve: Malware Explorer, July 16, 2008, http://www.nartv.org/2008/07/16/cbc-takes-down-hamas-hezbollah-websites/

[12] OpenNet Initiative, "Syria," August 7, 2009, http://opennet.net/research/profiles/syria

[13] Reporters Without Borders, "Enemies of the Internet" March 12, 2010, http://en.rsf.org/IMG/pdf/Internet_enemies.pdf

[14] Platinum Inc., "Who we are," http://platinum.sy/?d=50&id=24

[15] See http://whois.domaintools.com/69.10.157.240

[16] The Kernel identifies Platinum and Thundercache as "Our Products". See http://www.thekernel.com/about/profile

[17] The Kernel, "About The Kernel," http://thekernel.com/about

Platinum Inc. hosts their corporate website (http://platinum.sy) through iWeb, a Montreal-based hosting company.[18] In the course of our research we found more than 100 other domains also hosted at this same IP address, many of which are Syrian companies and organizations. This list includes the websites of a number of Syrian government ministries and agencies. Many of these Syrian government websites indicate that they are "Powered by Platinum Inc.," including the Ministry of Social Affairs and Labor[19] and the Ministry of Transport.[20] Several other government websites hosted within Syria also include the phrase "Powered by Platinum Inc.," including the Syrian Telecommunications Establishment (Syrian Telecom)[21] and Syrian Renewable Energy.[22]

This process led us to investigate other Syrian government websites that are hosted in Canada. Our research has uncovered a total of 17 Syrian government websites hosted through Canadian hosting providers (Table 1).

[18] See http://www.robtex.com/dns/platinum.sy.html#all

[19] See molsa.gov.sy

[20] See http://www.mot.gov.sy/

[21] See http://www.ste.gov.sy/

[22] See http://www.syreen.gov.sy/

Table 1: Syrian Government Websites Hosted in Canada

Department/Agency	Hostname	Hosting country	Hosting provider	IP Address
Ministry of Culture	www.moc.gov.sy	Canada	iWeb	174.142.53.8
Ministry of Electricity	www.moe.gov.sy	Canada	Rackforce	209.97.212.140
Ministry of Transport	www.mot.gov.sy	Canada	iWeb	174.142.53.8
Ministry of Electricity (Branch Office)	www.damasreef-elec.gov.sy	Canada	iWeb	67.205.85.166
Ministry of Social Affairs and Labor	molsa.gov.sy	Canada	iWeb	174.142.53.8
Syrian Patent Office (Ministry of Economy & Trade)	www.spo.gov.sy	Canada	iWeb	209.172.50.157
Ministry of Irrigation	irrigation.gov.sy	Canada	iWeb	174.142.53.8
The Directorate-General of Antiquities and Museums	www.dgam.gov.sy	Canada	iWeb	174.142.53.8
Public Establishment for Electrical Generation and Transfer (Ministry of Electricity)	peegt.gov.sy	Canada	iWeb	174.142.53.8
City of Homs	homs-city.gov.sy	Canada	iWeb	67.205.85.166
Industrial Research & Testing Center	itrc.gov.sy	Canada	iWeb	174.142.53.8
City of Deirezzor	deirezzor-city.gov.sy	Canada	iWeb	67.205.85.166
Palmyra City	palmyra-city.gov.sy	Canada	iWeb	67.205.85.166
Old City of Damascus	www.old-damascus.gov.sy	Canada	iWeb	67.205.85.166
Lattakia City	www.latakia-city.gov.sy	Canada	iWeb	67.205.85.166
Governorate of Raqqa Website	www.raqqa.gov.sy	Canada	iWeb	184.107.58.236
Tartous City	tartous-city.gov.sy	Canada	iWeb	67.205.85.166

We also discovered that a number of other Syrian government websites are hosted by providers in the United States and Germany (Table 2).

Table 2: Syrian Government Websites Hosted in the United States and Germany

Department/Agency	**Hostname**	**Hosting Country**	**Hosting Provider**	**IP Address**
Ministry of Economy and Trade	www.syrecon.gov.sy	United States	SoftLayer[23]	174.120.51.2
Ministry of Finance	syrianfinance.gov.sy	United States	SoftLayer	70.84.218.92
Ministry of Agriculture and Agrarian Reform	moaar.gov.sy	United States	HopOne Global	209.160.33.125
Ministry of Endowment (Religious Affairs)	www.mow.gov.sy	United States	Host Dime	66.7.198.11
General Commission for Competition and Antimonopoly	www.competition.gov.sy	United States	SoftLayer	174.120.51.2
Export Development and Promotion Agency	edpa.gov.sy	United States	Server Central	216.246.46.101
Governorate of Hama Website	www.hama.gov.sy	United States	WeHostWebSites	72.18.131.37
Aleppo Wakf (Endowment) Website	aleppowakf.gov.sy	Germany	Strato Hosting	85.214.127.204
General Syrian Authority for Books	syrbook.gov.sy	Germany	Giga Hosting	193.200.241.24

[23] This IP appears on ThePlanet ASN though that entity is now merged with SoftLayer Technologies Inc. See http://www.softlayer.com/softlayer-the-planet-merger-faq.

Syrian Addounia TV hosted on Canadian web servers

Addounia TV is a Syria-based private television station owned by a group of seven business people closely connected with the regime.[24] Since the beginning of the democratic demonstrations in Syria, activists have accused Addounia TV of inciting sectarianism, violence and the use of force against the peaceful protesters.[25] They have also accused it of siding with the Syrian regime and marketing its propaganda about the uprisings.[26] Pro-revolution websites have archived clips from Addounia TV as examples of incitement of violence. For instance, the Syrian Revolution News website syrrevnews.com posted a clip from Addounia TV in which a guest calls on the Syrian authorities to use decisive force against protesters to end the demonstrations immediately.[27] An Arabic Facebook page, apparently run by Syrians, campaigns to have two key Arab satellites (ArabSat and NileSat) discontinue carrying Addounia TV.[28]

Addounnia TV has also been involved in disseminating disinformation meant to obfuscate the nature and seriousness of the violence in Syria. For example, in a September 9, 2011 broadcast, Addounia TV argued that the Doha-based Al Jazeera network staged protests in “cinematic replicas” of Syrian cities built in Qatar in order to fabricate the uprisings.[29]

Addounia TV and Canadian servers

Addounia TV has registered at least two domains: addounia.tv and addounia.org. Both domains were originally registered in 2006 by Platinum, Inc. and are currently registered at the same Dubai address mentioned above.[30] Both domains display the same content and point to addounia.tv, which is hosted in Canada by iWeb Technologies.[31]

Addounia TV’s website includes functionality to stream direct video content of the station’s broadcasts. These webstreams originate from 38.96.148.40 and are hosted by U.S.-based Cogent Communications.[32]

[24] See http://aawsat.com/details.asp?section=4&article=632644&issueno=11927 (Arabic)
[25] Ibid.
[26] Ibid.
[27] See http://www.syrrevnews.com/archives/2142

[28] See Facebook Page at http://ar-ar.facebook.com/Shut.down.Addounia.TV
[29] Jillian Dunham, “Syrian TV station accuses Al Jazeera of fabricating uprising,” New York Times, September 14, 2011, http://thelede.blogs.nytimes.com/2011/09/14/syrian-tv-station-accuses-al-jazeera-of-fabricating-uprising/
[30] Domain Tools, “Whois history for Addounia.tv on 2007-01-04,” http://www.domaintools.com/research/whois-history/?page=details&domain=addounia.tv&date=2007-01-04

[31] See http://www.robtex.com/dns/addounia.tv.html#all

[32] See http://whois.domaintools.com/38.96.148.40

Addounia TV and Hacking Activities

As a result of Addounia TV's controversial role in the current uprisings its website has been targeted by pro-revolution hackers. In a recent Information Warfare Monitor report, *Syrian Electronic Army: Disruptive Attacks and Hyped Targets*, we documented Addounia TV's website as one of four pro-Syrian regime websites targeted by Denial of Service (DoS) software that was re-purposed by pro-revolution hackers. The software was originally designed to target international media websites, including Al Jazeera and BBC News, by pro-Syrian regime hackers who claimed the news organizations spread biased and hostile information about the protests in Syria.[33]

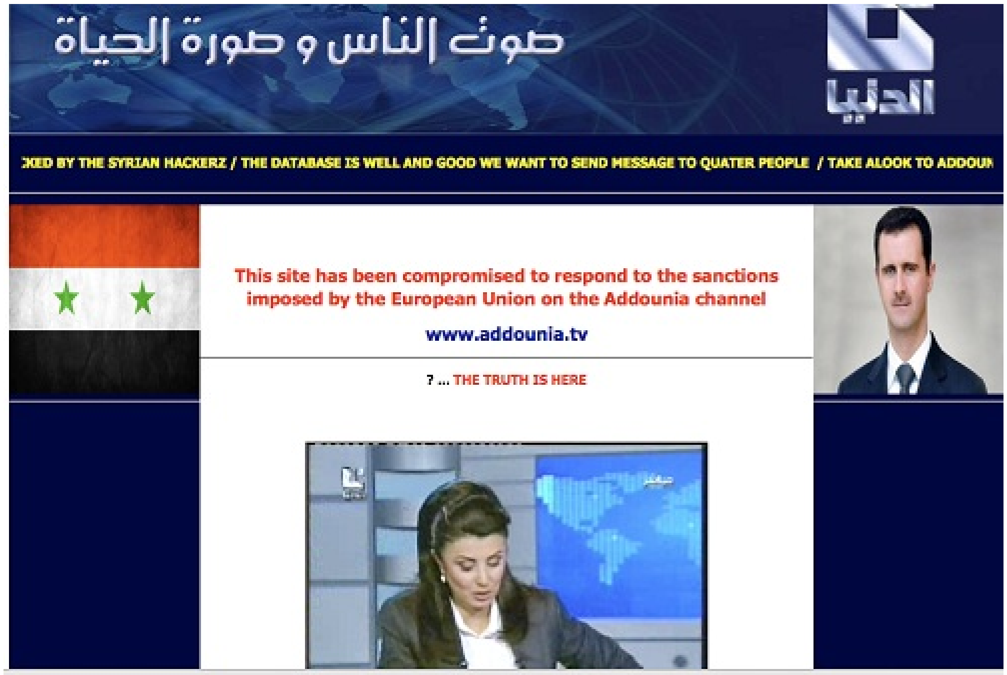
We have also documented instances of pro-Syrian regime hackers defacing several Arab and Western websites, replacing their default page with that of the Addounia TV page, and inserting links to the live TV webstream. These defacement attacks were conducted after the European Union imposed sanctions on Addounia TV.

The defacement message read:

> "This site has been compromised to respond to the sanctions imposed by the European Union on the Addounia channel."

This message can be seen on the Doha-based Shafallah Medical Genetics Center (http://smgc.org.qa/) (Figure 1).

[33] The Information Warfare Monitor is a collaborative research project between the Citizen Lab at the Munk School of Global Affairs (University of Toronto) and the SecDev Group (Ottawa) tracking the emergence of cyberspace as a strategic domain. Information Warfare Monitor, "Syrian Electronic Army: Disruptive Attacks and Hyped Targets," June 25, 2011, http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/



:KED BY THE SYRIAN HACKERZ / THE DATABASE IS WELL AND GOOD WE WANT TO SEND MESSAGE TO QUATER PEOPLE / TAKE ALOOK TO ADDOUN

This site has been compromised to respond to the sanctions imposed by the European Union on the Addounia channel

www.addounia.tv

? ... THE TRUTH IS HERE

Figure 1: Screenshot of the defaced Shafallah Medical Genetics Center website

Hezbullah in Canada

Background about Al-Manar

Al-Manar (the Beacon), the Lebanon-based satellite television broadcaster which is the official media arm of Hezbullah, has generated much debate in light of its controversial content.[34] Canada currently classifies Hezbullah as a terrorist organization.[35] Additionally, the U.S. includes Al-Manar on its Specially Designated Nationals List, a list of entities with which U.S. persons are generally prohibited from dealing, and the assets of which are blocked.[36]

[34] Ben Saul and Dr. Daniel Joyce, *International Approaches to the Regulation of Al-Manar Television and Terrorism-related content*, June 2010, http://www.acma.gov.au/webwr/_assets/main/lib310780/intntl_approaches-regulation-al-manar_tv_and_terrorism-related_content.pdf.

[35] *Regulations Establishing a List of Entities*, SOR/2002-284, July 23, 2002, http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-284/page-1.html#h-1

[36] U.S. Department of Treasury, Office of Foreign Assets Control, “Specially Designated Nationals and Blocked Persons,” November 3, 2011, http://www.treasury.gov/ofac/downloads/t11sdn.pdf.

Al-Manar and Canadian servers

In 2006 it was reported that iWeb had been "hacked" by Hezbullah in order to use the provider to host their content.[37] While denying that they had been compromised by attackers, iWeb acknowledged that their servers had been used to host Al-Manar and stated that once they became aware of the issue they notified their client and the site was removed.[38]

In 2008, the CBC reported that websites affiliated with Hezbullah and Hamas were being hosted on iWeb. Initial take down requests were not successful. However, after the CBC translated Arabic content on a discussion forum found on one of the sites and contacted iWeb claiming that the content could be considered a violation of Canadian anti-terrorism legislation, the websites were removed. Nart Villeneuve's commentary on the story explains that it was unclear which specific sites were taken down, but the sites for Al-Manar (www.almanar.com.lb) and Hamas run Al-Aqsa TV (www.aqsatv.ps) were both previously hosted on iWeb.[39] In reaction to the CBC story and take down request, iWeb issued a statement that noted "two websites that promote the activities of suspected terrorist organizations had indeed found their way onto iWeb's infrastructure; however these sites were shut down as soon as this was confirmed".[40] In response to follow-up inquires made by Villeneuve regarding the specific websites in question iWeb explained "we cannot go into the specific details of this situation."[41]

Citizen Lab research has shown that Al-Manar's primary website is still being hosted in North America. Almanar.com.lb is currently hosted in a round robin DNS configuration[42] by three different hosting providers: SoftLayer and Vault Networks in the U.S. and iWeb Technologies in

[37] CBC News, "Hezbollah hijacks Montreal firm's web server" August 11, 2006, http://www.cbc.ca/news/canada/montreal/story/2006/08/11/hezbollah-website.html

[38] iWeb blog, "Information ou Désinformation? Hébergement de Al-Manar (Relié au Hezbollah)", August 11, 2006, http://blog.iweb.com/fr/2006/08/information-ou-desinformation-hebergement-de-al-manar-relie-au-hezbollah/427.html

[39] Nart Villeneuve, "CBC takes down Hamas, Hezbullah websites." Nart Villeneuve: Malware Explorer, July 16, 2008, http://www.nartv.org/2008/07/16/cbc-takes-down-hamas-hezbollah-websites/

[40] iWeb Blog, "Reacting to illegal or questionable content on servers," July 15, 2008, http://blog.iweb.ca/en/2008/07/reacting-to-illegal-or-questionable-content-on-servers/742.html

[41] ibid. (See comments section)

[42] Round robin DNS configuration involves a domain name being associated with multiple IPs for the purpose of redundancy and load balancing.

Canada.[43] Like Addounia TV, Al-Manar offers video streaming of its live broadcasts. Citizen Lab researchers ran packet captures to confirm that all video content is being streamed from 72.55.164.21, an IP address in the iWeb Technologies address space. Al-Manar has an additional domain (http://almanarnews.net) that is also hosted in round robin DNS configuration on three U.S.-based hosting providers: SoftLayer, Vault Networks and MegaNET.[44]

Hezbullah's media operations also include a radio station called Al-Nour (http://www.al-nour.net/) that broadcasts from Lebanon and offers audio streaming of its live broadcasts. Like Al-Manar, the U.S. includes Al-Nour on its Specially Designated Nationals List.[45] Citizen Lab researchers have found that the Al-Nour website is hosted on U.S. web host Tiggee, while the radio stream is hosted by another U.S.-based web host, Sago Networks (66.111.34.191).[46] We have also found additional Hezbullah-associated websites hosted on U.S. web servers. For example, the website of "Islamic Resistance In Lebanon - Hezbullah" (http://moqawama.org) -- which refers to itself as the "official website of the Islamic Resistance in Lebanon" -- is hosted by U.S. web host Tiggee as well.[47]

[43] See http://www.robtex.com/dns/almanar.com.lb.html#all

[44] See http://www.robtex.com/dns/almanarnews.net.html

[45] U.S. Department of Treasury, Office of Foreign Assets Control, "Specially Designated Nationals and Blocked Persons," November 3, 2011, http://www.treasury.gov/ofac/downloads/t11sdn.pdf.

[46] See http://www.robtex.com/ip/66.111.34.191.html

[47] See http://www.robtex.com/dns/moqawama.org.html

Ethical and Legal Issues

The existing legal and regulatory framework applicable to the provision of web hosting services by private companies is limited, and short on guidance with respect to prevention of misuse of services by repressive regimes. Debate and resulting legislation thus far has focused primarily on the issue of intermediary liability, which concerns a web host's responsibility for content uploaded by a client that may constitute hate speech, incitement to violence, or other illegal content.[48] Precedent and legislation in jurisdictions such as Canada and the U.S. has established that a web host is typically not liable for such content, provided the company responds promptly to take-down requests.[49]

However, separate and apart from any assessment of the legality of content -- which is largely outside the scope of this report -- is the issue of provision of services in the first instance by private companies in liberal democratic countries to entities owned or controlled by, or otherwise affiliated with, repressive regimes. On this matter, the legal framework applicable to web hosting companies is less clear, though the human rights consequences of that provision of services may be significant -- particularly as the importance of a government's online presence and activities to its overall strategy, policies, and very existence continues to grow.

When it comes to the question of engaging in business with an entity associated with a repressive regime, the primarily applicable set of laws and regulations are those that concern sanctions. Sanctions imposed by Canada against Syria currently list 56 individuals and 21 entities -- including Addounia TV -- as "designated persons" to which Canadian persons are prohibited from making goods available, given these individuals' and entities' close ties to the Syrian regime.[50] However, it is unknown whether providing hosting services to an entity on the "designated person" list would constitute provision of "goods" in violation of the regulations, and, if so, whether any of the web hosting services cited in this report may have applied for a permit to conduct such business as delineated in the *Special Economic Measures (Syria) Permit Authorization Order*.[51]

The existence of sanctions against Syrian entities like Addounia TV, however, should itself prompt some inquiry from web hosting services as to the human rights implications of providing an online platform to organizations associated with the Syrian regime. Like Canada, the U.S. and

[48] See, e.g., Center for Democracy & Technology, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation*, April 2010, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf.

[49] Ibid; OpenNet Initiative, "United States and Canada," 2010, http://opennet.net/research/regions/united-states-and-canada

[50] Department of Justice Canada, *Special Economic Measures (Syria) Regulations*, SOR/2011-114, http://laws-lois.justice.gc.ca/eng/regulations/SOR-2011-114/FullText.html

[51] *Special Economic Measures (Syria) Permit Authorization Order*, SOR/2011-115, May 24, 2011, http://www.gazette.gc.ca/rp-pr/p2/2011/2011-06-08/html/sor-dors115-eng.html

the EU also impose sanctions against Syria, which merits additional consideration regarding the significance of the human rights violations occurring in the country. The U.S. sanctions widely prohibit export or re-export of U.S. products to Syria,[52] including "the direct or indirect exportation of web-hosting services that are for purposes other than personal communications (e.g., web-hosting services for commercial endeavors) or of domain name registration services."[53] In May 2011, the EU enacted its own strict sanctions against Syria, noting that, "[i]n view of the seriousness of the situation, restrictive measures should be imposed against Syria and against persons responsible for the violent repression against the civilian population in Syria."[54]

The EU has continued to expand these sanctions, which require, *inter alia*, the freezing of funds and economic resources of designated individuals and entities affiliated with the regime, as well as non-provision of such funds and economic resources going forward.[55] On September 23, 2011, the Council of the European Union added Addounia TV to its list of sanctioned individuals and entities, on the basis that Addounia TV had "incited violence against the civilian population in Syria."[56] Addounia TV, on the other hand, condemned its inclusion by the EU on the sanctions list, asserting that the station was neutral in its coverage.[57] Thus, while compliance

[52] U.S. Department of the Treasury, "Syria Sanctions," http://www.treasury.gov/resource-center/sanctions/Programs/pages/syria.aspx

[53] U.S. Department of Treasury, Office of Foreign Assets Control, "General License No. 5: Exportation of Certain Services Incident to Internet-Based Communications Authorized," August 18, 2011, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_gl5.pdf

[54] Council of the European Union, Decision 2011/273/CFSP, May 9, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:121:0011:0014:EN:PDF; see also Council of the European Union: Regulation (EU) No. 442/2011, May 9, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:121:0001:0010:EN:PDF; Decision 2011/522/CFSP, September 2, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:228:0016:0018:EN:PDF; Regulation (EU) No. 878/2011, September 2, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:228:0001:0005:EN:PDF; Decision 2011/628/CFSP, September 23, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:247:0017:0021:EN:PDF; Regulation (EU) No. 950/2011, September 23, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:247:0003:0007:EN:PDF; Decision 2011/684/CFSP, October 13, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:269:0033:0035:EN:PDF; Regulation (EU) No. 1011/2011, October 13, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:269:0018:0020:EN:PDF; Decision 2011/735/CFSP, November 14, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:296:0053:0054:EN:PDF; Regulation (EU) No. 1150/2011, November 14, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:296:0001:0002:EN:PDF

[55] Ibid.

[56] Council of the European Union, Decision 2011/628/CFSP, September 23, 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:247:0017:0021:EN:PDF.

[57] "Addounia TV Honored by the EU Sanctions," Syrian Arab News Agency, September 25, 2011, http://www.sana.sy/eng/21/2011/09/25/371585.htm.

with complex sanctions regulations by web hosting services raises a number of issues (see discussion below), this is an area that web hosting companies will increasingly face.

Finally, anti-terrorism legislation is also relevant to assessing the legality of providing web hosting services to certain entities -- including Hezbullah. Canada employs three terrorist listing mechanisms to designate individuals and entities subject to anti-terrorism measures: the *United Nations Al-Qaida and Taliban Regulations*, the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*, and the *Criminal Code*, pursuant to which have been adopted *Regulations Establishing a List of Entities*.[58] The latter regulations designate Hezbullah as an entity that "has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity or is knowingly acting on behalf of, at the direction of or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity."[59] (Hezbullah is also designated a terrorist organization by the U.S.).[60] Under section 83.18 of the *Criminal Code*, it is an indictable offense to knowingly participate in or contribute to -- directly or indirectly -- any activity of a terrorist group, including listed entities.[61] Inclusion of individuals or entities on such lists may also raise due process concerns -- for example, regarding what criteria and evidence were employed for inclusion of a person or group, or the ability to challenge a listing decision -- yet web hosting companies are obligated to comply with the anti-terrorism laws of their own jurisdiction.

Discussion and Next Steps

The cases discussed in this report underscore the very complex, highly nuanced, and globally distributed world of web hosting. Organizations resident in one political jurisdiction of the world can have their content and websites hosted and streamed from an entirely different region of the world, and sometimes several, and be subject to the laws of those political jurisdictions. As more social, political, and economic life takes place online, pressures have grown on web hosting companies from a variety of quarters to remove or refrain from hosting particular organizations and their content. There have been numerous instances of content removal taking place without proper due process or accountability. It is imperative that the conditions under which content is

[58] Foreign Affairs and International Trade Canada, "Terrorists," November 1, 2011, http://www.international.gc.ca/sanctions/terrorists-terroristes.aspx?lang=eng&menu_id=24&view=d

[59] *Regulations Establishing a List of Entities*, SOR/2002-284, July 23, 2002, http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-284/page-1.html#h-1

[60] U.S. Department of State, "Foreign Terrorist Organizations," September 15, 2011, http://www.state.gov/s/ct/rls/other/des/123085.htm

[61] *Criminal Code* § 83.18, http://laws-lois.justice.gc.ca/eng/acts/C-46/page-30.html

removed from web hosting platforms be given careful scrutiny, that vigilantism is avoided, and that any removal be in line with due process and proper oversight and accountability.

The online presence on Canadian servers of numerous Syrian and other entities that have compromised international human rights raises difficult questions. What is the appropriate course of action when a Canadian- or U.S.-based web hosting service contracts with an entity owned or controlled by a repressive regime with a track record of human rights abuse? A solution is not clear cut, and no existing legal or regulatory framework appears to adequately account for the problem presented. Nor is it necessarily a simple matter for a web hosting company to gauge with whom they are contracting when entities in question may use intermediaries to undertake contracts on their behalf.

This report urges governments, web-hosting services, and civil society organizations to engage in greater dialogue about how to prevent provision of an electronic "safe haven" to regimes that use such resources in violating human rights. While drawing on the current sanctions regime may be an appropriate starting point, further consideration is essential to avoid subjecting legitimate expression to unwarranted takedown or to impose unrealistic demands on web hosting companies to “police the Internet.”

On the one hand, as a matter of public policy, providing an online platform to a government that engages in well-documented and ongoing human rights abuses could significantly exacerbate such abuses -- particularly if government entities use that online space to incite violence, as appears to be the case with Addounia TV. On the other hand, how should a web hosting company go about determining when its potential clients present such human rights concerns? What if the client is an intermediary, obfuscating whom they represent? There is a risk that web hosting providers will overcompensate when it comes to screening entities that may expose them to reputational or legal liability, and possibly refuse to provide services to legitimate organizations, thereby also creating a negative human rights impact.

Moreover, *reactive* take-downs by web hosts may not account for due process considerations and may compromise legitimate users. They are also not effective in preventing misuse of the resource in the first instance. The concept of enforcing "intermediary liability" has been a subject of much debate, but web hosts are typically not called upon to take action without first receiving a (possibly illegitimate) take down request.[62]

[62] Ethan Zuckerman, ”Intermediary Censorship,” in Deibert, R., Palfrey, J., Rohozinski, R. and J. Zittrain (Eds), *Access Controlled: The shaping of power, rights and rule in cyberspace*, MIT Press 2010. http://www.access-controlled.net/wp-content/PDFs/chapter-5.pdf
OpenNet Initiative, “Policing Content in the Quasi-Public Sphere,” September 2010, http://opennet.net/sites/opennet.net/files/PolicingContent.pdf

While imperfect, the existence of a sanctions regime with respect to Syria creates at least some set of guidelines for web host companies to follow. As part of such a regime, a designated persons list is key in that it will inform a clear procedure for engagement or disengagement with clients, rather than leaving interpretation of the human rights record of a particular entity up to a web host that may have little or no experience in the field or familiarity with the background of a given client.

It is essential, however, that web hosting companies carefully assess and not misinterpret government sanctions and designated persons lists, as misinterpretation can also create negative human rights impact.[63] Blanket contractual exclusions (such as "prohibited persons" clauses) covering individuals or entities that are merely located in a sanctioned country may not properly limit the measures web hosting companies pursue to avoid providing material support to repressive regimes as envisioned by sanctions regulations, and may inadvertently compromise legitimate organizations through an overly broad approach.[64] The demonstrated track record of ISPs and web hosting companies so far suggests that they should not be left without guidance on how to properly implement such measures or incorporate due process mechanisms. Guidance from government institutions and civil society actors is, therefore, essential.

In sum, sanctions are an imperfect and relatively blunt instrument, more so when filtered through the individual interpretations (or misinterpretations) of private companies seeking to determine compliance requirements. Moreover, the fear of sanctions penalties cannot be the only motivating factor for restricting provision of services, and is unlikely to lead to optimal outcomes. Companies should proactively consider the human rights impact of the services they provide that may enable regimes,[65] as well as the associated reputational risk to the company. In addition to due diligence measures, web hosts should carefully consider the contractual language they incorporate pertaining to this issue, providing the required level of nuance, and do their best to gauge the intermediaries with whom they are contracting.

Taken in its entirety, we hope the cases highlighted in this report will serve as inspiration to Canadians (including civil society, academia, and the private sector) and the Canadian government that a broader discussion of cyberspace policy, governance, and security is required than has taken place to date. That the Syrian government and Addounia TV host their content

[63] Ibid; Evgeny Morozov, "Do-It-Yourself Censorship," Newsweek, March 6, 2009, http://www.thedailybeast.com/newsweek/2009/03/06/do-it-yourself-censorship.html.

[64] Ibid.

[65] See, for example, the standards articulated by Electronic Frontier Foundation (EFF) regarding proactive steps companies providing surveillance technologies can take to help protect human rights: EFF, "'Know Your Customer' Standards for Sales of Surveillance Equipment," October 24, 2011, https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment. Elements of such standards may be adaptable to the context of web hosting services.

from servers in Canada is at minimum in contradiction to Canada’s stated foreign policy with regard to the ongoing violence in Syria, and possibly material support to a regime that is engaged in systematic violence against peaceful demonstrators. More broadly, we encourage governments, civil society, and the private sector to seriously consider how best to handle the expanding responsibilities of web hosting companies and how due process and proper accountability mechanisms can be normalized in ways that protect free speech and access to information, while avoiding support for human rights abuses and repressive regimes in ways that have arisen here in Canada.

About the Canada Centre for Global Security Studies

The Canada Centre for Global Security Studies is an interdisciplinary unit at the Munk School of Global Affairs, University of Toronto that engages in advanced research and policy development around global security issues including cyber security, global health, and region-specific concerns, such as the Arctic, Europe and the Commonwealth of Independent States, Asia, and the changing face of the Americas.

About the Citizen Lab

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada focusing on advanced research and development at the intersection of digital media, global security, and human rights. The Citizen Lab's ongoing research network includes the Information Warfare Monitor, the OpenNet Initiative, OpenNet Eurasia, and Opennet.Asia.