UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

*Join the Global Conversation*

**The Citizen Lab**

**Research Brief**
Number 13 – January 2013

# *Planet Blue Coat:*

# *Mapping Global Censorship and Surveillance Tools*

The following individuals contributed to this report:
**Morgan Marquis-Boire** (lead technical research) and **Jakub Dalek** (lead technical research), **Sarah McKune** (lead legal research), **Matthew Carrieri**, **Masashi Crete-Nishihata**, **Ron Deibert**, **Saad Omar Khan**, **Helmi Noman**, **John Scott-Railton**, and **Greg Wiseman**.

Read The New York Times article associated with this report.

## SUMMARY OF KEY FINDINGS

- Blue Coat Devices capable of filtering, censorship, and surveillance are being used around the world. During several weeks of scanning and validation that ended in January 2013, we uncovered 61 Blue Coat ProxySG devices and 316 Blue Coat PacketShaper appliances, devices with specific functionality permitting filtering, censorship, and surveillance.

- 61 of these Blue Coat appliances are on public or government networks in countries with a history of concerns over human rights, surveillance, and censorship (11 ProxySG and 50 PacketShaper appliances). We found these appliances in the following locations:

  - **Blue Coat ProxySG:** Egypt, Kuwait, Qatar, Saudi Arabia, the United Arab Emirates.

  - **PacketShaper:** Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela.

- Our findings support the need for national and international scrutiny of Blue Coat implementations in the countries we have identified, and a closer look at the global proliferation of "dual-use" information and communication technologies. Internet service providers responsible for these deployments should consider publicly clarifying their function, and we hope Blue Coat will take this report as an opportunity to explain their due diligence process to ensure that their devices are not used in ways that violate human rights.

## PART I: BACKGROUND AND CONTEXT

Blue Coat Systems is a California-based provider of network security and optimization products. These products include: ProxySG devices that work with WebFilter,[1] which categorizes web pages to permit filtering of unwanted content; and PacketShaper, a cloud-based network management device that can establish visibility of over 600 web applications and control undesirable traffic.[2] ProxySG provides "SSL Inspection" services to solve "…issues with intercepting SSL for your end-users."[3] PacketShaper is integrated with WebPulse, Blue Coat Systems' real-time network intelligence service that can filter application traffic by content category.[4] Blue Coat Systems states that it "provides products to more than 15,000 customers worldwide,"[5] and indeed, it maintains offices globally, including in Latin America, the Middle East, and the Asia Pacific region.[6]

In 2011, researchers (including a team from the Citizen Lab) found evidence of the use of Blue Coat Systems products in Syria. These findings raised concerns that Blue Coat products were being used as part of the network filtering and monitoring apparatus of the Syrian government, known for its violations of human rights and widely condemned crackdown against ongoing domestic opposition. In such provision of secure web gateway and filtration products, Blue Coat Systems exemplifies the manufacture and service of so-called "dual use" technology: information and communication technology (ICT) that may equally serve legitimate and positive purposes, or purposes resulting in adverse impact on human rights, depending on its deployment or particular "end use."[7]

In August 2011, the website Reflets.info, in collaboration with Telecomix and Fhimt.com, began to release a series of blog posts concerning the use of Blue Coat Systems devices in Syria.[8] Reflets.info documented the

[1] "WebFilter," Blue Coat, http://www.bluecoat.com/products/proxysg/addons.
[2] Blue Coat PacketShaper Application List," Blue Coat, http://www.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf.
[3] "The Growing Need for SSL Inspection", Blue Coat, https://www.bluecoat.com/security/security-archive/2012-06-18/growing-need-ssl-inspection.
[4] "PacketShaper," Blue Coat, http://www.bluecoat.com/products/packetshaper.
[5] http://www.bluecoat.com/products/packetshaper.
[6] "Company," Blue Coat, http://www.bluecoat.com/company.
[7] Some ISPs in the Middle East and North Africa and other regions in the developing world deploy Blue Coat Systems appliances such as Blue Coat CacheFlow mainly to reduce bandwidth costs, which tend to be expensive in these countries. Lebanon Online for example is one of the region's ISPs using Blue Coat CacheFlow for this purpose. "Lebanon Online Deploys Blue Coat CacheFlow Appliance to Reduce Bandwidth Costs and Enhance End-User Experience," Blue Coat, August 15, 2011, http://www.bluecoat.com/company/press-releases/lebanon-online-deploys-blue-coat-cacheflow-appliance-reduce-bandwidth-costs.
[8] "Web Censorship Technologies in Syria Revealed," Reflets.info, August 12, 2011, http://reflets.info/opsyria-web-censorship-technologies-in-syria-revealed-en.

presence of Blue Coat devices through in-country testing done in collaboration with Telecomix,[9] and in October 2011, Telecomix released 54 gigabytes of data purportedly consisting of Syrian censorship log files collected from Blue Coat devices active in Syria.[10]

Initially, Blue Coat Systems denied that its equipment had been sold to Syria,[11] a country subject to US sanctions.[12] Soon after, however, Blue Coat Systems acknowledged that at least thirteen of its devices were active in Syria and that these devices had been communicating with Blue Coat Systems-controlled servers. In October 2011, the company told the *Wall Street Journal* that it had shipped the devices to a distributor in Dubai, believing that they were destined for the Iraqi Ministry of Communications.[13]

In November 2011, following Blue Coat Systems' admission, Citizen Lab researchers documented the use of Blue Coat Systems commercial filtering products in both Syria and Burma, in the report *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma*.[14] Employing network scans of publicly accessible servers in the IP address ranges of the Syrian Telecommunications Establishment, the Citizen Lab report identified devices in Syria not previously identified in the first Reflets and Telecomix release. In the case of Burma, the findings were gathered on the basis of data gathered from in-country field testing and research.[15]

Blue Coat Systems soon announced in a statement that it was no longer "providing support, updates or other services" to its ProxySG appliances in Syria. The company stated that its devices in Syria were no longer "able to use Blue Coat's cloud-based WebPulse service" or "run the Blue Coat WebFilter database" and were now "operating independently." Blue Coat Systems added they did not have a "kill switch" to remotely disable the devices.[16] An experiment conducted by Citizen Lab researchers, over a period of three weeks in July 2012, revealed evidence that suggests Blue Coat devices in Syria were no longer 'phoning home' to Blue Coat Systems' servers. Citizen Lab also found that many Blue Coat Systems domains were being blocked in Syria, perhaps to prevent existing devices from receiving updates.[17]

[9] Blue Coat's Role in Syria Censorship and Nationwide Monitoring System," Reflets.info, September 1, 2011, http://reflets.info/bluecoats-role-in-syrian-censorship-and-nationwide-monitoring-system.

[10] #OpSyria: Syrian Censorship Logs (Season 3)," Reflets.info, October 4, 2011, http://reflets.info/opsyria-syrian-censoship-log.

[11] Sari Horwitz, "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.

[12] See U.S. Executive Order 13582, which prohibits "the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any services to Syria." *Executive Order 13582: Blocking Property of the Government of Syria and Prohibiting Certain Transactions With Respect to Syria*, August 17, 2011, at Sec. 2(b), available at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_eo_08182011.pdf.

[13] Nour Malas, Paul Sonne, and Jennifer Valentino-Devries, "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web," *Wall Street Journal*, October 29, 2011, http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.

[14] "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma," Citizen Lab, November 9, 2011, https://citizenlab.org/2011/11/behind-blue-coat; and "Behind Blue Coat: An Update from Burma," Citizen Lab, November 29, 2011, https://citizenlab.org/2011/11/behind-blue-coat-an-update-from-burma.

[15] "Behind Blue Coat: An update from Burma."

[16] "Update on Blue Coat Devices in Syria," Blue Coat Systems, December 15, 2011, http://www.bluecoat.com/update-blue-coat-devices-syria.

[17] For details see "Update: Are Blue Coat Devices Phoning Home?" Citizen Lab, https://citizenlab.org/2011/11/behind-blue-coat/#update.

The US Department of Commerce launched an investigation to determine whether Blue Coat Systems had prior knowledge of the use of its equipment in Syria.[18] The investigation was launched following a call from US Senators requesting an investigation into Blue Coat Systems and NetApp, another US company whose equipment had been implicated in Syria's surveillance system as detailed by Bloomberg shortly before the publication of Citizen Lab's Blue Coat reports.[19] In December 2011, the US Department of Commerce's Bureau of Industry and Security (BIS) added one individual and one company based in the United Arab Emirates to its Entity List for purchasing US commercial filtering products from Blue Coat and exporting the products to Syria.[20]

## PART II: FINGERPRINTING THE GLOBAL NETWORK OF BLUE COAT SYSTEMS DEVICES

### A: Methodology

This project set out as an effort to understand the widespread nature and geographic spread of Blue Coat Systems' commercial filtering and traffic inspection products, using several techniques to identify Blue Coat devices. It is not intended to provide an exhaustive enumeration of all Blue Coat hosts on the Internet.

From December 2012 to mid-January 2013, we used the Shodan Computer Search Engine to search for Blue Coat PacketShaper and Blue Coat ProxySG hosts.[21] Results from the Shodan Computer Search Engine were subsequently verified by scanning[22] and followed by manual inspection. In addition to surveying Shodan for Blue Cost hosts, we undertook substantial whole-country scanning from hosts in Europe and the US.

Our investigation yielded a significant number of hosts identifying themselves in ways that indicated they were a Blue Coat device, including Telnet and FTP banners, specific HTML pages, and so on. Because of our primary interest in devices that could be used for surveillance, filtering, and censorship, we narrowed in on PacketShaper and ProxySG Blue Coat appliances. We then worked through the results of our initial scanning, and excluded many devices from our final analysis that could not be identified with high confidence as PacketShaper and ProxySG appliances.

[18] Shyamantha Asokan, "U.S. Probing Use of Surveillance Technology in Syria," *Washington Post*, November 17, 2011, http://articles.washingtonpost.com/2011-11-17/world/35283442_1_blue-coat-systems-syrian-government-syrian-president-bashar.

[19] Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," *Bloomberg*, November 3, 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.

[20] BIS Adds Two Parties to Entity List for Sending Internet Filtering Equipment to Syria," U.S. Department of Commerce Bureau of Industry and Security, December 15, 2011, http://www.bis.doc.gov/news/2011/bis_press12152011.htm.

[21] The Shodan search engine provides information on devices connected to the Internet, including industrial control systems, web filtering, and network security and optimization products. See: http://www.shodanhq.com/help/tour.

[22] Nmap (network mapper) was the primary scanning tool used in surveying large parts of the global internet. See http://nmap.org.

The installations included in the final report met the following criteria: (1) a Blue Coat Systems ProxySG or PacketShaper device on what we think is a public network (i.e. not a private company), (2) located in a country that is the subject of ongoing concern over compliance with international human rights law, legal due process, freedom of speech, surveillance, and censorship.

## B: Results

The scanning and validation process yielded 61 Blue Coat ProxySG devices and 316 Blue Coat PacketShaper devices located all over the world. Of these, we identified 11 ProxySG and 50 PacketShaper devices on public or government networks in countries with a history of concerns over human rights, surveillance, and censorship. These hosts were present on either government networks or on netblocks associated with telecommunication companies that provide Internet access of some sort. Specific efforts were made to exclude devices we believed to be on health, education, or commercial networks not associated with providing Internet service or telecommunications. The only exception is a device we found on the "King Abdulaziz City for Science and Technology" network which, although it is an educational institution, is involved in the implementation of national filtering.[23]

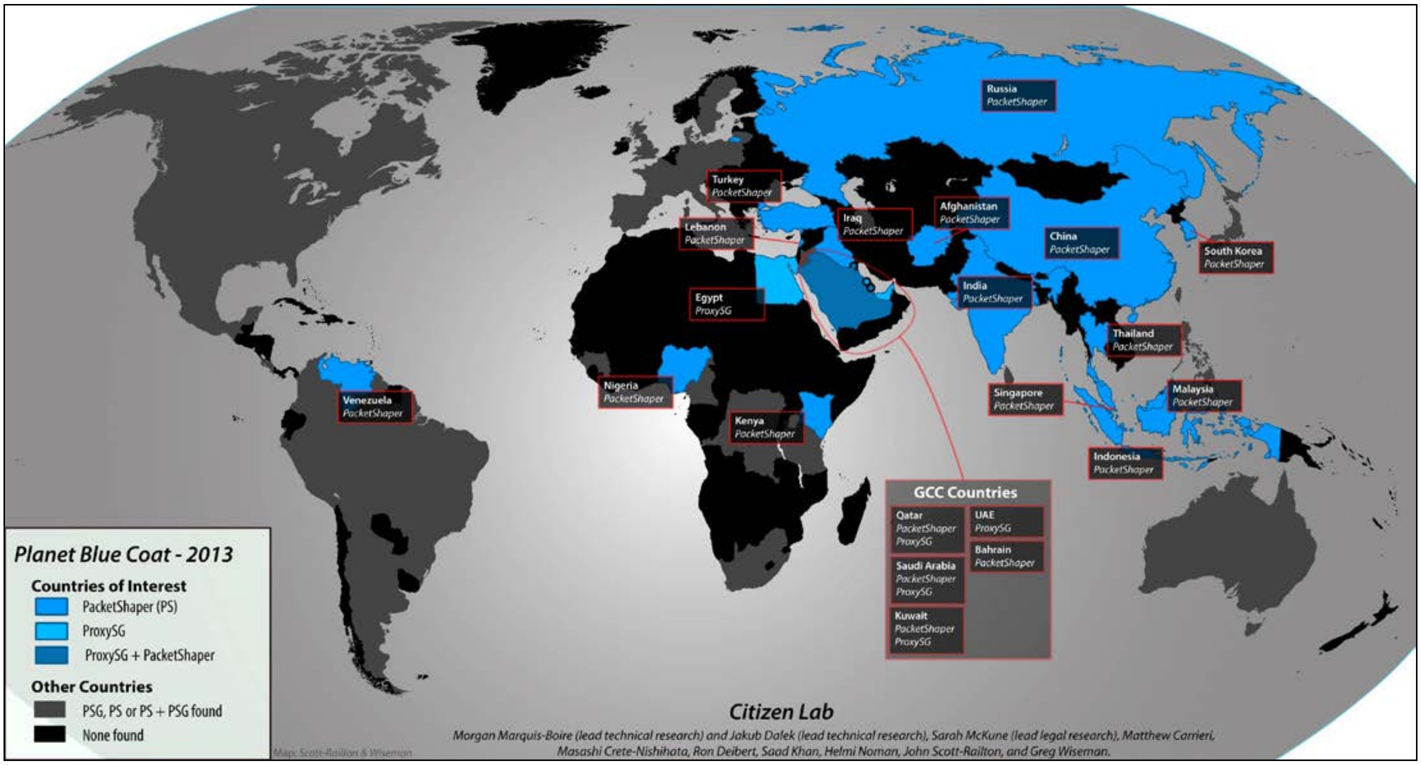
Hosts found to be used on health, education or commercial networks are included in the maps to display the widespread use of this technology, but will not be specifically discussed in this report.

We identified ProxySG installations in the following countries of interest: Egypt, Saudi Arabia, Kuwait, the United Arab Emirates, and Qatar. We have also noted that Shodan has reported Egyptian ISP Nile Online as having a ProxySG installation as recently as August 2012, although we were unable to identify it in our testing. Nevertheless, we have decided to include it in our results because of its recent detection by Shodan.

We discovered PacketShaper installations in the following countries of interest: Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela. We were able to visit these hosts and confirm that they were running the product. Bahrain is the only exception; however, Shodan has reported the presence of a PacketShaper installation as recently as December 31, 2012. This host was located on ASN named "BIX-AS Bahrain Internet Exchange." Using the service provided by iplocation.net, the IP in question was listed as being on an ISP named the "Central Informatics Organisation" by two data location companies: maxmind and db4.

[23] Introduction to Content Filtering," King Abdulaziz City for Science and Technology, Internet Services Unit, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm.

*ProxySG and PacketShaper deployments:*



**Map of BlueCoat worldwide deployments in countries of interest.**

(Basemap: Wikimedia Commons, Creative Commons License)
Graphics: John Scott-Railton & Greg Wiseman
View larger image or see page 18 for full page image.
View as PDF.
Explore the data further.

*A summary of data is available for download in a variety of formats:*
Google Doc:
https://docs.google.com/spreadsheet/pub?key=0AtJqKcMmUwTKdDRkU1BiMHc4UGdPaGtNWndiWm5RaEE&output=html
Excel: https://citizenlab.org/data/planetbluecoat_data.xlsx
CSV: https://citizenlab.org/data/planetbluecoat_data.csv

## C: Summary of Country Results

The countries featured in this report are a subset of the cases where we identified Blue Coat Systems filtering and monitoring products (ProxySG and PacketShaper) on public networks. We've focused on a subset of cases where our scanning identified Blue Coat devices in countries with widely-reported concerns over legal due process, human rights, and transparency, especially pertaining to filtering, censorship or surveillance. What emerged is a picture of the global spread of Blue Coat devices to countries where their presence raises substantial concerns. The picture varies across regions and between countries, and we think these are a natural topic for further research, especially as this pertains to our findings.

We found Blue Coat devices in all countries of the Gulf Cooperation Council except Oman (**Bahrain**, **Kuwait**, **Qatar**, **Saudi Arabia**, and **the United Arab Emirates**). These states all have well known and pervasive regimes of Internet content filtering, so the presence of Blue Coat filtering products is not surprising. In several cases it has already been reported on.[24]

The region is also experiencing massive growth in Internet penetration, triggering aggressive marketing efforts by Western technology companies, intent on accessing these new markets. Less well known, however, is the extent of domestic electronic surveillance regimes in these countries, particularly in light of crackdowns on domestic dissent in Bahrain and Saudi Arabia, and where the devices we found were in locations suggestive of national filtering.

The finding of a Blue Coat device in **Egypt** is noteworthy in light of the widespread condemnation of the Mubarak regime's use of electronic surveillance to monitor activists that came to light after the 2011 Revolution.[25] The Egyptian government has reportedly continued to acquire the means to filter and surveil its national Internet using Deep Packet Inspection, and has recently proposed new online content regulations.[26]

The case of Blue Coat products in **Lebanon** is interesting because, while the country does not have a history of Internet filtering,[27] the government has recently drafted online content regulations concerning public morals.[28] This makes Lebanon a good case for follow-up research to clarify the function of these devices.

**Iraq** and **Afghanistan** are especially noteworthy cases. As they undergo reconstruction, both countries are the subject of international concern and scrutiny for ongoing human rights abuses, including a trend towards greater regulation and criminalization of some aspects of free expression,[29] including freedom of the press.[30] Additional concerns have been raised over increasing pressure by these governments on ISPs

[24] Paul Sonne and Steve Stecklow. "U.S. Products Help Block Mideast Web." *Wall Street Journal*, March 27, 2011. http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html.

[25] "Egypt," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/egypt.

[26] "Freedom on the Net 2012: Egypt," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/egypt.

[27] "Lebanon," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/lebanon.

[28] Khodor Salameh, "Lebanese Internet Law Attacks Last Free Space of Expression," Al Akhbar, March 9, 2012, http://english.al-akhbar.com/node/4997.

[29] See, for example, Iraq's Information Crimes Law: "Iraq's Information Crimes Law: Badly Written Provisions and Draconian Punishments Violate Due Process and Free Speech," Human Rights Watch, July 12, 2012, http://www.hrw.org/sites/default/files/reports/iraq0712webwcover.pdf.

[30] World Report – Iraq," in Press Freedom Index 2011-2012, Reporters Without Borders, http://en.rsf.org/report-iraq,152.html.

to implement these controls and submit to monitoring requirements.[31] In both cases, Blue Coat products have the necessary features to help ISPs comply with these requests. The presence of these devices raises serious concerns about "surveillance-by-design" being built in from the ground up as the countries undergo reconstruction and expansion in telecommunications sectors.

In **China** we found several Blue Coat devices on a state-controlled ISP. The country is known for its comprehensive and multifaceted Internet filtering and surveillance regime, often referred to as the "Great Firewall."[32]

**Russia** and **Venezuela** are noteworthy because of serious concerns about the regimes in power, and their track record of using unlawful surveillance along with non-technical means to control political dissent and opposition.[33]

Elsewhere, **Turkey** has recently passed a series of laws empowering ISPs to filter a wide range of content,[34] and in **India**, government agencies are explicitly authorized to monitor and intercept Internet traffic and user information for purposes of national security or cyber security.[35]

The government of **South Korea**, despite its sophisticated telecommunications sector, has an extensive set of legal and technical mechanisms to control online content and expression, although the overall rate of filtering is low.[36] Meanwhile, the case of **Kenya** is also potentially interesting as the government is reportedly in the process of implementing a domestic monitoring apparatus.[37]

Blue Coat products emerged repeatedly in Southeast Asia, where technology sectors and Internet penetration are growing rapidly, and new forms of online activism pose challenges to ruling governments: **Malaysia** has a documented history of state control, regulation, and monitoring of online expression, and recent legislation in the country authorizes warrantless interception with a vaguely defined scope.[38] **Thailand** engages in widespread Internet filtering and blocking, supplemented with substantial non-

[31] In Afghanistan: Danny O'Brien and Bob Dietz, "Using New Internet Filters, Afghanistan Blocks News Site," *Yahoo! Business and Human Rights Program*, October 6, 2010, http://www.yhumanrightsblog.com/blog/2010/10/12/using-new-internet-filters-afghanistan-blocks-news-site/.

[32] "China," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/china.

[33] Andrei Soldatov and Irina Borogan,"The Kremlin's New Internet Surveilance Plan Goes Live Today," Wired, November 1, 2012, http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/; and "Countries Under Surveillance – Venezuela," Reporters Without Borders, http://en.rsf.org/surveillance-venezuela,39770.html.

[34] "Freedom on the Net 2011: Turkey," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/turkey.

[35] *Information Technology (Amendment) Act 2008*, http://www.mit.gov.in/sites/upload_? les/dit/? les/downloads/itact2000/it_amendment_act2008.pdf.

[36] See: "South Korea," OpenNet Initiative, August 6, 2012, http://opennet.net/research/profiles/south-korea.

[37] Okuttah Mark, "CCK Sparks Row with Fresh Bid to Spy on Internet Users," *Business Daily*, March 20, 2012, http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/item/2/-/edcfmqz/-/index.html; and Winfred Kagwe, "Kenya: CCK Defends Plan to Monitor Private Emails," *All Africa*, May 17, 2012, http://allafrica.com/stories/201205181170.html.

[38] "Freedom on the Net 2012: Malaysia," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/malaysia; and "Malaysia: Security Bill Threatens Basic Liberties," Human Rights Watch, April 10, 2012, http://www.hrw.org/news/2012/04/10/malaysia-security-bill-threatens-basic-liberties.

technical legal mechanisms.[39] Currently, the Thai government is extending its ability to engage in surveillance and monitoring, explicitly for the purpose of unmasking those engaging in speech critical of the monarchy.[40]

**Indonesia** employs widespread but inconsistent filtering that emphasizes blocking content featuring some sexual, gender, and religious themes, and access to circumvention tools.[41] With respect to **Singapore**, which implements limited Internet filtering, but has broad general censorship focused on potentially divisive racial, political, or religious content, a 2006 Privacy International report found that Singaporean law permits government surveillance of Internet activity and "grants law enforcement broad power to access data and encrypted material when conducting an investigation."[42]

A more complete overview of each of the countries of interest can be found in Appendix A.

## PART III: EXPORT OF DUAL USE AND COMMUNICATION TECHNOLOGIES—ETHICAL AND LEGAL CONSIDERATIONS

The geographic spread of Blue Coat Systems technology outlined above, including within countries that have presented significant human rights concerns, highlights the importance of addressing at a number of levels the expanding dual-use ICT sector. Blue Coat Systems is only one of many participants in this industry, which includes numerous types of technologies and services utilized by governments as well as private actors. With respect to the market for secure web gateway solutions alone—which primarily include filtering software and related products such as those of Blue Coat Systems—analysts estimated the size of the market at nearly US$1.2 billion in 2012, and recognized five market leaders (Blue Coat Systems, Cisco, McAfee, Websense, and Zscaler), all of which are companies based in the US.[43] Accordingly, the role of Western companies in providing dual-use technologies is a crucial subject for discussion among governments and policy makers, civil society, and the private sector. Such discussion is currently under way in a variety of fora, raising complex questions to which there are no simple solutions.

One of the key goals of the debates surrounding dual-use technologies is to determine a method of crafting effective controls on such technology that simultaneously limit its sale and deployment for purposes that negatively impact human rights, while protecting those uses that serve legitimate purposes and result in benefits to society. Such an approach requires an understanding of the likely end use of the technology in any given scenario, as well as carefully crafted legal and regulatory language to prevent over- or under-

[39] "Thailand," OpenNet Initiative, August 7, 2012, http://opennet.net/research/profiles/thailand.

[40] "Web Censor System Hits Protest Firewall," *Bangkok Post*, December 15, 2011, http://www.bangkokpost.com/learning/learning-from-news/270926/new-web-censorship-worries.

[41] "Indonesia," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/indonesia.

[42] Privacy International, "Chapter II. Surveillance Policy," *Singapore*, December 12, 2006, https://www.privacyinternational.org/reports/singapore/ii-surveillance-policy.

[43] Lawrence Orans and Peter Firstbrook, "Magic Quadrant for Secure Web Gateways," Gartner Inc., May 24, 2012, available at http://www.gartner.com/technology/research/methodologies/magicQuadrants.jsp.

inclusiveness by companies when assessing whether particular products and services fall within the scope of controls.

For example, the Electronic Frontier Foundation (EFF) has warned of potential problems with legislation that is based on pre-defining *types of technology* "because broadly written regulations could have a net negative effect on the availability of many general-purpose technologies and could easily harm the very people that the regulations are trying to protect."[44] The EFF points out that legal terms to define harmful technology could encompass basic technologies such as web browsers, and would result in denying citizens of the use of basic technologies.[45] Therefore, rather than focusing on the technology, the EFF advocates for a "Know Your Customer" approach, encouraging companies to investigate a customer before and during a transaction.[46]

Government use of sanctions to control the flow of dual-use and other sensitive technologies to repressive regimes has run up against this dilemma. For example, while US sanctions against Iran and Syria restrict the sale by US companies of most goods and services to these countries, in order to support freedom of expression and access to information among the Iranian and Syrian populations, the US has found it necessary to issue general licenses enumerating that some (but not all) services related to Internet-based communications and telecommunications are authorized.[47] Yet companies providing such services have in many instances erred on the side of caution and avoided providing technologies that would serve legitimate ends within these two countries altogether, given the possibility of significant penalties and reputational damage should they be found in violation of the sanctions.[48] This collateral effect of the sanctions has had the unintended consequence of pitting US goals regarding isolation of authoritarian regimes and promotion of Internet freedom against each other. The need for precise, strategic language surrounding controlled technologies was reiterated in the US State Department's November 2012 call for comments on its draft "Guidance on the

[44] Trevor Timm, "Time to Act on Companies Selling Mass Spy Gear to Authoritarian Regimes," Electronic Frontier Foundation, February 7, 2012, https://www.eff.org/deeplinks/2012/02/time-act-companies-selling-mass-spy-gear-authoritarian-regimes.

[45] Trevor Timm, "Time to Act on Companies Selling Mass Spy Gear to Authoritarian Regimes," Electronic Frontier Foundation, February 7, 2012, https://www.eff.org/deeplinks/2012/02/time-act-companies-selling-mass-spy-gear-authoritarian-regimes.

[46] Cindy Cohn and Jillian C. York, "'Know Your Customer' Standards for Sales of Surveillance Equipment," Electronic Frontier Foundation, October 24, 2011, https://www.eff.org/deeplinks/2011/10/it's-time-know-your-customer-standards-sales-surveillance-equipment.

[47] See U.S. Department of the Treasury Office of Foreign Assets Control, "Iran: General License Related to Personal Communication Services," March 3, 2010, available at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/soc_net.pdf; United States Department of the Treasury Office of Foreign Assets Control, *Interpretive Guidance and Statement of Licensing Policy on Internet Freedom in Iran*, March 20, 2012, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/internet_freedom.pdf; "General License No. 5: Exportation of Certain Services Incident to Internet-Based Communications Authorized" (Syria), U.S. Department of the Treasury, August 18, 2011, available at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_gl5.pdf; United States Department of the Treasury Office of Foreign Assets Control, *General License No. 14: Transactions Related to Telecommunications Authorized (Syria)*, October 3, 2011, available at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_gl14.pdf.

[48] For examples, see Jillian C. York, "EFF Signs Joint Coalition Letter Urging Companies to be Proactive on Export Regulations," Electronic Frontier Foundation, June 27, 2012, https://www.eff.org/deeplinks/2012/06/eff-signs-joint-coalition-letter-urging-companies-be-proactive-export-regulations.

Provision of 'Sensitive Technology' to Iran and Syria," which concerns the scope of the term "sensitive technology" as utilized in the language of Iran and Syria sanctions.[49]

In addition to the matter of careful calibration of language to ensure clear and appropriate restrictions on dual-use technologies, is the matter of determining appropriate methods of control. While sanctions are perhaps one of the most potent methods of control given the significant penalties and policy interests at stake, their application is typically limited to those few countries that members of the international community generally agree represent threats to international order. Thus, the use of Blue Coat Systems technologies highlighted in this report is largely beyond the scope of sanctions, as, with the exception of certain limited sanctions applicable to Iraq[50] and Lebanon,[51] the countries in which Blue Coat Systems products were found are not currently subject to US sanctions—yet significant human rights concerns regarding the application of these technologies remain. Moreover, government entities involved in sanctions regimes that cover a wide variety of critical products and services, such as banking, petroleum products, insurance, etc., across multiple countries, may allocate a smaller percentage of their institutional resources to the matter of dual-use technologies, both in the drafting and enforcement of sanctions. Dual-use technologies employed in both the sanctioned and unsanctioned world therefore require further methods of attention, inquiry, and control.

Export control frameworks offer an additional method for control of dual-use technologies, if effectively adapted to the issue. Export controls generally restrict the transfer of products that are "dual use" in the classic sense of having both commercial and military application, in order to protect national security, though other products may be covered as well. At the international level, the Wassenaar Arrangement covers dual use goods and technologies in the US, Canada, European Union, and other countries with participating countries committing to maintain national export controls on listed items—which include items related to "telecommunications" (Category 5, Part 1) and "information security" (Category 5, Part 2).[52] Notably, the Wassenaar Arrangement served as grounds for the UK government to assert that FinFisher spyware reported

[49] "State Department Sanctions Information and Guidance," U.S. Department of State, November 8, 2012, http://www.state.gov/e/eb/tfs/spi/iran/fs/200316.htm.

[50] It must be noted that the United States have imposed limited sanctions on Iraq and Lebanon. In Iraq, the United States has placed "certain prohibitions and asset freezes against specific individuals and entities associated with the former Saddam Hussein regime, as well as parties determined to have committed, or to pose a significant risk of committing, an act of violence that has the purpose or effect of threatening the peace or stability of Iraq or the Government of Iraq or undermining efforts to promote economic reconstruction and political reform in Iraq or to provide humanitarian assistance to the Iraqi people." See U.S. Department of the Treasury Office of Foreign Assets Control, *Iraq: An Overview of the Iraq Stabilization and Insurgency Sanctions Regulations*, September 15, 2010, available at http://www.treasury.gov/resource-center/sanctions/Programs/Documents/iraq.pdf; and "Iraq-Related Sanctions," U.S. Department of the Treasury, December 5, 2012, http://www.treasury.gov/resource-center/sanctions/Programs/pages/iraq.aspx.

[51] In 2007, President George W. Bush signed Executive Order 13441, "Blocking the Property of Certain Persons Undermining the Sovereignty of Lebanon or its Democratic Processes or Institutions and Certain Other Persons." See "Lebanon-Related Sanctions," U.S. Department of the Treasury, December 5, 2012, http://www.treasury.gov/resource-center/sanctions/Programs/pages/leb.aspx.

[52] "How Does the Wassenaar Arrangement Work?," Wassenaar Arrangement, http://www.wassenaar.org/introduction/howitworks.html.

by Citizen Lab and others[53] was subject to export controls, arguing that the technology made use of controlled cryptography as listed Category 5, Part 2.[54]

Generally, however, international and national export controls have not proven applicable to so-called dual-use ICTs, given that many such products and services fall within the realm of commercial application or public security rather than military application or national security. For example, at the national level in the US, while a number of different agencies are involved in export control administration,[55] licensing of most items of commercial nature is carried out by the Bureau of Industry and Security at the US Department of Commerce pursuant to the Export Administration Regulations.[56] Depending on their destination, items on the Commerce Control List[57] require a license to export if they fall within a designated “reason for control”—namely, if they are linked to chemical and biological weapons, nuclear nonproliferation, national security, missile technology, regional stability, firearms convention, crime control, or anti-terrorism.[58] It appears unlikely that technologies such as the Blue Coat Systems ProxySG or PacketShaper products would fit these criteria to trigger the licensing requirement.

If export control frameworks are adapted to better incorporate dual-use ICTs, however, they might serve as a method to restrict provision of technologies that have potential to negatively impact human rights, on the basis of the characteristics of the technology in question and its ultimate destination. Such an approach would require political commitment by governments to develop significant additions to their export control regulations, a process that may also be complicated by necessary export control reforms already in progress on different fronts.[59] Yet if companies were required to build compliance with export regulations into trade of dual-use ICTs, such mandate could serve as an important stimulus to internalization of human rights risk assessments in the surveillance and filtration technology industry, as well as overall corporate social

[53] “The SmartPhone Who Loved Me: FinFisher Goes Mobile?,” Citizen Lab, August 29, 2012. https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile; “From Bahrain With Love: FinFisher’s Spy Kit Exposed?,” Citizen Lab, July 25, 2012, https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed; and “Privacy International Commences Legal Action Against British government for failure to Control Exports of Surveillance Technologies,” Privacy International, July 19, 2012, https://www.privacyinternational.org/press-releases/privacy-international-commences-legal-action-against-british-government-for-failure.

[54] See “Electronic Surveillance: Export Controls” in http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm120907/text/120907w0002.htm#12090723000801; and “British Government Admits It Has Already Started Controlling Exports of Gamma International’s FinSpy,” Privacy International, September 10, 2012, https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma.

[55] See “Resource Links: United States Government Departments and Agencies with Export Control Responsibilities,” U.S. Department of Commerce Bureau of Industry and Security, http://www.bis.doc.gov/about/reslinks.htm.

[56] “Introduction to Commerce Department Export Controls,” U.S. Department of Commerce Bureau of Industry and Security, http://www.bis.doc.gov/licensing/exportingbasics.htm.

[57] 15 C.F.R. pt. 774 (The Commerce Control List), available at http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=ec4619c9b370f71ebcbaf93b0a25e619&n=15y2.1.3.4.45&r=PART&ty=HTML.

[58] 15 C.F.R. pt. 738, supp. no. 1 (Commerce Country Chart), available at http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=59ee1d5eeb8f1d444ba88927fa1eaaff&rgn=div9&view=text&node=15:2.1.3.4.24.0.1.5.27&idno=15.

[59] See, e.g., Ian F. Fergusson and Paul K. Kerr, *The U.S. Export Control System and the President’s Reform Initiative*, Congressional Research Service, May 18, 2012, http://www.fas.org/sgp/crs/natsec/R41916.pdf.

responsibility (CSR) efforts. As with sanctions, the effectiveness of export control frameworks will depend on how carefully such regulations are calibrated.

While the applicability of export controls in this industry is a matter for ongoing discussion, noteworthy steps in that direction are taking place within the EU, including with respect to its "Community regime for the control of exports, transfer, brokering and transit of dual-use items."[60] In September 2011, the European Parliament passed a resolution to prohibit authorization of the export of telecommunications technologies to certain specified countries if they are used "in connection with a violation of human rights, democratic principles or freedom of speech (…) by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use."[61] In October 2012, the European Parliament expanded upon its earlier effort, approving proposals put forward by Dutch Member of Parliament Marietje Schaake that would require authorization for any sale of dual-use technologies designated by European authorities as violative of human rights, democratic principles, or freedom of speech.[62] Finally, the European Parliament passed a resolution in December 2012 on a "Digital Freedom Strategy," which, *inter alia*, called for "a ban on exports of repressive technologies and services to authoritarian regimes" and establishment of a list of countries to which exports of "single-use" technologies (those that inherently threaten human rights) should be banned.[63]

Such multilateral efforts are essential to the success of export controls in curbing the inappropriate use of ICTs. A common justification of companies supplying such technology is that "if we don't sell it, someone else will." Coordinated international measures would help prevent problematic sales of dual-use technology by

[60] Council of the European Union, Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, May 5, 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF.

[61] See Annex IIe, Union General Export Authorisation No EU005, Part 3, Sec. 1(1)(d) in European Parliament, *European Parliament Legislative Resolution of 27 September 2011 on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 1334/2000 Setting Up A Community Regime for the Control of Exports of Dual-Use Items and Technology* (COM(2008)0854 – C7-0062/2010 – 2008/0249(COD)), September 27, 2011, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0406+0+DOC+XML+V0//EN&language=EN; and European Parliament, *Controlling Dual-Use Exports*, September 27, 2011, http://www.europarl.europa.eu/news/en/pressroom/content/20110927IPR27586/html/Controlling-dual-use-exports.

[62] See European Parliament, *European Parliament Legislative Resolution of 23 October 2012 on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 428/2009 Setting Up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items* (COM(2011)0704 – C7-0395/2011 – 2011/0310(COD)), October 23, 2012, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0383&language=EN&ring=A7-2012-0231 (Note the amendment to Article 4 of Regulation (EC) No 428/2009: "An authorisation shall also be required for the export of dual-use items not listed in Annex I if the exporter has been informed by the authorities referred to in points 1 and 2 or by the Commission that the items in question are or may be intended, in their entirety or in part, for use in connection with a violation of human rights, democratic principles or freedom of speech as defined by the Charter of Fundamental Rights of the European Union, by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use (e.g. via monitoring centres or lawful interception gateways)."); and "European Parliament Endorses Stricter European Export Control of Digital Arms," Marietje Schaake, October 23, 2012, http://www.marietjeschaake.eu/2012/10/ep-steunt-d66-initiatief-controle-europese-export-digitale-wapens.

[63] European Parliament, *European Parliament Resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy* (2012/2094(INI)), December 11, 2012, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0470+0+DOC+XML+V0//EN&language=EN.

industry leaders in multiple countries, limiting the availability of top-of-the-line equipment and software that could effectively advance the state of surveillance and filtration within authoritarian regimes. It is noteworthy, therefore, that the European Parliament's "Digital Freedom Strategy" also "calls for the inclusion of targeted repression technologies in the Wassenaar Arrangement,"[64] which would extend the effort beyond the EU to the US, Canada, the Russian Federation, and other countries.

Corporate social responsibility measures are another method relevant to control of dual-use technologies. Inappropriate use of a technology may stem from its technical attributes as well as the behavior of the company supplying or employing it, and it is essential that companies themselves take steps to prevent complicity in human rights compromise. ICT companies can draw on the significant progress that has been made on CSR standards over time, including the UN Guiding Principles on Business and Human Rights[65] and the ICT sector guidance currently in development in the EU.[66]

Moreover, companies such as Blue Coat Systems that make their profits in surveillance and filtering technology would be well-served to explore possibilities for effective self-regulation through CSR if they are indeed concerned about human rights, the possibility of onerous government requirements being imposed on them, or soured public relations. If, for example, Blue Coat Systems had conducted a human rights impact assessment or other due diligence measures regarding the use of its technology by client King Abdulaziz City for Science and Technology (KACST), perhaps it would have come to the conclusion that KACST was an agent of the government in national-level filtering, including of content related to political reform and human rights issues.[67] It appears Blue Coat Systems may not have fully appreciated or addressed the ramifications of such deployment of its technology, given its inclusion in marketing materials of KACST as a client "success

[64] See Para. 43 in European Parliament, *European Parliament Resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy* (2012/2094(INI)), December 11, 2012, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0470+0+DOC+XML+V0//EN&language=EN.

[65] "UN Guiding Principles on Business and Human Rights," Business & Human Rights Resource Centre, http://www.business-humanrights.org/Documents/UNGuidingPrinciples. The UN Guiding Principles note as a basic foundational principle, "Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved" (see Principle 11). Furthermore, companies should "[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts" (see Principle 13(b)). The document details how companies should carry out such obligations.

[66] "Draft Guidance Consultation (Dec. 2012 – Feb. 2013)," Institute for Human Rights and Business, http://www.ihrb.org/project/eu-sector-guidance/draft-guidance-consultation.html. (Discussing corporate policy commitments, human rights due diligence measures, and remediation mechanisms).

[67] "Introduction to Content Filtering," King Abdulaziz City for Science & Technology Internet Services Unit, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm. ("The [KACST] Internet Services Unit oversees and implements the filtration of web pages in order to block those pages of an offensive or harmful nature to the society, and which violate the tenants of the Islamic religion or societal norms. This service is offered in fulfillment of the directions of the government of Saudi Arabia and under the direction of the Permanent Security Committee chaired by the Ministry of the Interior. . . . KACST maintains a central log and specialized proxy equipment, which processes all page requests from within the country and compares them to a black list of banned sites. If the requested page is included in the black list then it is dropped, otherwise it is executed, then the request is archived. These black lists are purchased from commercial companies and renewed on a continuous basis throughout the year. This commercial list is then enhanced with various sites added locally by trained staff."). See also "Saudi Arabia," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/saudi-arabia; and Noman and York, "West Censoring East."

story."[68] On the other end of the spectrum, Websense, previously noted as one of the market leaders in secure web gateway solutions, has already taken steps toward CSR integration: it joined the Global Network Initiative (GNI) in December 2011, thus committing to the GNI's freedom of expression and privacy principles and accountability framework.[69] The more companies take proactive measures to prevent complicity in human rights abuses, the more normalization of corporate social responsibility will take place within the industry.

A combination of the methods described above and other measures is essential to addressing the human rights impact of the booming market for surveillance, filtration, and other sensitive technologies, including dual-use ICTs. Scrutiny and foresight regarding what this market has and has yet to become are critical, as the societal and political ramifications will only grow more profound as technologies develop and use becomes more widespread. Proposals on a framework for control (through sanctions, export regulations, and other methods) of dual-use and other technologies that may compromise human rights are forthcoming in a future blog post by Citizen Lab.

## PART IV: AREAS FOR FURTHER RESEARCH AND POLICY DISCUSSIONS

This report raises several issues for further research and policy discussion:

**There is a need for more transparency around censorship and surveillance practices as well as dialogue among states, ISPs, civil society, and the private sector.** States and large ISPs have tended toward a lack of transparency when it comes to their capabilities for censorship and interception of network traffic. Their silence, however, should not be mistaken for the absence of such activity; indeed, many of them have moved to acquire and deploy powerful filtering and monitoring infrastructure, including Blue Coat Systems technology, as our report makes clear. Some countries have had elements of a public dialogue over network monitoring and filtering, others have not. In the US, for example, a raucous debate continues over whether ISPs should be able to massively filter network traffic based on content and type. These public debates have also emerged in Germany and France.[70] Similarly, some debates have taken place over state surveillance and ISP participation in monitoring, although these are often hampered by limited public evidence of the scope and scale of these practices. Yet, as this report shows, **even in countries where ISPs or governments may not have publicly declared their ability to exercise this kind of control and little public notice or debate has taken place, opponents of Internet filtering and massive interception should be aware that the infrastructure may already be present** — and in some cases, built from the ground up as a kind of

[68] "KACST Deploys Blue Coat Appliances to Provide Secure and Productive Web Access in the Kingdom of Saudi Arabia," Blue Coat, http://www.bluecoat.com/company/customers/kacst-deploys-blue-coat-appliances-provide-secure-and-productive-web-access.
[69] "Websense Joins the Global Network Initiative," Global Network Initiative, December 8, 2011, http://www.globalnetworkinitiative.org/newsandevents/Websense_Joins_the_Global_Network_Initiative.php.
[70] Jillian C. York, "EFF Signs Joint Coalition Letter Urging Companies to be Proactive on Export Regulations," Electronic Frontier Foundation, June 27, 2012, https://www.eff.org/deeplinks/2012/06/eff-signs-joint-coalition-letter-urging-companies-be-proactive-export-regulations.

"surveillance-by-design." By providing this overview, we hope to encourage civil society groups, governments, and researchers to take a closer look at why these devices are present in their country. We also hope that this report will encourage ISPs, manufacturers, and other actors involved in deployment of these products to consider publicly clarifying their scale and function.

**More independent, evidence-based research on the global spread and use of censorship, surveillance, and other "dual-use" technologies is essential.** Providing a clearer picture of the global presence of Blue Coat Systems devices highlights how widely such technologies are used and how technical interrogation methods can be used to determine their presence in specific instances. We see our methodology as an important component of the civil society toolkit (including academia) for engaging in ongoing debates over the proliferation of censorship and intercept technologies, among others. We hope to stimulate dialogue surrounding deployment of dual-use technologies, and provide empirical support for ongoing efforts to develop appropriate control strategies. It is important to note that our methodology does not reveal the intentions or exact uses of the Blue Coat Systems devices in question. We expect these to be different in each case, and think this is an important area for future research. If such contributions are going to be credible, however, it is important that the research be independently conducted and based on open and reproducible methods and empirical evidence.

**It is time to examine the appropriate course of action for companies that participate in the industry for network surveillance, censorship and other sensitive technologies.** While the pursuit and development of new markets and products is naturally a priority to for-profit companies, they remain obliged at all times to respect human rights and avoid activities that would infringe upon them.[71] The events of the Arab Spring have raised awareness that the products and services of this sector can and will be used to advance illegitimate ends that violate international human rights law. Companies can no longer simply assert that it is acceptable to provide their technology to any prospective client, no matter how questionable, until their home governments instruct them otherwise. Civil society and academic groups have indicated this is an area of high concern, key governments have begun pursuing this issue, and it is time for the private sector to join the dialogue and commit to finding solutions.

To that end, we pose the following questions to Blue Coat Systems, which we hope will spark further constructive dialogue:

- What human rights policy commitments and due diligence measures does Blue Coat Systems have in place concerning the development and sales of its products and services?
- In designing its products, does Blue Coat Systems assess their potential human rights impact? Have product designs ever been considered "off-limits" given inherent capabilities to undermine privacy or freedom of expression?

[71] See "UN Guiding Principles on Business and Human Rights," Business & Human Rights Resource Centre, http://www.business-humanrights.org/Documents/UNGuidingPrinciples.

- What if any resources does Blue Coat Systems devote to human rights compliance at the operational level? For example, what percentage of the annual budget is allocated to human rights programs, investigations or training? What human rights training is provided to staff in each department of the company (including executive leadership as well as engineering, sales and legal departments)? What is staff awareness of the human rights implications of deployment of Blue Coat Systems products?

- Does Blue Coat Systems attempt to integrate a "know your customer" standard into its business practices? Does it attempt to discern the purpose for which a client seeks to purchase its products or services? If so, how (for example, in the case of the services provided to King Abdulaziz City for Science and Technology Internet Services Unit)? If the potential client is a government or located in a country known to have experienced unrest, does Blue Coat Systems investigate the human rights track record of that potential client? If human rights concerns are flagged, how does Blue Coat Systems act on such concerns?

- What is the process at Blue Coat Systems for evaluating compliance with US sanctions and export controls?

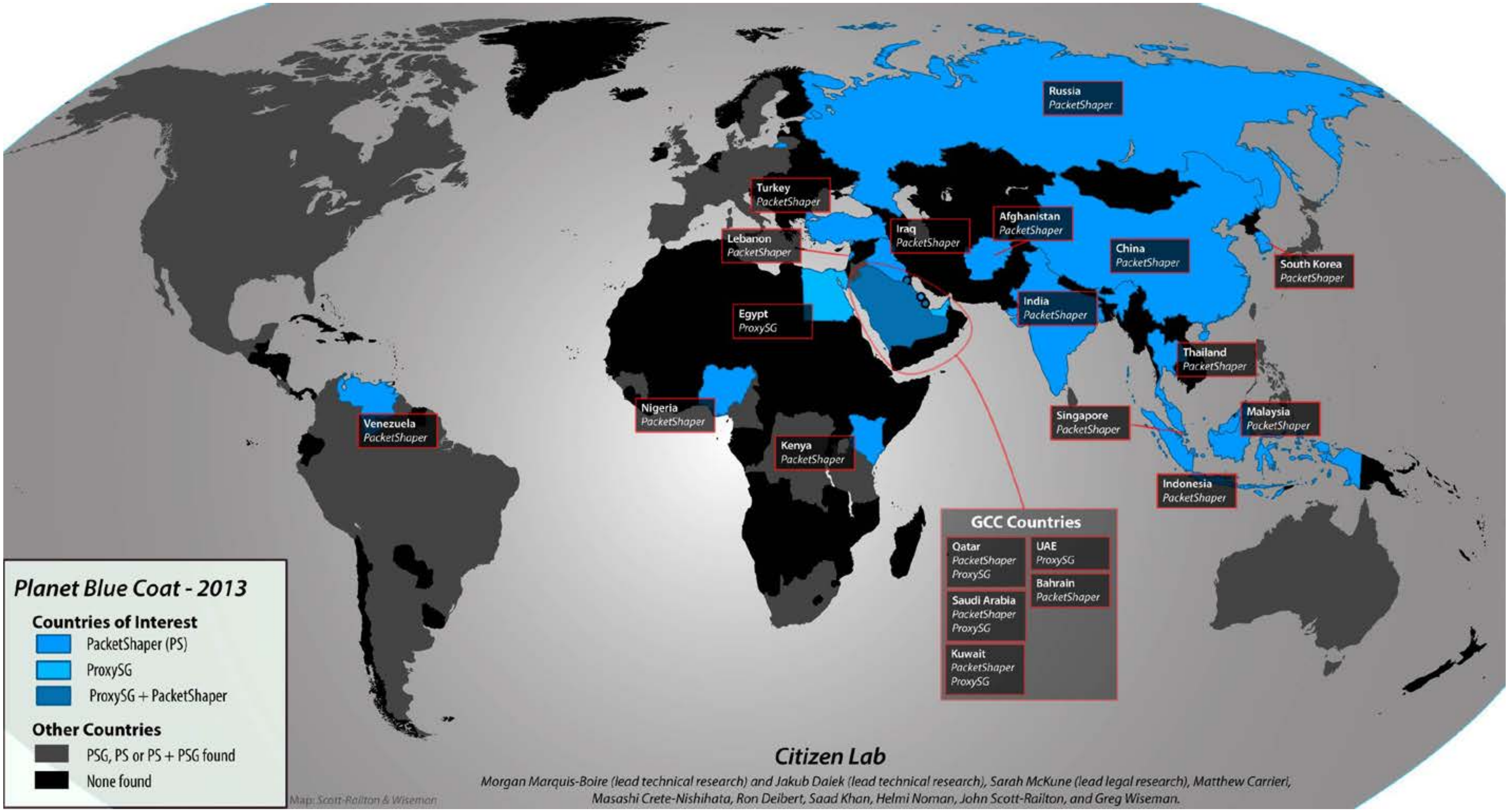
- What processes are in place for ensuring "downstream" compliance with human rights policy commitments and due diligence by resellers, distributors and other third parties with whom Blue Coat Systems contracts? Particularly after the discovery of Blue Coat devices in Syria as described in Part I of this report, were any changes made concerning such processes?

We commit to publishing in full Blue Coat System's reply.

**Our work supports the need for an effective framework for control of technologies that have significant potential to undermine human rights.** It is important to emphasize that the questions posed to Blue Coat Systems (above) are pertinent as well for all other companies active in this industry. Given the many documented instances of advanced information communication technologies put to use by governments and other actors for the purpose of maintaining power and control at the expense of human rights, and the rapid, lucrative growth of the market, it is clear that this industry cannot continue to operate in a largely unregulated atmosphere. While control of dual-use and other sensitive technologies raises significant complexities (see Part III above), some form of check on this industry is essential—whether it be proactive self-regulation, export controls, sanctions, or a combination of these and other efforts. We hope that more companies will step forward to discuss how such controls can be applied in a pragmatic manner. The input of civil society is likewise crucial, as is the leadership of governments in developing multilateral approaches for effective control.

## ACKNOWLEDGEMENTS

Thanks to Eireann Leverett and Shawn Merdinger for pointing the way.



Map: Scott-Railton & Wiseman

Morgan Marquis-Boire (lead technical research) and Jakub Dalek (lead technical research), Sarah McKune (lead legal research), Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Khan, Helmi Noman, John Scott-Railton, and Greg Wiseman.

# APPENDIX A: SUMMARY ANALYSIS OF “COUNTRIES OF INTEREST”

**Countries of interest in which Blue Coat devices were located:**

**ProxySG**
Egypt, Kuwait, Qatar, Saudi Arabia, United Arab Emirates

**PacketShaper**
Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, Venezuela

## Bahrain

We identified a single PacketShaper installation flagged by Shodan as recently as December 31, 2012. The address identified by Shodan was on a netblock associated with the Bahrain Internet Exchange (BIX). Additional research using the iplocation.net service and databases provided by db4 and maxmind identify the ISP as “Central Informatics Organisation.” Despite the recent identification by Shodan, this host was not accessible during the verification period in early January 2013. According to its website, BIX is an Internet exchange point that serves “ISPs and the Government Sector in the Kingdom of Bahrain.”[1] Privacy International has stated that BIX “may have the capacity to play a role in communications monitoring,” and BIX itself has openly acknowledged that they may monitor ports and connections when “information is required by applicable law.”[2] The existence of Blue Coat products on an Internet exchange network suggests a state-level initiative. Bahrain’s extensive censorship regime has only intensified in the wake of the Arab Spring protests. The government actively filters websites critical of the regime, as well as content that is perceived as pornographic, un-Islamic, or accepting of LGBT issues.[3] In the past, the Bahraini government has reportedly used web filtering technologies created by Blue Coat Systems and McAfee.[4] Bahrain extensively monitors online activity and has used Western-made surveillance software to generate transcripts as part of the interrogation and torture of prisoners.[5]

## Kuwait

We have identified three Blue Coat products present in Kuwait. ProxySG was present on a network belonging to Mada Communications, while the ISPs of Gulfnet and Fast Telco each had a PacketShaper installation present on their networks. These were all initially identified by Shodan and were verified during our testing. Kuwait has targeted blasphemous, LGBT, and perceived un-Islamic content online for censorship.[6] The Kuwaiti government has also considered criminalizing the “misuse” of social media, especially with regards to defamation and criticism of government policies, and “allow[ing] government entities to regulate the use of the different new media outlets such as Twitter.”[7] In the past, Kuwaiti ISPs have reportedly used SmartFilter and Netsweeper to censor content.[8]

## Qatar

We identified an installation of both ProxySG and PacketShaper on netblocks associated with Qatar Telecom (QTel). Shodan initially identified the PacketShaper installation in late September 2012 and this was verified during testing. The ProxySG installation was initially found as a result of network scanning in October 2012 and verified as accessible in January 2013. A 2011 *Wall Street Journal* investigation found that Blue Coat technologies have been used in Qatar among other countries in the Gulf.[9] Qatar's censorship regime focuses on websites it considers socially inappropriate, including anti-Islamic, LGBT, and sexual health-related content. Some political websites are also censored.[10] According to the U.S. State Department, Qatar censors online content through state-owned ISPs and through proxy servers that monitor chat rooms and email.[11] Qatar's Telecommunications Law punishes those "using a telecommunication network or allowing such use for the purposes of disturbing, irritating or offending any person," thus giving free reign to authorities to crack down on controversial content.[12] Moreover, Chapter 15 of the law requires service providers to comply with government requests for information deemed "necessary for exercising its powers."[13]

## Saudi Arabia

We were able to identify five total Blue Coat products in Saudi Arabia. There are two installations of the ProxySG product on a network block identified as SaudiNet that was initially detected in mid-2012 by Shodan and verified during testing. Additionally, there are three total PacketShaper installations on the networks identified as ITC, King Abdulaziz City for Science and Technology (KACST) and Nournet. Shodan initially identified the installations on KACST and ITC, while a Google search identified the installation on Nournet. Notably, KACST's Internet Services Unit (ISU) is responsible for implementing the state's filtering regime.[14] Blue Coat Systems has reportedly been present in Saudi Arabia since 2007, when the company announced its intention to expand operations across the region, and has since been open about its relationship with the Saudi government.[15] The company cites ISU's use of ProxySG appliances as a success story, noting that its products allow ISU to "implement flexible policy control over content, users, applications and protocols to protect its users from malicious content."[16] Saudi Arabia's strict regime of Internet censorship has only intensified following the Arab Spring revolutions and protests in the Middle East and North Africa.[17] The government openly acknowledges its engagement in Internet and telecommunications censorship "to block those pages of an offensive or harmful nature to society, and which violate the tenants [sic] of Islamic religion or societal norms."[18] Saudi Arabia has used SmartFilter, now owned by McAfee, to index websites by category and implement mass filtering of content deemed insulting to the political system and offensive to Islamic morals.[19]

## United Arab Emirates

We found five installations of ProxySG on networks in the United Arab Emirates (UAE). All of these installations were on network blocks belonging to the ISP Etisalat. Shodan initially identified one installation on January 1, 2013 while follow up scans around the netblock turned up three additional installations. These installations were accessible during verification but have become sporadically available since their initial verification. Blue Coat Systems maintains a support centre in Dubai's Internet City (its only known Middle East office) for its regional clients.[20] In 2011, the *Wall Street Journal* reported that the company's technologies have been used in the UAE, along with a number of other Gulf countries.[21] (The same report revealed that one of Blue Coat Systems' authorized Emirati distributors had sent ProxySG devices to the Syrian regime.[22]) In the UAE content is blocked pursuant to instructions from the Telecommunications Regulatory Authority (TRA) to ISPs, based on pre-determined content categories. Etisalat, the UAE's dominant ISP, outlines TRA's "Prohibited Content Categories" on its website, including content related to pornography, gambling, malicious computer use, circumvention tools, terrorism, and religious hate speech.[23] However, the government also filters political websites on an *ad hoc* basis. Like Kuwait, ISPs in the UAE have used both SmartFilter and NetSweeper to censor content.[24] The UAE has made surveillance of cybercafé patrons mandatory by requiring ID and the recording of personal information of users.[25]

## Afghanistan

We identified a single installation of the PacketShaper product on a network identified as an "Afghan Telecom Government Communication" network in Kabul. This was initially identified by Shodan on December 31, 2012 and was accessible during our verification. Pursuant to Afghanistan's 2005 Telecom Law, monitoring of communication and Internet traffic is permitted when demanded by the Afghanistan Telecom Regulatory Authority, and ISPs must comply with government requests for data in matters of national security.[26] In 2010, Afghanistan's Minister of Information and Culture stated the government's intent to block websites that promote violence and terrorism, facilitate gambling, deal with "sexual issues," and associate with drug production and trafficking.[27] The government admitted at the time that it did not yet possess the technology to institute website blocking, and reports from the same year indicated that Afghani ISPs were "struggling to enforce" official directives to filter the Internet.[28] It is possible that Blue Coat PacketShaper devices that are now employed in the country could have been used to bridge that initial technological gap and build a state-level filtering and surveillance regime from the ground up.

## Egypt

We identified a single installation of ProxySG though it was not verified during our testing phase and was inaccessible in follow-up connection attempts. Shodan identified the presence of the product on a network belonging to an Etisalat netblock as recently as October 2012. The IP that Shodan identified resolves to a domain that is associated with the nile-online.net domain. Prior to the 2011 revolution, the Mubarak regime actively monitored social networking platforms, e-mail exchanges, and mobile phone communications.[29] In response to the Arab Spring protests of 2011, the government employed a number of techniques to control dissent, including the complete shutdown of Internet access on most ISPs.[30] The Mubarak regime also allegedly used Deep Packet Inspection (DPI) tools provided by Narus, a Silicon Valley-based firm and Boeing subsidiary.[31] Freedom House reports that the post-Mubarak government has continued to selectively remove controversial content and closely surveil activists and bloggers on Internet and social media.[32] In March 2012, for example, the Ministry of Telecommunications and Information Technology announced its intention to block pornographic websites from within the country.[33] Additionally, Freedom House reports that the Homeland Security Agency allegedly acquired DPI and filtering equipment in 2011.[34]

## Iraq

We identified a single PacketShaper installation that was present on the network of City Telecom, an ISP based in Baghdad. It was identified by Shodan as early as August 2012 and was still accessible during our verification in early January 2013. The current mapping of Blue Coat PacketShaper products in Baghdad coincides with the post-war reconstruction of Iraq's telecommunications industry and the drafting of legislation specifically tailored to address Internet use. Most recently, the Iraqi government drafted an "Information Crimes Law" that would ostensibly aim to "to provide legal protection for the legitimate use of computers and information networks, and punish those who commit acts that constitute encroachment on the rights of their users,"[35] including perpetrators of vaguely defined "prohibited activities" such as harming the "reputation of the country," broadcasting "false or misleading facts," and violating "religious, moral, family, or social values."[36] The law also sets out penalties for ISPs that fail to comply with government requests for user data.[37] As of December 2012, parliament has reportedly placed the Information Crimes Law on hold.[38] However, the deployment of Blue Coat PacketShaper devices, in conjunction with legislation that permits the monitoring and prosecution of Internet users, indicates possible 'surveillance by design' in the context of post-conflict reconstruction.

## Lebanon

We identified two installations of PacketShaper during the course of research. One installation was identified initially by Shodan on December 12, 2012. This installation was found on a netblock associated with "IncoNet Data Management." An additional PacketShaper installation was identified by a Google search on a netblock associated with "Virtual ISP Lebanon" (visp). Tests performed in 2009 indicated no known state-level Internet filtration or surveillance in Lebanon.[39] Since 2010, however, Lebanese authorities have detained many citizens for criticizing the government and army.[40] Most recently, the Lebanese Ministry of Information has drafted a new law prohibiting the publication of online content deemed offensive to "public morals."[41]

## Turkey

We identified a single installation of PacketShaper that was identified by a Google search in early 2013. This was on a netblock associated with TTNet, Turkey's largest ISP and a subsidiary of the formerly state-owned Turk Telecom.[42] Blue Coat Systems expanded its presence in the country in 2008 by adding a number of Turkish distributors "to better serve Turkish companies and organizations."[43] One reseller, Innova, reportedly sought to combine "its technical expertise and reputation in the market with Blue Coat ProxySG appliances to provide organizations with tools they need to gain control over the appliances on their networks."[44] Freedom House reports that, since 2001, Turkey has passed a series of laws that collectively empower state organizations to filter content.[45] Law No. 5651 — "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication" — ostensibly seeks to prevent youths from accessing illicit content such as pornography and gambling. However, that regulation and other laws have been applied more broadly to block political content such as criticism of Kemal Ataturk, news sources, and media sharing websites.[46] In November 2011, the Turkish government instituted a national filtering system that requires ISPs to offer customers the option to block content deemed inappropriate for families and children.[47] Engelli Web, a Turkish website that tracks censored content, lists over 22,000 blocked websites as of January 14, 2013.[48]

## Russia

We identified a single installation of the PacketShaper product on a netblock associated with the Vimpelcom ISP. This was initially identified by Shodan on December 30, 2012 and was verified during testing. A high level of state control over the domestic telecommunications market exists in Russia.[49] Recently, Prime

Minister Dmitry Medvedev signed a new law “blacklisting” sites the government views as fronts for illegal content.[50] Roskomnadzor — Russia’s federal service for monitoring mass media compliance — has introduced Deep Packet Inspection “on a nationwide scale,”[51] having previously announced a competitive “contest” for software designed to monitor sites for “extremist” content.[52] Russia’s Soviet-era system to intercept phone traffic has also undergone recent upgrades.[53] One of the largest providers in the region, Mobile TeleSystems OJSC (MTS), has used Blue Coat in the past at the Internet gateway of MTS’s headquarters in Moscow to protect against “Internet threats.”[54] It is reasonable to surmise that other telecoms in Russia are using Blue Coat for the same purposes; however, as Russia seems to be increasing surveillance of online content, the use of foreign technology for political purposes must be monitored in the future.

## China

We identified three installations of Blue Coat products present on the netblock associated with ChinaNet. Two were identified by Shodan initially in late 2012 and verified during testing. One additional installation of PacketShaper was found through a Google search. This installation had a system name of “WT-CHENGDU-INT-PS” and was present on a ChinaNet IP in Sichuan. ChinaNet is an “operational brand” of state-owned China Telecom and is described as “the world’s largest Internet network.”[55] China’s Internet filtering and surveillance regime, often referred to as the “Great Firewall,” is pervasive and multifaceted. The government employs a variety of means to prevent citizens from accessing material that is deemed politically threatening or socially controversial, including “tight regulations on domestic media, delegated liability for online content providers, just-in-time filtering, and ‘cleanup’ campaigns.”[56] Deep Packet Inspection technology is used to blacklist pages based on pre-defined keywords, as well as to monitor users’ Internet activity.[57] Moreover, thousands of government and private sector workers reportedly monitor and censor objectionable content on social media platforms, blogs, and political websites.[58] Chinese legislation holds Internet information service providers accountable for content on their servers and specifies nine forbidden content categories, including material that opposes constitutional principles, threatens national security and the state, or “undermines social stability.”[59]

## South Korea

There were three installations of PacketShaper identified on netblocks associated with Korea Telecom. All three installations were initially identified by Shodan in December 2012. These were verified as accessible, though some of these have been sporadically available since verification. South Korea’s government imposes more constraints on online speech than most democratic countries. While the rate of filtering is generally low, online content and expression is heavily regulated through legal and technical measures.[60] ISPs target social content, and content related to conflict and security — especially content that is pro-North Korea or considered threatening to national security.[61] The Korea Communications Standards Commission is authorized to order the blocking or closure of websites, the deletion of messages, and the suspension of users, as well as to mediate online defamation disputes.[62] Although the Constitutional Court recently ruled a five-year-old online real-name registration rule to be unconstitutional, concerns over government surveillance remain.[63] In 2012, Freedom House reported that the government has increased purchases of interception equipment and documented instances where authorities have not followed protocol when obtaining information on citizens.[64]

For instance, a scandal emerged in 2012 over unlawful surveillance activities by the Civil Service Ethics Division, a division established in 2008 for the purposes of monitoring corruption amongst government officials. The Korean Broadcasting System released over 2,600 records documenting the illegal surveillance of civilians known to be critical of the government, such as labour union leaders and journalists.[65] In 2010, seven members of the Division were convicted for illegal surveillance of citizens.[66]

## Indonesia

A single installation of PacketShaper was identified by a Google search. This installation was present on a netblock associated with the Lintasarta ISP. ISPs in Indonesia are subject to filtering requests from the Ministry of Communication and Information Technology.[67] Indonesian Internet filtering heavily targets pornographic Web sites. Several ISPs also blocked some sex education and LGBT content, as well as sites offering circumvention tools. However, testing revealed that filtering was unsystematic and inconsistent, as demonstrated by differences across ISPs.[68] The government has occasionally blocked anti-Islamic content.[69]

## Malaysia

We identified three PacketShaper installations in Malaysia during research. Two installations were initially identified by Shodan in late 2012 and subsequently verified. They were present on netblocks associated with Jaring and TMNet. They have since been sporadically accessible. There was an additional installation identified by a Google search in early 2013 on a netblock associated with the Arcnet ISP. Blue Coat Systems maintains a physical presence in the country, with its Asia Pacific Headquarters located in Kuala Lumpur. While there is no evidence of technical Internet filtering in Malaysia, online content is regulated through other means.[70] The Communications and Multimedia Act (1998) prohibits online content that is “indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.”[71] The Malaysian Communications and Multimedia Commission, which is responsible for regulating the Internet, is known for tracking online discussions and asking content creators to remove such content.[72] Freedom House has expressed concern that authorities seem to be capable of identifying anonymous Internet and mobile users with the help of service providers.[73] In April 2012, the government passed the Security Offenses (Special Measures) Act, which authorizes the interception of communications without a judicial order in cases of vaguely defined security offences.[74]

## Singapore

During research, we identified two installations of PacketShaper in Singapore. One was initially identified by Shodan in mid-2012 and verified on a netblock associated with SingNet. This installation has been sporadically accessible since verification. An additional installation was found by a Google search on a netblock associated with the ViewQwest ISP. Singapore engages in minimal Internet filtering by blocking only a small set of high-profile pornographic Web sites, suggesting that filtering is imposed for symbolic, rather than preventative, purposes.[75] Rather than employing technical measures to control online content, the government utilizes licensing controls as well as legal pressures, such as defamation suits.[76] All ISPs offer content filtering services for residential broadband subscribers.[77] A 2006 Privacy International report found that Singaporean law permits government surveillance of Internet activity and "grants law enforcement broad power to access data and encrypted material when conducting an investigation."[78]

## Thailand

A single PacketShaper installation was identified by Shodan in late 2012, which was verified as accessible. This installation was present on a netblock associated with the ISP CS Loxinfo, which provides home and business Internet service. Thailand primarily blocks sites related to political opposition, pornography, online gambling, and circumvention tools.[79] A central focus of blocking is lèse-majesté content.[80] Lèse-majesté refers to punishment for any negative critical remarks about the monarchy and is strictly enforced through provisions in the Penal Code. Internet filtering in Thailand is governed by the Computer Crime Act (2007), which authorizes the prosecution of Internet intermediaries for "intentionally supporting or consenting for crimes linked to the use of computers," effectively making Internet intermediaries legally responsible for policing lèse-majesté content.[81] There has been some concern over indications that the Thai government intends to increase its capacity to intercept private communications.[82] For example, in December 2011, Thai authorities introduced a proposal for purchasing a four million baht lawful interception system for the purposes of cracking down on online lèse-majesté content.[83]

## India

We identified four PacketShaper installations present in India. These installations were all initially identified by Shodan in late 2012 and verified as accessible. They were present on netblocks associated with the ISPs of Bharti Airtel, Reliance, and Tata Communications, all of which have been implicated in filtering to some degree. In July 2012, Citizen Lab found that websites in Omani cyberspace were being inadvertently filtered as a result of a traffic peering arrangement between Bharti Airtel and Omani ISP Omantel.[84] Reliance Communications was one of several ISPs to block file-sharing sites,[85] while Tata Communications has reportedly used Netsweeper for filtering.[86] India engages in selective filtering in many categories, including politically "extremist" websites.[87] Despite its commitment to free expression, amendments to the country's Information Technology Act (ITA) in 2008 have been criticized as overly broad. Section 66A, for example, criminalizes the sending of "offensive messages" through telecommunications services without clarifying what constitutes "offensive."[88] Moreover, Section 69 of the ITA authorizes government agencies to monitor and intercept Internet traffic and user information for purposes of national security or cyber security.[89]

## Kenya

There were three PacketShaper installations found in Kenya during research. All three were initially identified by Shodan in December 2012 and were verified as accessible. These were on netblocks associated with Hughes Network Systems, which is a satellite-based Internet provider. The hostnames of the IP addresses of these installations resolve to the iWayAfrica domain, which is an African provider of broadband Internet service. In 2012, it was reported that the Communications Commission of Kenya was implementing a system to monitor incoming and outgoing traffic on the country's networks, including personal e-mails, in order to respond to potential cyber threats. Mobile operators were instructed to cooperate in the installation of Internet traffic monitoring equipment known as Network Early Warning Systems.[90]

## Nigeria

During research there were two PacketShaper installations found on networks in Nigeria. One was identified by Shodan during mid-2012 and was verified as accessible. This installation was present on a netblock associated with the IPNX ISP, and had a system name of "IPNX_SHAPER" set on the login screen. There was an additional installation on a netblock associated with Cobranet. (Note that in the data provided, the installation is listed as a Lebanese IP address because the ISP operating in Nigeria is of Lebanese ownership, as seen in the whois record for cobranet.org.) No evidence of filtering has been found in Nigeria in the past.[91] It has been reported that some ISPs block access when users are found to be downloading copyrighted content. Freedom House states that this is done not to protect intellectual property but to manage network traffic.[92]

## Venezuela

We identified a single installation of PacketShaper on a netblock belonging to CANTV Servicios, one of the country's largest telecommunications providers and a state-owned enterprise.[93] This was identified by Shodan in August 2012 and was verified during testing. There is no current evidence of filtering of political or social sites in Venezuela.[94] However, Reporters Without Borders has expressed concern that the lack of extensive Internet censorship in the country ignores other methods of controlling Venezuelan cyberspace, such as the monitoring of Internet forums and websites for politically sensitive content.[95]

## FOOTNOTES

[1] "FAQ," Bahrain Internet Exchange, http://www.bix.bh/faq_general.php.
[2] https://www.privacyinternational.org/reports/surveillance-briefing-bahrain/surveillance-in-practice; and "Memorandum of Understanding (MoU)," Bahrain Internet Exchange, http://www.bix.bh/mou.php.
[3] "Bahrain," OpenNet Initiative, http://opennet.net/research/profiles/bahrain.
[4] Paul Sonne and Steve Stecklow. "U.S. Products Help Block Mideast Web." Wall Street Journal, March 27, 2011. http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html
[5] "Freedom on the Net 2012: Bahrain," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/bahrain#_ftn8; and Ben Elgin and Vernon Silver, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," Bloomberg, August 22, 2011, http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.
[6] "Kuwait," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/kuwait.
[7] Kevin Collier, "Kuwait moves toward criminalizing online dissent," The Daily Dot, August 16, 2012, http://www.dailydot.com/news/kuwait-social-media-dissent-law/.
[8] Helmi Noman and Jillian C. York, "West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011, March 2011, http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011; and Helmi Noman "When a Canadian Company Decides What Citizens in the Middle East Can Access Online," OpenNet Initiative, May 16, 2011, http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-

online.

[9] Malas et al., "U.S. Firm Acknowledge Syria Uses Its Gear to Block Web." http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

[10] "Qatar," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/qatar.

[11] "Qatar," U.S. Department of State Bureau of Democracy, Human Rights, and Labor, March 11, 2008, http://www.state.gov/j/drl/rls/hrrpt/2007/100604.htm

[12] Telecommunications Law of the State of Qatar. Unofficial English translation available at http://www.ictqatar.qa/sites/default/files/documents/telecom%20law%202006.pdf.

[13] Ibid.

[14] King Abdulaziz City for Science and Technology, Internet Services Unit, "Introduction to Content Filtering," http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm.

[15] "Blue Coat expansion in region touches Saudi Arabia and Egypt," AMEinfo.com, August 15, 2007, http://www.ameinfo.com/129219.html.

[16] "KACST Deploys Blue Coat Appliances to Provide Secure and Productive Web Access in the Kingdom of Saudi Arabia," Blue Coat Systems, http://www.bluecoat.com/company/customers/kacst-deploys-blue-coat-appliances-provide-secure-and-productive-web-access.

[17] "Freedom on the Net 2012: Saudi Arabia," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/saudi-arabia.

[18] "Introduction to Content Filtering," King Abdulaziz City for SCience and Technology Internet Services Unit, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm.

[19] "Saudi Arabia," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/saudi-arabia; and Noman and York, "West Censoring East."

[20] "Company," Blue Coat Systems, http://www.bluecoat.com/company.

[21] Malas et al., "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web."

[22] See William McQuillen, "U.S. Bans UAE Company for Supplying Internet Filter to Syria," Bloomberg, December 15, 2011, http://www.bloomberg.com/news/2011-12-15/u-s-bans-uae-company-for-supplying-internet-filter-to-syria.html.

[23] "Prohibited Content Categories," Etisalat, http://www.etisalat.ae/assets/document/blockcontent.pdf.

[24] Helmi Noman, "A Blind-date with the Censors in UAE," OpenNet Initiative, June 20, 2008, http://opennet.net/blog/2008/06/a-blind-date-with-censors-uae; and Noman and York, "West Censoring East."

[25] "Countries Under Surveillance: United Arab Emirates," Reporters Without Borders, http://en.rsf.org/surveillance-united-arab-emirates,39760.html.

[26] "Afghanistan," OpenNet Initiative, May 8, 2007, http://opennet.net/research/profiles/afghanistan.

[27] Susan J. Campbell, "Afghan Government Plans to Ban Certain Internet Sites, Denies Censorship," TMCnews, March 4, 2010, http://ipcommunications.tmcnet.com/topics/ip-communications/articles/77614-afghan-government-plans-ban-certa-internet-sites-denies.htm.

[28] "Internet Censorship in Afghanistan," The World, March 24, 2010, http://www.theworld.org/2010/03/internet-censorship-in-afghanistan-2/; and Danny O'Brien and Bob Dietz, "Using New Internet Filters, Afghanistan Blocks News Site," Yahoo! Business and Human Rights Program, October 6, 2010, http://www.yhumanrightsblog.com/blog/2010/10/12/using-new-internet-filters-afghanistan-blocks-news-site/.

[29] "Egypt," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/egypt.

[30] Iljitsch van Bejnum, "How Egypt Did (And Your Government Could) Shut Down the Internet," Ars Technica, January 30, 2011, http://arstechnica.com/tech-policy/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet.

[31] Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," Huffington Post, January 28, 2011, http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html; and "Telecom

Egypt Selects Narus for Traffic Anomaly Detectionl Telecom Egypt Leverages Narus' Security Expertise to Protect Financial Service Data," Business Wire, February 23, 2005, http://www.thefreelibrary.com/Telecom+Egypt+Selects+Narus+for+Traffic+Anomaly+Detection;+Telecom …-a0129070647.

[32]"Freedom on the Net 2012: Egypt," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/egypt.

[33]"Blocking Internet Pornography A Priority for Telecom Minister," Egypt Independent, March 22, 2012, http://www.egyptindependent.com/news/blocking-internet-pornography-priority-telecom-minister.

[34]"Freedom on the Net 2012: Egypt."

[35]"Iraq's Information Crimes Law: Badly Written Provisions and Draconian Punishments Violate Due Process and Free Speech," Human Rights Watch, July 12, 2012, http://www.hrw.org/sites/default/files/reports/iraq0712webwcover.pdf.

[36]Danny O'Brien, "Iraqi Cybercrime Bill is the Worst Kind," Committee to Protect Journalists, March 30, 2012, http://cpj.org/internet/2012/03/iraqi-cybercrime-bill-is-the-worst-kind.php.

[37]"Iraq's Information Technology Crimes Act of 2011: Vague, Overbroad, and Overly Harsh," Access, April 2012, https://s3.amazonaws.com/access.3cdn.net/fa4f8b344e40e560c3_pum6ib7e1.pdf.

[38]Laith Hammoudi, "Tough "Cybercrimes Bill" on Hold in Iraq," Institute for War and Peace Reporting, December 24, 2012, http://iwpr.net/report-news/tough-cybercrimes-bill-hold-iraq.

[39]"Lebanon," OpenNet Initiative, August 6, 2009, http://opennet.net/research/profiles/lebanon.

[40]Josh Wood, "Lebanon Cracks Down on Internet Freedom," New York Times, November 3, 2010, http://www.nytimes.com/2010/11/04/world/middleeast/04iht-m04m1leblog.html?_r=0.

[41]Khodor Salameh, "Lebanese Internet Law Attacks Last Free Space of Expression," Al Akhbar, March 9, 2012, http://english.al-akhbar.com/node/4997.

[42]"Turk Telecom Announces Re-shuffle," TMTFinance.com, July 9, 2012, http://www.tmtfinance.com/news/turk-telecom-announces-re-shuffle.

[43]"Blue Coat Expands Presence in Turkey with Leading Distributor," The Content Factory, September 15, 2008, http://www.tcf-me.com/client_portal/26/news_releases/1004364240.

[44]"Blue Coat Partners with Turkey's Innova to Extend Regional Presence," Al Bawaba, October 21, 2008, http://www.albawaba.com/news/blue-coat-partners-turkey%E2%80%99s-innova-extend-regional-presence.

[45]"Freedom on the Net 2011: Turkey," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/turkey.

[46]"Turkey," OpenNet Initiative," http://opennet.net/research/profiles/turkey; and "Freedom on the Net 2012: Turkey."

[47]"New Internet Filtering System Condemned As Backdoor Censorship," Reporters Without Borders, December 2, 2011, http://en.rsf.org/turquie-new-internet-filtering-system-02-12-2011,41498.html.

[48]"Categories," Engelli Web, http://engelliweb.com/kategoriler/.

[49]"Russia," OpenNet Initiative, December 19, 2010, http://opennet.net/research/profiles/russia.

[50]Reuven Cohen, "Russia Passes Far Reaching Internet Censorship Law Targeting Bloggers and Journalists," Forbes, November 1, 2012, http://www.forbes.com/sites/reuvencohen/2012/11/01/russia-passes-far-reaching-internet-censorship-law-targeting-bloggers-journalists/.

[51]Andrei Soldatov and Irina Borogan,"The Kremlin's New Internet Surveilance Plan Goes Live Today," Wired, November 1, 2012, http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/.

[52]"Danger of Generalized Online Surveillance and Censorship," Reporters Without Borders, March 30, 2011, http://en.rsf.org/russia-danger-of-generalized-online-30-03-2011,39910.html.

[53]Andrei Soldatov and Irina Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You," December 21, 2012, http://www.wired.com/dangerroom/2012/12/russias-hand/all/.

[54]"Mobile TeleSystems OJSC Uses Blue Coat Appliances to Protect Employees from Internet Threats," Blue

Coat, http://bluecoat.com/company/customers/mobile-telesystems-ojsc-uses-blue-coat-appliances-protect-employees-internet.

[55]"Company Overview 2009," China Telecom, http://en.chinatelecom.com.cn/corp; and "ChinaNet," China Telecom, http://en.chinatelecom.com.cn/products/t20060116_48406.html.

[56]"China," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/china.

[57]Ben Wagner, "Study: Deep Packet Inspection and Internet Censorship," Global Voices Advocacy, June 25, 2009, http://advocacy.globalvoicesonline.org/2009/06/25/study-deep-packet-inspection-and-internet-censorship/; and "Freedom on the Net 2012: China," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/china.

[58]"Freedom on the Net 2012: China."

[59]"Measures for Managing Internet Information Services," China Culture, http://www.chinaculture.org/gb/en_aboutchina/2003-09/24/content_23369.htm.

[60]See: "South Korea," OpenNet Initiative, August 6, 2012, http://opennet.net/research/profiles/south-korea.

[61]Ibid.

[62]Ibid.

[63]The Online Verification Law was introduced in 2007 in order to reduce abusive behaviour online, such as spreading false rumours. See Choe Sang-Hun, "South Korean Court Rejects Online Name Verification Law," New York Times, August 23, 2012, http://www.nytimes.com/2012/08/24/world/asia/south-korean-court-overturns-online-name-verification-law.html.

[64]"Freedom on the Net 2012: South Korea," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/south-korea.

[65]"Surveillance Case Ripped Wide Open," Korea Joongang Daily, March 31, 2012, http://koreajoongangdaily.joinsmsn.com/news/article/article.aspx?aid=2950775.

[66]Choe Sang-Hun, "In South Korea Scandal, Echoes of Watergate," New York Times, April 9, 2012, http://www.nytimes.com/2012/04/10/world/asia/government-spying-charges-complicate-korean-vote.html?pagewanted=all.

[67]"Brief Paper: "Internet Freedom at Indonesia," Best Bits, August 2012, http://bestbits.igf-online.net/wp-uploads/2012/10/internet-freedom-indonesia.pdf.

[68]"Indonesia," OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/indonesia.

[69]Melody Zhang, "Indonesia Increases Censorship for Ramadan," Herdict Blog, July 30, 2012, http://blogs.law.harvard.edu/herdict/2012/07/30/indonesia-increases-censorship-for-ramadan; and "Internet Cafes Given a Month to Block Porn Websites," Jakarta Post, August 2, 2010, http://www.thejakartapost.com/news/2010/08/02/internet-cafes-given-a-month-block-porn-websites.html-0.

[70] "Freedom on the Net 2012: Malaysia," Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/malaysia.

[71]Section 211, Malaysian Communications and Multimedia Act, 1998.

[72]"Freedom on the Net 2012: Malaysia."

[73]"Freedom on the Net 2012: Malaysia."

[74]"Malaysia: Security Bill Threatens Basic Liberties," Human Rights Watch, April 10, 2012, http://www.hrw.org/news/2012/04/10/malaysia-security-bill-threatens-basic-liberties.

[75]"Singapore," OpenNet Initiative, May 10, 2007, http://opennet.net/research/profiles/singapore.

[76]See Ibid.

[77]"S'pore ISPs to Actively Promote Internet Filters," Yahoo News, July 15, 2011, http://sg.news.yahoo.com/blogs/fit-to-post-technology/pore-isps-told-promote-mobile-internet-filters-052641650.html.

[7]Privacy International, "Chapter II. Surveillance Policy," Singapore, December 12, 2006, https://www.privacyinternational.org/reports/singapore/ii-surveillance-policy.

[79]“Thailand,” OpenNet Initiative, August 7, 2012, http://opennet.net/research/profiles/thailand.

[80]“Freedom on the Net 2012: Thailand,” Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/thailand.

[81]Kieran Bergmann, “Outsourcing Censorship,” Open Canada, Kieran Bergmann, http://opencanada.org/features/the-think-tank/essays/outsourcing-censorship/.

[8]“Freedom on the Net 2012: Thailand.”

[8]“Web Censor System Hits Protest Firewall,” Bangkok Post, December 15, 2011, http://www.bangkokpost.com/learning/learning-from-news/270926/new-web-censorship-worries.

[8]“Routing Gone Wild: Documenting Upstream Filtering in Oman via India,” Citizen Lab, July 12, 2012, https://citizenlab.org/2012/07/routing-gone-wild/.

[85]Rajini Vaidyanathan, “Hacking Group Anonymous Takes on India Internet ‘Censorship,’” BBC, June 9, 2012, http://www.bbc.co.uk/news/technology-18371297.

[86]Noman and York, “West Censors East.”

[87]“India,” OpenNet Initiative, August 9, 2012, http://opennet.net/research/profiles/india.

[88]“Breaking Down Section 66A of the IT Act,” The Centre for Internet & Society, November 25, 2012, http://cis-india.org/internet-governance/blog/breaking-down-section-66-a-of-the-it-act.

[89]Information Technology (Amendment) Act 2008, http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

[90]Okuttah Mark, “CCK Sparks Row with Fresh Bid to Spy on Internet Users,” Business Daily, March 20, 2012, http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/item/2/-/edcfmqz/-/index.html; and Winfred Kagwe, “Kenya: CCK Defends Plan to Monitor Private Emails,” All Africa, May 17, 2012, http://allafrica.com/stories/201205181170.html.

[91]“Nigeria,” OpenNet Initiative, October 1, 2009, http://opennet.net/research/profiles/nigeria.

[92]“Freedom on the Net 2012: Nigeria,” Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/nigeria#_ftn1.

[93]“Venezuela’s CANTV: What Should a 21st Century “Socialist” Telecommunications Company Look Like?” Venezuela Analysis, March 15, 2010, http://venezuelanalysis.com/analysis/5189.

[94]“Freedom on the Net 2012: Venezuela,” Freedom House, http://www.freedomhouse.org/report/freedom-net/2012/venezuela.

[95]“Venezuela,” Reporters Without Borders, http://en.rsf.org/surveillance-venezuela,39770.html.