The Citizen Lab

Research Brief
November 2011

Behind Blue Coat:
Commercial Filtering in Syria and Burma

SUMMARY

Citizen Lab research into the use of commercial filtering products in countries under the rule of authoritarian regimes has uncovered a number of devices manufactured by U.S.-based Blue Coat Systems in Syria and Burma. Although Blue Coat has recently acknowledged the presence of their devices in Syria, this brief contributes to previous findings of devices in the country, documents additional devices in use in Syria, and identifies Blue Coat devices actively in use in Burma. This brief urges Blue Coat to investigate these claims and take action to prevent the further use of its technology in Syria and Burma.

BACKGROUND

In recent months concern has grown over the use of commercial filtering technology in Syria, particularly in light of the Syrian regime's violent crackdown against the 2011 uprising.[1] Debate has recently focused on Blue Coat Systems, a California-based manufacturer of networking technology that develops network security and optimization tools. These tools include ProxySG devices that work with WebFilter, a product that categorizes billions of web pages to permit filtering of unwanted content.[2] In August 2011, the website Reflets.info announced that it would be releasing a series of blog posts concerning the use of Blue Coat devices in Syria.[3] Reflets.info later documented the presence of Blue Coat devices through in-country testing.[4] This work was done in collaboration with the group Telecomix, which in October 2011 released 54gb of data purporting to be log files from Blue Coat devices active in Syria.[5]

Following the release of this information, Blue Coat initially denied that its equipment had been sold to Syria, a country to which the export or reexport of U.S. products is prohibited pursuant to U.S. sanctions (with certain limited exceptions).[6] Media reports cited an unnamed Blue Coat representative who refuted the claim

that the company had sold equipment to the Syrian government and stated that "under Blue Coat's company policy, sales to countries subject to U.S. trade embargoes are not authorised."[7] Further reports quoted Blue Coat spokesperson Steve Schick as stating: "Blue Coat does not sell to Syria. We comply with U.S. export laws and we do not allow our partners to sell to embargoed countries."[8] It was also reported that the U.S. State Department was actively investigating the issue, with an unnamed official stating: "The issue of Blue Coat's technology being used in Syria is one that the State Department is taking very seriously and is very concerned about."[9]

However, on October 29, 2011, Blue Coat changed course and acknowledged the use of its technology in Syria. In a report in the Wall Street Journal, the company acknowledged that 13 of its devices, initially shipped through a distributor from Dubai and destined for the Iraqi Ministry of Communications, ended up in Syria.[10] The company further acknowledged that the devices had been communicating with Blue Coat-controlled servers; however, the company claimed it does not monitor the locations from which such communications originate.[11] Blue Coat senior vice president Steve Daheb stated: "We don't want our products to be used by the government of Syria or any other country embargoed by the United States."[12]

Since August 2011, Citizen Lab researchers have been conducting technical research into the presence of Blue Coat devices in Syria and in other countries under the rule of authoritarian regimes. While Blue Coat's most recent admissions confirm a number of our findings, our research has also raised additional questions relevant to the use of Blue Coat technology for purposes that compromise internationally-recognized human rights. Our findings include the presence of additional Blue Coat devices active in Syria, as well as the presence of a number of Blue Coat devices in Burma. We urge Blue Coat to investigate these matters further in a transparent manner, and take action to prevent further use of Blue Coat technology in Syria and Burma.

METHODOLOGY

This report is a continuation of past OpenNet Initiative[13] (ONI) research into the use of commercial filtering technologies to implement Internet censorship, particularly the sale of commercial technologies to Internet service providers (ISPs) in countries where government policy and practice is to restrict Internet content and violate human rights.[14] The objective of this research was to document empirically and from an evidential basis that such technologies were and are in use in such countries, including Syria and Burma, and were and are actively being employed to censor Internet content.

Two methods were employed in conducting this research. In the case of Syria, all data was gathered remotely and no field research within the country was conducted. Evidence was gathered through network scans of publicly accessible servers in the IP address ranges of the Syrian Telecommunications Establishment. In the case of Burma, research was based on data gathered from in-country field testing and research. Testers within Burma ran ONI-developed software that tested access to 1,669 URLs, both within Burma and from a country

that does not filter Internet content simultaneously. The data gathered from the country with no filtering is used as a control to compare the data from the country suspected of filtering. Two lists of URLs are tested: a 'local' list unique to each country and a 'global' list tested in all countries, which allows for comparisons across countries. The global list is comprised of internationally relevant websites with a range of content including political, social, conflict / security and Internet tools. The local list is designed individually for a specific country with URLs relevant to local politics and context. These lists are samples and are not meant to be exhaustive. The results of these tests are analyzed by ONI researchers to determine if a URL is blocked and how that block is occurring.[15] The results obtained from this testing were combined with publicly available data gathered from technical analysis of Burmese networks and Blue Coat's Site Review website to develop a fuller picture of Burma's filtering regime.[16]

In the course of this project, we carefully deliberated on the ethics of our research methods.[17] Issues raised included the ethics of accessing publicly available computer systems which, it is reasonable to believe, the administrators of such systems do not want outsiders to access. We concluded that as such systems were publicly available on the open Internet, the information gathered is fair grounds for research purposes. No attempts were made to subvert security measures, discover or use user credentials, or disrupt the operation of any computer system. Furthermore, no information disclosed here contains personally identifiable information.

The Citizen Lab contacted Blue Coat Systems on October 27, 2011, requesting more information regarding the sale and use of Blue Coat technology in countries against which U.S. trade sanctions are imposed. As of November 9, 2011, we have received no response.

FINDINGS

While Blue Coat has acknowledged that 13 of their devices are present in Syria, there are additional aspects of this case that warrant further discussion and raise additional questions about the use of commercial filtering technologies in Syria and other countries under the rule of authoritarian regimes.

1. Additional Blue Coat devices present in Syria

Blue Coat has claimed that there are 13 of its devices present in Syria, which were part of a shipment of 14 devices reportedly sold to the Iraqi government.[18] Additional information gathered by Citizen Lab researchers and other groups indicates, however, that there are more than 13 Blue Coat devices active in the country. The website Reflets.info, in collaboration with the Telecomix group, identified upwards of 15 Blue Coat devices actively in use in Syria.[19] Separate from and additional to those devices identified by Reflets, Citizen Lab has identified Blue Coat devices active on four other IP addresses belonging to the Syrian Telecommunications Establishment, which are:

- 213.178.244.100
- 213.178.244.173
- 213.178.244.174
- 213.178.244.175

Citizen Lab identified these as Blue Coat devices through their web administration, security certificates and HTTP header data. Three of these have security certificates identifying them as Blue Coat SG8100 series devices (figure 1).

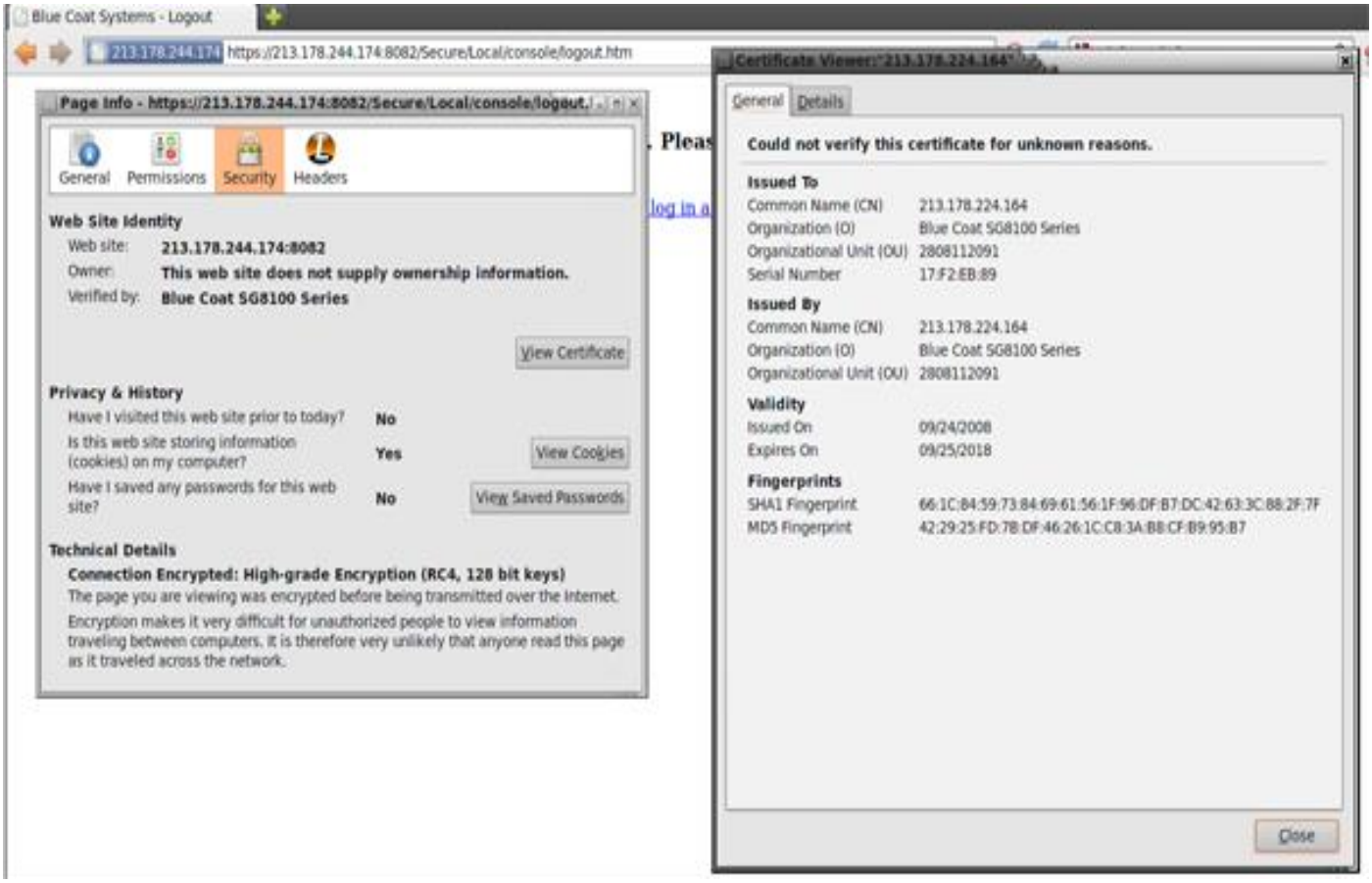

Figure 1: Blue Coat device on SCS IP address [213.178.244.174]

The devices displayed “Blue Coat Systems” in their logout page (figure 2).

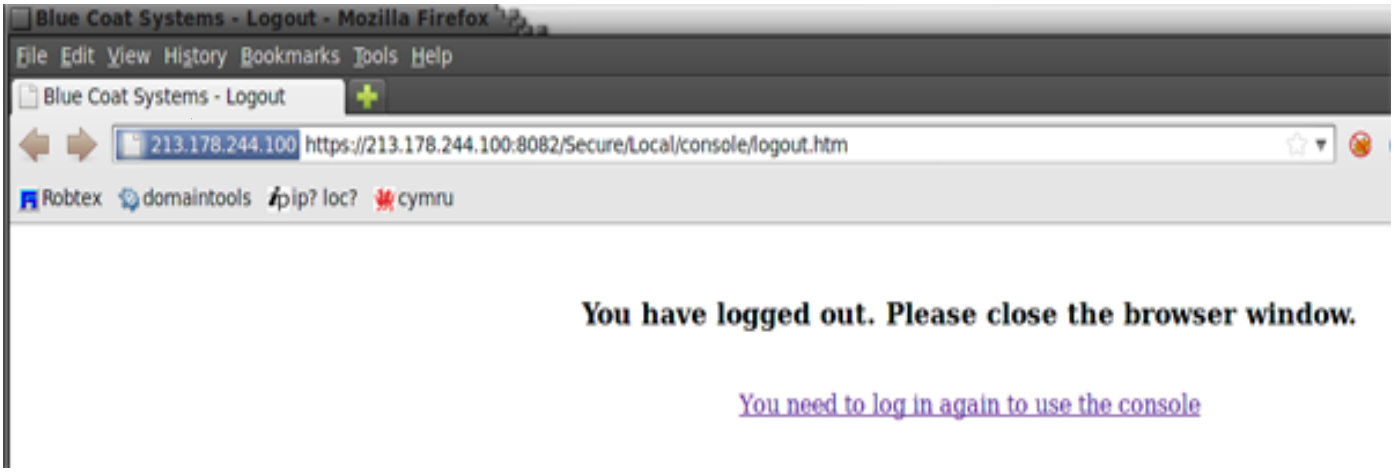

Figure 2: “Blue Coat Systems” displayed in logout screen of device on SCS IP address [213.178.244.100]

The HTTP headers also identified these as Blue Coat devices (figure 3).

```
https://213.178.244.175:8082/Secure/Local/console/logout.htm

GET /Secure/Local/console/logout.htm HTTP/1.1
Host: 213.178.244.175:8082

HTTP/1.0 200 OK
Server: BlueCoat-Security-Appliance
Pragma: no-cache
Cache-Control: no-cache
Set-Cookie: BCSI_MC=0:0; path=/
Set-Cookie: ; path=/
Content-Length: 432
Content-Type: text/html; charset=utf-8
-------------------------------------------------------
```

Figure 3: HTTP headers of Blue Coat device on SCS IP address [213.178.244.175]

The HTTP headers of one device identified it as a NetCache Appliance, a product line that was purchased by Blue Coat from Network Appliance in 2006 (figure 4). [20]

```
http://213.178.244.173:8081/

GET / HTTP/1.1
Host: 213.178.244.173:8081

HTTP/1.1 403 Forbidden
Date: Thu, 13 Oct 2011 08:47:52 GMT
Content-Length: 257
Content-Type: text/html
Server: NetCache appliance (NetApp/6.0.2)
-----------------------------------------
```

Figure 4: Device identified as a NetCache appliance on SCS IP address [213.178.244.173]

Given these findings, it is clear that there are more than 13 Blue Coat devices currently active in Syria.

This information also raises questions around Blue Coat's method of accounting for and tracking the presence of its devices in sanctioned countries. If the 13 devices referenced in Blue Coat's statement to the Wall Street Journal are in fact "transmitting automatic status messages back to the company," is it possible for Blue Coat to detect additional devices? If not, what explains the difference in the behaviour/visibility of these devices? Does Blue Coat intend to actively monitor for such devices in sanctioned countries in the future?

2. Possible obfuscation of Blue Coat devices

Citizen Lab research documented changes made in October 2011, to the names of Blue Coat devices, and traffic logs associated with these devices, which suggests an attempt to minimize information identifying usage of Blue Coat products in Syria. A publicly accessible network monitoring system on a Syrian Computer Society IP address displays usage statistics of devices identified as Blue Coat technology. Prior to October 18, 2011, this system identified a number of devices by name ("Blue Coat," "NetApp") on the IP addresses documented in the previous section of this brief and by other researchers.[21] Those names and IP addresses are as follows:

- BlueCoat 213.178.244.16
- BlueCoat 77.44.210.15
- BlueCoat 213.178.244.174
- BlueCoat 213.178.244.175
- BlueCoat 77.44.210.179
- NetApp 213.178.244.5
- NetApp 77.44.210.6

- NetApp 77.44.210.176
- NetApp 213.178.244.173
- BlueCoat 77.44.210.178

The traffic data displayed on this network monitoring system indicates that the devices had been in use since at least April 2011 (figure 5).

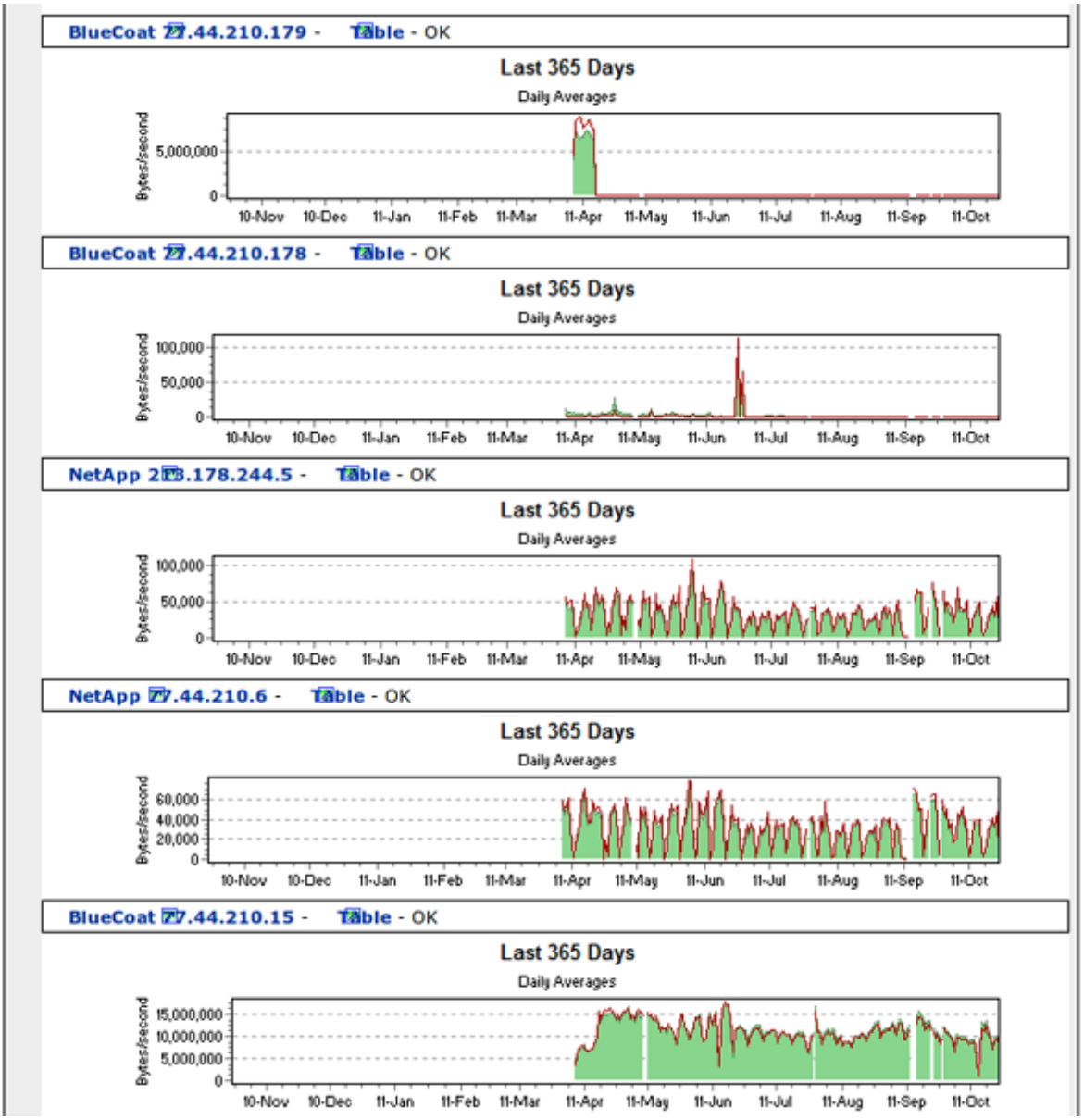

Figure 5: Traffic data from Syrian network monitoring system showing Blue Coat devices actively in use since April 2011.

A second traffic monitoring system found on another SCS IP address also listed a number of Blue Coat devices (figure 6).

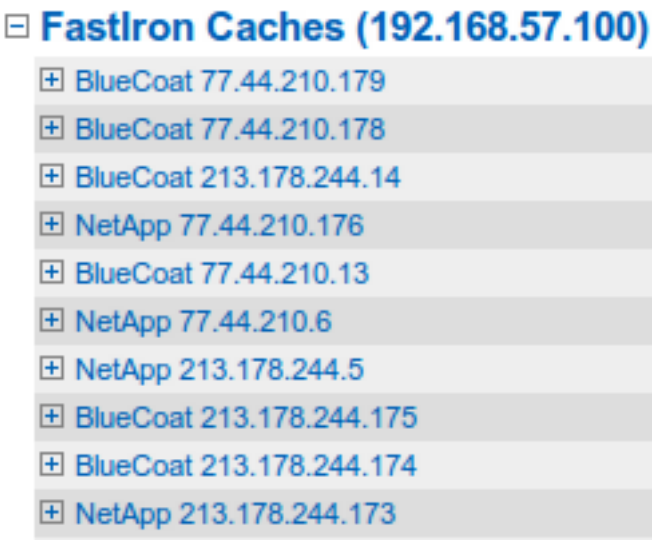

Figure 6: Additional list of devices found on an alternate network monitoring system

This list contains many of the same device names and IP addresses as the first list, with two additional IP addresses listed. The network monitoring system indicates that both of these devices are active, with traffic data dating back to September 2011 (figures 7 and 8).

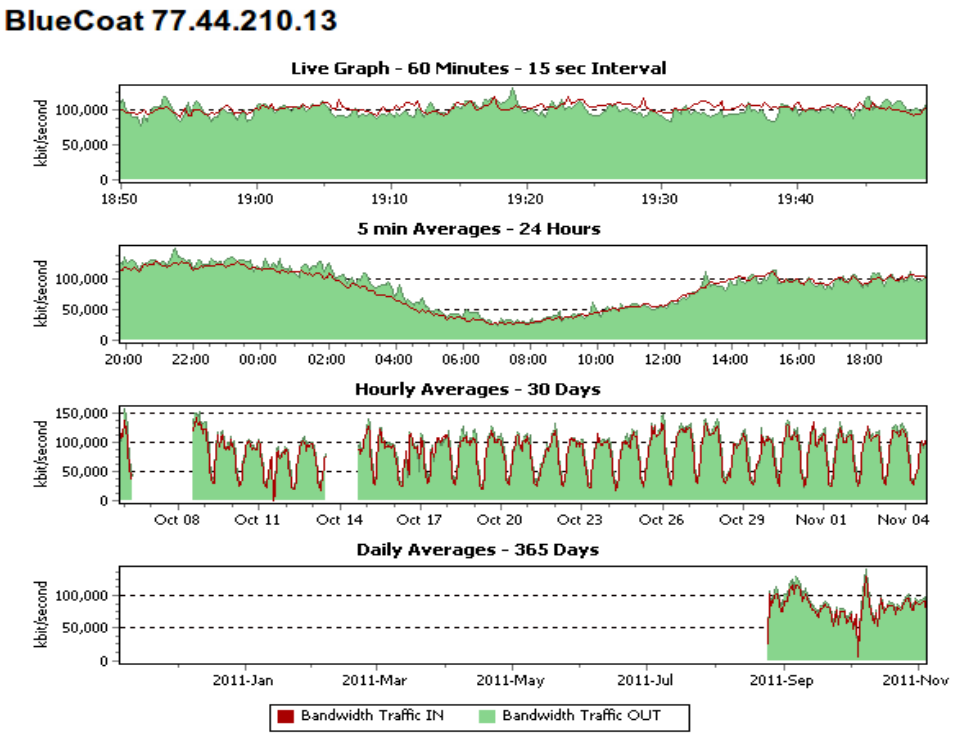

Figure 7: Traffic data displayed by network monitoring system

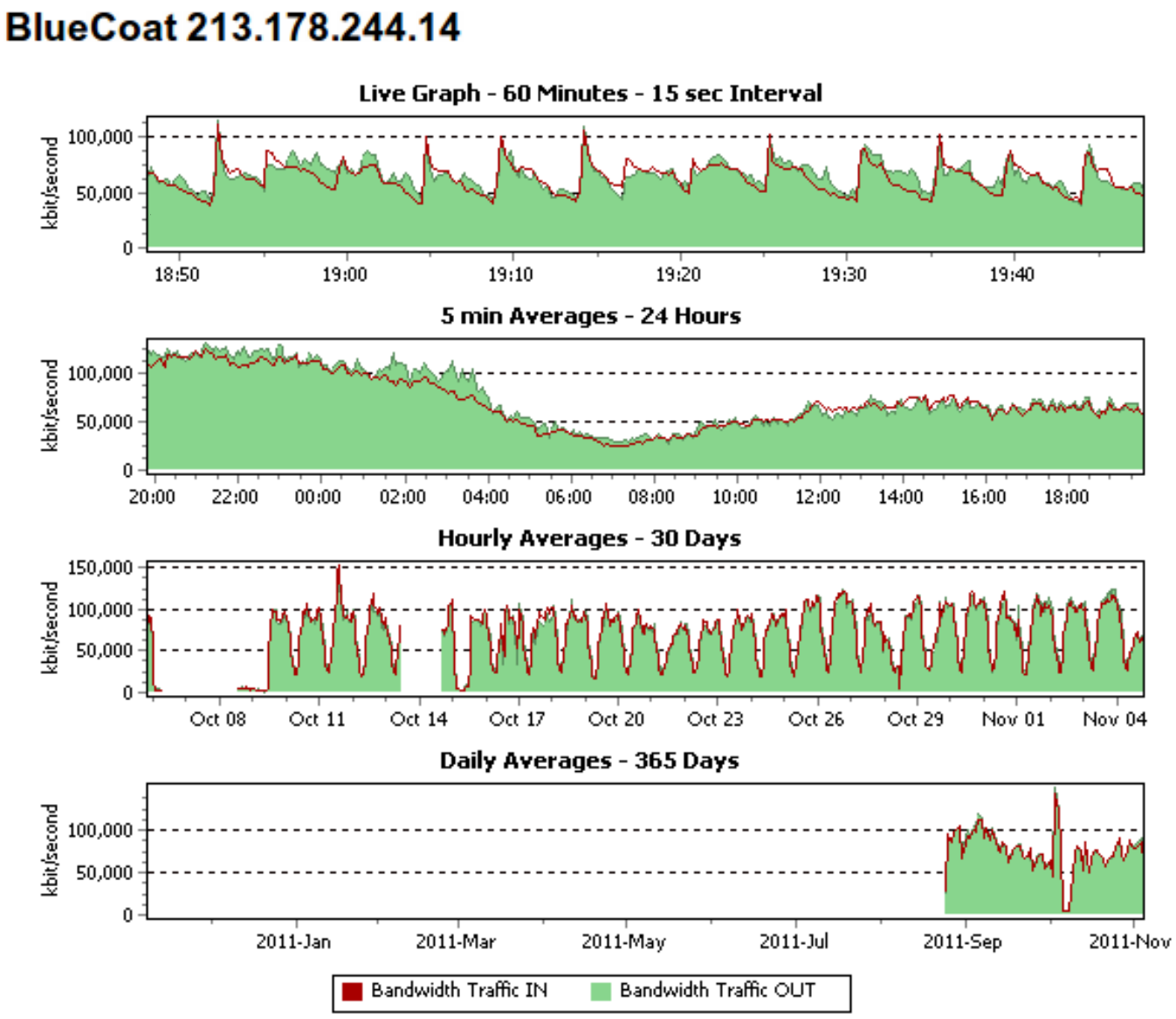

Figure 8: Traffic data displayed by network monitoring system

Interestingly, the device names displayed by the first monitoring system changed sometime between October 14 and 18, 2011. This name change occurred shortly after the October 4 release of logs from Blue Coat devices by the Telecomix group.[22] Several devices previously labeled as "BlueCoat" changed names to "Blue" or "Bue" (figure 9). Devices previously labeled as "NetApp," another Blue Coat product, were renamed to "Net."

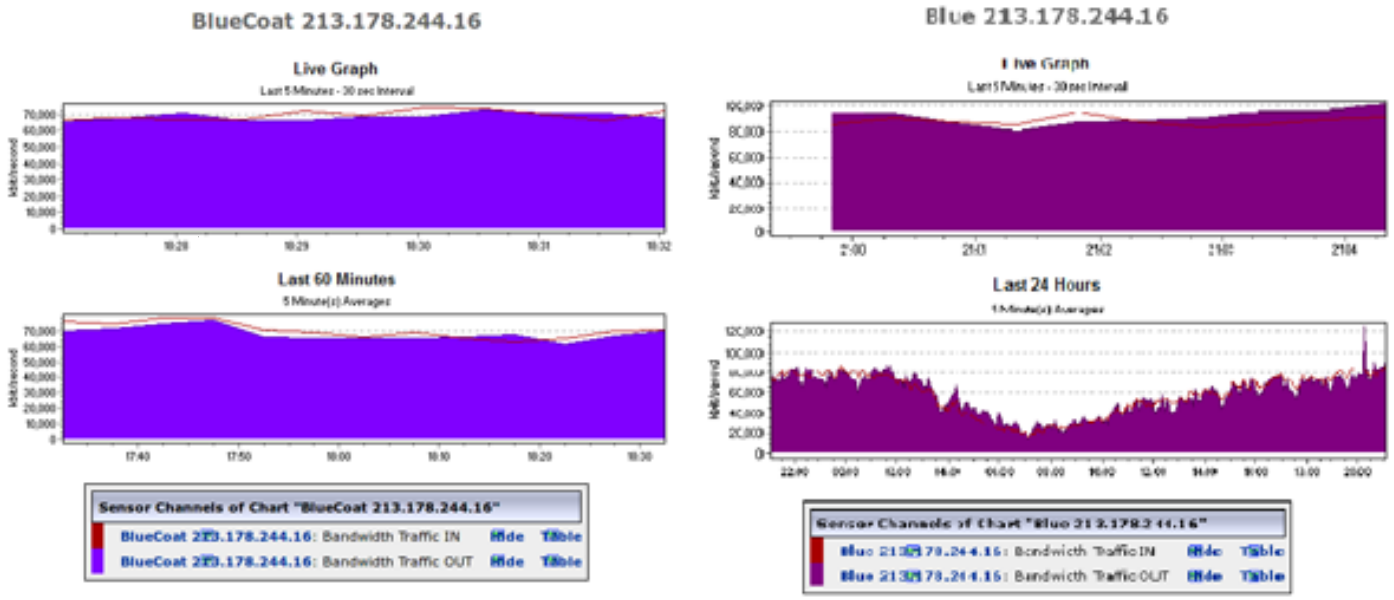

Figure 9: SCS Network Monitoring page. Image on left is before name change; image on right is after.

Further, all traffic data visible through the network monitoring system appears to have been removed in mid-October 2011. While traffic data had previously varied by device and dated as far back as February 2011, all devices now display traffic data beginning on October 17, 2011 (figure 10).

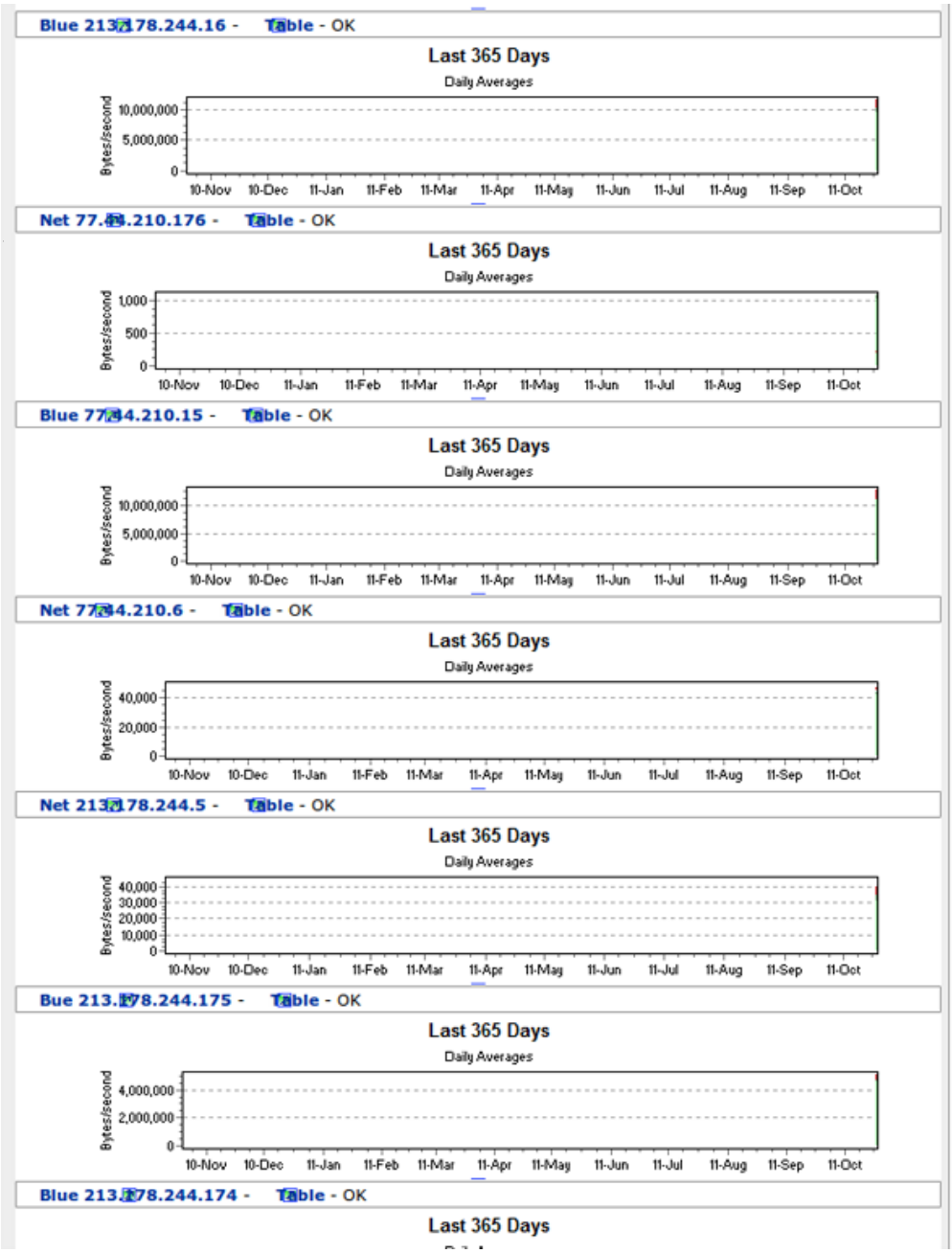

Figure 10: Traffic data on traffic monitoring system; data removed as of October 18, 2011. Compare to Figure 5.

The device names and traffic data on the second network monitoring system have not changed as of November 8, 2011.

The name change and removal of traffic data so soon after the release of data by Telecomix strongly suggests an attempt to obfuscate the presence of Blue Coat devices in Syria. While it is not clear who was responsible for these changes or why no further attempts to restrict access to this information were taken, it does suggest a deliberate attempt to conceal the presence of these devices.

3. Blue Coat devices used in Burma

Citizen Lab researchers have documented evidence that suggests Blue Coat devices are also used to filter Internet content in Burma.[23] The Burmese military junta is well-known for its serious human rights violations,[24] including its repressive tactics for Internet control and surveillance.[25] Burma is subject to U.S. sanctions as well, which (with certain exceptions) prohibit imports from, export or reexport of financial services to, and new investment in Burma.[26] Such sanctions demonstrate the U.S. government's intent to restrict economic activity that will support the Burmese regime. Accordingly, it is of significant concern that the evidence we have gathered suggests Blue Coat technology is also used in Burma to filter Internet traffic. Three pieces of evidence support this conclusion:

i. ISP hostnames match Blue Coat add-on names

Blue Coat's ProxySG appliances work with a variety of add-on features for additional functionality. These include "WebFilter," the tool used to filter web content; "Director," a web tool to manage a ProxySG deployment; "Reporter," a tool for reporting usage data; and "ProxyAV," a malware scanning and protection tool.[27]

Our research has found hostnames on the Yatanarpon Teleport domain, Burma's primary ISP, that directly match the names of several of these add-on features:

fw-webfilter.yatanarpon.net.mm (203.81.161.137)
bc-director.yatanarpon.net.mm (203.81.166.14)
reporter.yatanarpon.net.mm (203.81.166.16)
proxyav1.tlp.yatanarpon.net.mm (203.81.166.3)
proxyav2.tlp.yatanarpon.net.mm (203.81.166.4)[28]

The similarity of these hostnames to the names of Blue Coat products (including "BC Director") strongly suggests there is an installation of Blue Coat technology present on Yatanarpon's network.

ii. Network error page found in both Syria and Burma attributed to Blue Coat

ONI testing in Burma revealed that attempts to access some URLs, particularly those that are no longer active, received the message seen in figure 11:

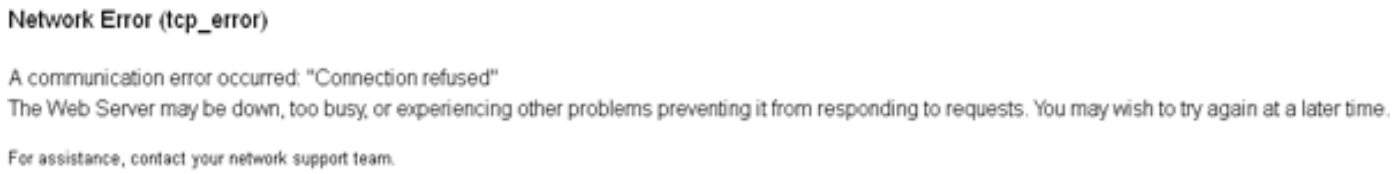

Figure 11: Error message received during ONI testing in Burma in August 2011.

This error message is nearly identical to one received as a result of tests run on the Syrian ISP SCS in October 2011, which uncovered the error page seen in figure 12:

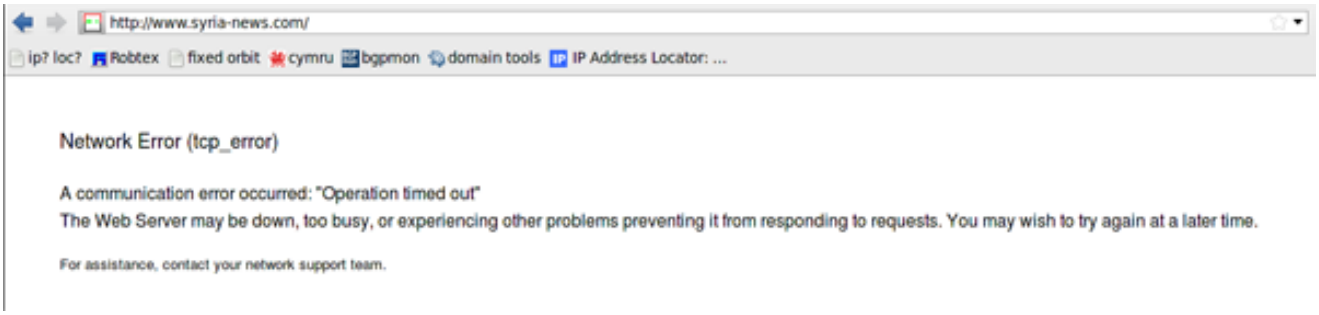

Figure 12: Network error page from SCS. Text is almost identical to error messages seen in Burma, shown in Figure 11.

There is evidence that this error message is generated by Blue Coat's ProxySG system. An entry on the Blue Coat support forums explaining how to modify error messages displayed by ProxySG devices identifies the exact text seen in figure 11 as the default message.[29]

Blue Coat's acknowledgement that its devices are being used in Syria, and its documentation indicating that this error message is generated by a Blue Coat device, lend support to the conclusion that Blue Coat devices are active in Burma.

iii. Correlation between ONI testing data and Blue Coat's categorization of URLs

Blue Coat's WebFilter filtering software works by assigning URLs to a variety of different categories, allowing system administrators the ability to block entire categories of content covering billions of URLs.[30] It is possible to identify the categorization of any given URL through the use of Blue Coat's publicly available Site Review website.[31] In total, Blue Coat groups all URLs into 82 different content categories.[32]

In August 2011, ONI conducted tests of Internet filtering on Yatanarpon Teleport in Burma following the methodology described earlier in this report. Of the 1,669 URLS tested, 500 of these URLs were determined to be blocked. The results of this testing in Burma were then correlated with Blue Coat's URL categorizations to explore which content categories were likely blocked by Yatanarpon Teleport. The Blue Coat categorization for all 1,669 URLs tested was obtained, and these categorizations were evaluated against URLs determined to be blocked in Burma.

URLs belonging to a total of 37 Blue Coat content categories were tested in Burma. Of these 37 categories, 10 categories appeared to be blocked entirely. Within these 10 categories, a total of 330 URLs were tested, with 326 (98.8%) of these URLs found to be blocked. Table 1 shows the 10 content categories that were suspected of being blocked entirely.

Blue Coat Category	**URLs found blocked**	**URLs found accessible**	**Percentage blocked**
Pornography	100	0	100%
LGBT	34	0	100%
Intimate Apparel/Swimsuit	29	0	100%
Sex Education	25	0	100%
Adult/Mature Content	24	0	100%
Nudity	11	0	100%
Malicious Outbound Data / Botnets	6	0	100%
Email	33	1	97.1%
Hacking	29	1	96.7
Proxy Avoidance	35	2	94.6%
Total	326	4	98.8%

Table 1: The proportion of URLs blocked in Burma belonging to 10 categories suspected of blocking

The strong correlation between Blue Coat's categorization of these URLs and those URLs found blocked during ONI testing provides further evidence that Blue Coat's devices are actively used to filter Internet content in Burma. While not definitive, it is unlikely that this correlation would be as strong were Burma to use an alternative filtering system.

It is not clear why four URLs belonging to these 10 categories were not found to be blocked in ONI testing. There are several explanations. First, past testing by ONI has found blocking on this ISP to be intermittent and inconsistent; it is possible that these instances were simply the result of random error.

Second, two of these four URLs used HTTPS rather than HTTP, and no HTTPS URLs were found to be blocked in ONI testing. Anecdotal reports from Burmese Internet users have suggested that the HTTPS version of many sites are not blocked in the country, providing an easy method of circumvention.[33] It is thus possible that these two URLs were accessible because no HTTPS URLs are blocked in Burma, although further testing would be required to confirm this.

Third, systems administrators are able to adjust blocking settings to supplement lists of blocked URLs. For example, an independent Burmese news website based in Thailand, http://www.mizzima.com, is classified by Blue Coat as News/Media, a content category that was not found to be uniformly blocked in ONI testing. However, ONI testing did find this particular URL to be blocked, as it has been consistently since 2005.[34] While systems administrators may not block access to all URLs categorized as News/Media, they likely make exceptions for particular sites of interest. Thus, it is possible that some of the aberrations seen in Table 1 reflect manual adjustments to what is or is not blocked within a particular content category.

Lastly, it is possible that Yatanarpon is using an alternate filtering system and this correlation with Blue Coat categories is merely a reflection of different filtering systems blocking similar content. Determining this more definitively would require testing of a much larger sample size and additional content from categories suspected of blocking. Although this type of additional testing has not yet been conducted, we believe that the existing correlation shown with this smaller sample size, combined with the additional technical evidence mentioned, makes a strong case that Blue Coat's devices are used in Burma.

QUESTIONS FOR BLUE COAT

The findings outlined in this brief raise a number of additional questions about the use of Blue Coat technology in Syria and Burma. Such questions include:

- Is Blue Coat aware of the use of their products and/or services in Burma/Myanmar?
- If so, has Blue Coat taken any steps to restrict the functionality of those devices?
- Has Blue Coat identified any Blue Coat products or services being used in Syria outside of the 13 already identified?

- In light of these recent findings, will Blue Coat actively monitor the devices that contact its servers to prevent Blue Coat technology from being used in embargoed countries?
- If Blue Coat forbids its resellers from selling to embargoed countries, what actions will Blue Coat take with respect to the reseller who brought the 13 devices identified by Blue Coat to Syria?
- Does Blue Coat have a policy for evaluating the sale of products and services to government, government-controlled or government-affiliated entities that engage in filtering of political content? If so, will Blue Coat share that policy?

The Citizen Lab strongly urges Blue Coat to investigate the additional findings presented in this brief, and to take all necessary steps to limit the functionality of Blue Coat devices located in Syria and Burma.

Acknowledgments: The Citizen Lab and OpenNet Initiative would like to thank two anonymous testers for their assistance in collecting data from Burma.

UPDATE: ARE BLUE COAT DEVICES IN SYRIA "PHONING HOME"? (JANUARY 2013)

Following the discovery of Blue Coat Systems networking devices in Syria, the company claimed in a statement that the devices are "not able to use Blue Coat's cloud-based WebPulse service" or "run the Blue Coat WebFilter database". Blue Coat also suggested that the devices are now "operating independently" and that the company does not have a "kill switch" to remotely disable the devices.Over the period of 3 weeks in July 2012, we tested this claim through the use of Blue Coat's Site Review process, which allows anyone to determine Blue Coat's categorization of a website. The experiment was based on the hypothesis that should a new website which had not been accessed anywhere but via a Syrian ISP be found to be categorized by Blue Coat, this could indicate the Syrian devices were "phoning home" to the company. Also, should a newly-created website which belongs to a Blue Coat category blocked in Syria be found to be blocked in that country, this could indicate the devices were receiving updates from Blue Coat.

As an experiment, three groups of domains were created (A, B and C) with newly registered, previously unused domain names. Each of the sites contained the same content, that of a proxy circumvention service. It is well established that Syria actively targets circumvention tools and services for filtering. The group A URLs were submitted to Blue Coat's Site Review process for analysis and within a day were identified as proxy sites. The group B URLs were accessed exclusively through a Syrian proxy and were found to be accessible. The group C URLs were left idle as a control.

Five days following the categorization of the group A URLs, these URLs were checked through a Syrian proxy and found to be accessible. This suggests that either the Blue Coat devices in Syria did not receive these updates or that the Syrian proxy used for testing was not on a network which uniformly blocked the "Proxy Avoidance" category.

Fourteen days after the group B URLs were accessed from Syria, their categorization was identified through the Site Review process. All URLs in this group were found to not have been categorized. This result suggests that the Syrian devices did not send any information about the group B URLs back to Blue Coat.

Interestingly, attempts to access a number of Blue Coat related web domains from Syria also failed. Using both a publicly available proxy and a privately operated proxy in Syria, a number of domains related to Blue Coat (www.bluecoat.com, cfauth.com, bluecoat.com.tw and k9webprotection.com) were found to be inaccessible in all tests. These domains were previously accessible through the same proxies prior to the release of this report.

While these experiments are not definitive, they do suggest that Blue Coat devices in Syria are not 'phoning home' to the company's servers in California and further, that Blue Coat may have blocked traffic on Syrian ISPs from accessing its websites.

FOOTNOTES

[1] Amnesty International, "Syria - Annual Report 2011," http://www.amnesty.org/en/region/syria/report-2011; Human Rights Watch, "Syria's human rights crisis: Myths and realities," August 24, 2011, http://www.hrw.org/news/2011/08/24/syria-s-human-rights-crisis-myths-and-realities

[2] Blue Coat Systems, "Largest companies in the world rely on Blue Coat solutions," October 12, 2011, http://www.bluecoat.com/company/press-releases/largest-companies-world-rely-blue-coat-solutions; Blue Coat, "ProxySG Addons," http://www.bluecoat.com/products/proxysg/addons.

[3] Reflets.info, "Web censorship technologies in Syria revealed," August 12, 2011, http://reflets.info/opsyria-web-censorship-technologies-in-syria-revealed-en/

[4] Reflets.info, "Bluecoat's role in Syria censorship and nationwide monitoring system," September 1, 2011, http://reflets.info/bluecoats-role-in-syrian-censorship-and-nationwide-monitoring-system/

[5] Horwitz, S., "Syria using American software to censor Internet, experts say," Washington Post, October 23, 2011, http://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-internet-experts-say/2011/10/22/gIQA5mPr7L_story.html

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

[7] Espiner, T., "Blue Coat web filtering technology 'used by Syria', ZDNet, September 5, 2011, http://www.zdnet.co.uk/blogs/security-bullet-in-10000166/blue-coat-web-filtering-technology-used-by-syria-10024276/

[8] Horwitz, S., "Syria using American software to censor Internet, experts say," Washington Post, October 23, 2011, http://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-internet-experts-say/2011/10/22/gIQA5mPr7L_story.html

[9] Horwitz, S.i, "Syria using American software to censor Internet, experts say," Washington Post, October 23,

2011, http://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-internet-experts-say/2011/10/22/gIQA5mPr7L_story.html

[10] Valentino-Devries, J., Sonne, P. and N. Malas, 'U.S. firm acknowledges Syria uses its gear to block web," Wall Street Journal, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

[11] Valentino-Devries, J., Sonne, P. and N. Malas, 'U.S. firm acknowledges Syria uses its gear to block web," Wall Street Journal, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

[12] Valentino-Devries, J., Sonne, P. and N. Malas, 'U.S. firm acknowledges Syria uses its gear to block web," Wall Street Journal, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

[13] The ONI 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). Some of the research in this brief was carried out under the auspices of the ONI.

[14] OpenNet Initiative, "West censoring East: The use of Western technologies by Middle East censors", 2011, http://opennet.net/sites/opennet.net/files/ONI_WestCensoringEast.pdf

[15] Faris, R. and N. Villeneuve, "Measuring Global Internet Filtering" in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, (eds)., Access Denied: The Practice and Policy of Global Internet Filtering, (Cambridge: MIT Press) 2008. http://opennet.net/sites/opennet.net/files/Deibert_02_Ch01_005-028.pdf

[16] Blue Coat, "Web Page Review Process," https://sitereview.bluecoat.com/sitereview.jsp

[17] For a further discussion of methods and ethics in cyberspace research, see Deibert, R. and M. Crete-Nishihata, "Blurred Boundaries: Probing the ethics of cyberspace research," 2011, Review of Policy Research, Vol. 28, No. 5, pp. 531-537.

[18] Valentino-Devries, J., Sonne, P. and N. Malas, 'U.S. firm acknowledges Syria uses its gear to block web," Wall Street Journal, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

[19] Reflets.info, "BlueCoat's presence in Syria finally uncovered," October 29, 2011, http://reflets.info/bluecoats-presence-in-syria-finally-uncovered/

[20] Blue Coat Systems, "Blue Coat completed acquisition of NetCache assets from Network Appliance," September 11, 2006, http://www.bluecoat.com/company/press-releases/blue-coat-completes-acquisition-netcache-assets-network-appliance

[21] Reflets.info, "Bluecoat's role in Syrian censorship and nationwide monitoring system," September 1, 2011, http://reflets.info/bluecoats-role-in-syrian-censorship-and-nationwide-monitoring-system/

[22]Telecomix: Syria, October 4, 2011, http://tcxsyria.ceops.eu/

[23] Past ONI research has documented the use of Fortinet technology in Burma. See Villeneuve, N., "Fortinet for who?", October 13, 2005, http://www.nartv.org/2005/10/13/fortinet-for-who/

[24] Human Rights Watch, "Burma's continuing human rights challenges," November 3,

2011, http://www.hrw.org/node/102763

[25] OpenNet Initiative, "Burma," December 22, 2010, http://opennet.net/research/profiles/burma

[26] See U.S. Department of the Treasury, "Burma Sanctions," http://www.treasury.gov/resource-center/sanctions/Programs/pages/burma.aspx

[27] Blue Coat, "Products," http://www.bluecoat.com/products

[28] http://www.robtex.com/cnet/203.81.166.html

[29] Blue Coat, "Solutions: How to add the server name to an exception," September 1, 2009, https://kb.bluecoat.com/index?page=content&id=KB3349&actp=LIST

[30] Blue Coat, "WebFilter" http://www.bluecoat.com/products/proxysg/addons/webfilter

[31] Blue Coat, "Web page review process," https://sitereview.bluecoat.com/sitereview.jsp

[32] Blue Coat, "Blue Coat Category Descriptions," https://sitereview.bluecoat.com/catdesc.jsp

[33] Floss Manuals, "Bypassing Internet censorship," http://en.flossmanuals.net/bypassing-censorship/ch010_simple-tricks/; Today in Myanmar, "Gmail, Yahoo Mail and Myanmar," http://www.myanmar2day.com/myanmar-life/2009/01/gmail-yahoo-mail-and-myanmar/

[34] OpenNet Initiative, "Pulling the plug: A technical review of the Internet shutdown in Burma," http://opennet.net/research/bulletins/013