UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Canada Centre for Global Security Studies

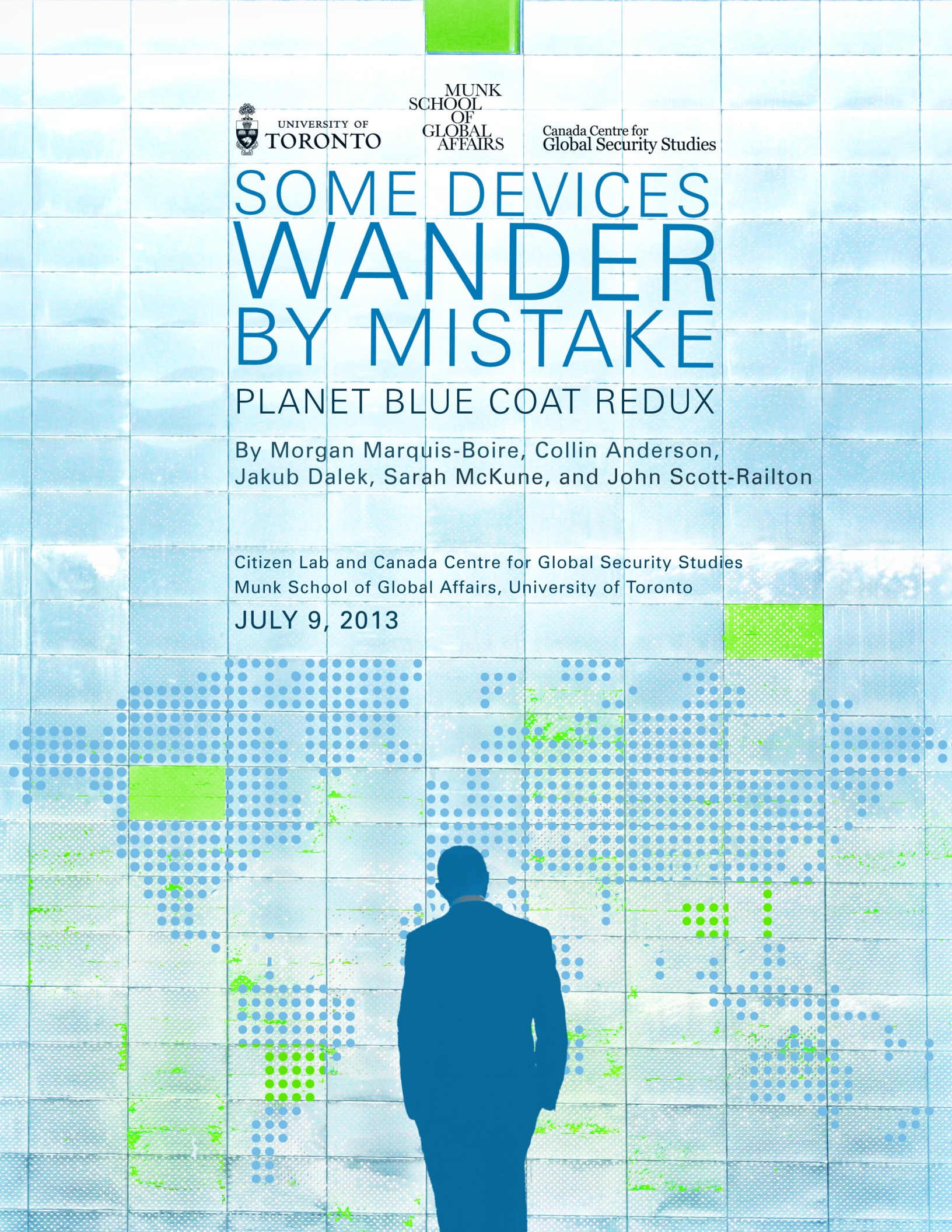
SOME DEVICES WANDER BY MISTAKE

PLANET BLUE COAT REDUX

By Morgan Marquis-Boire, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton

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

JULY 9, 2013



AUTHORS

PROJECT LEADER: Morgan Marquis-Boire
TECHNICAL LEADS: Collin Anderson and Jakub Dalek
LEGAL / POLICY LEADS: Sarah McKune and John Scott-Railton
WRITING AND ANALYSIS SUPPORT: Adam Senft and Ron Deibert
ADDITIONAL RESEARCH ASSISTANCE: Matthew Carrieri and Saad Khan

Morgan Marquis-Boire

Morgan Marquis-Boire is a Security Researcher and Technical Advisor at the Citizen Lab, Munk School of Global Affairs, University of Toronto. He works as a Security Engineer at Google specializing in Incident Response, Forensics and Malware Analysis. He also serves as a Special Advisor to Google Ideas.

Collin Anderson

Collin Anderson is a Washington D.C.-based researcher documenting the conflict between the free flow of information and state repression. He has been involved in identifying the international trade of surveillance equipment and exploring alternative means of communications that bypass normal channels of control. His participation in issues of connectivity has lead to work on availability and legality of online communications services under sanctions restrictions, as well as the ramifications of export regulations to democratization movements.

Jakub Dalek

Jakub Dalek is researcher and systems administrator at the Citizen Lab, Munk School of Global Affairs, University of Toronto. His research focuses on the identification and mapping of devices used for Internet filtering and surveillance.

Sarah McKune

Sarah McKune is Senior Researcher at the Citizen Lab, Munk School of Global Affairs, University of Toronto. Her work includes comparative analysis of targeted cyber threats against human rights organizations, as well as research and analysis regarding international cyber security initiatives and export of rights-impacting technologies. Sarah is a lawyer with a background in international human rights law.

John Scott-Railton

John Scott-Railton is a Citizen Lab Fellow conducting research on electronic attacks in the Middle East and North Africa region. He also co-developed the Voices Projects to support the free and secure flow of information from Egypt and Libya during the Arab Spring. His dissertation work at UCLA also includes research on the human security implications of climate change adaptation failure in West Africa.

TABLE OF CONTENTS

SUMMARY OF MAIN FINDINGS

In this report, our third on Blue Coat Systems, we use a combination of network measurement and scanning methods and tools to identify instances of Blue Coat ProxySG and PacketShaper devices. This kind of equipment can be used to secure and maintain networks, but it can also be used to implement politically-motivated restrictions on access to information, and monitor and record private communications.

We found Blue Coat devices on public networks of 83 countries (20 countries with both ProxySG and PacketShaper, 56 countries with PacketShaper only, and 7 countries with ProxySG only).

Included in these countries are regimes with questionable human rights records and three countries that are subject to US sanctions: Iran, Syria, and Sudan.

Our findings raise questions around the sale of "dual-use" communication technologies to national jurisdictions where the implementation of such technology has not been publicly debated or shaped by the rule of law. The issues raised by this report go beyond one company and its products and services, and underscore the imperatives of addressing global public policy implications of internationally-marketed communications infrastructure and services.

INTRODUCTION

This report documents the global spread of network security and optimization appliances that provide mass filtering and Internet traffic monitoring capability. We focus on the global spread of two "dual-use" devices manufactured by the Sunnyvale, California-based Blue Coat Systems Inc., ProxySG and PacketShaper. This kind of equipment can be used to secure and maintain networks, but it can also be used to implement politically-motivated restrictions on access to information, and monitor and record private communications. Thus, depending on who acquires this equipment and how it is used, the technology may serve legitimate and positive purposes, or be used in ways that result in an adverse impact on human rights. This capacity is often referred to as "dual-use," a term adapted from language used to describe technologies with both civilian and military applications.

BACKGROUND

Blue Coat is just one among the many companies that develop, market, and export dual-use technologies, including technologies that can be used to monitor Internet traffic, block websites, and by extension track users' online activities and communications.[1] Many of the same technologies, of course, can fulfill purely technical functions. Blue Coat achieved unexpected notoriety in 2011 when its ProxySG appliances were found in Syria.[2] The initial announcements triggered investigations, regulatory action against a reseller, and attracted the attention of research groups and civil society.[3] We suspect that Blue Coat also attracts disproportionate attention for one of the same reasons that we continue to

1 Gamma International's FinFisher surveillance software has had command and control servers identified in 36 countries; Siemens and offshoot Trovicor have sold surveillance equipment used against activists in Bahrain; French firm Amesys sold surveillance equipment to Gadhafi's regime in Libya; Netsweeper and McAfee's Smartfilter products have been used to filter web content in dozens of countries; Cisco faced a US congressional investigation in 2006 relating to its involvement in developing the country's Internet censorship system, and in 2011 it supplied networking equipment to a large-scale video surveillance project in the city of Chongqing; Nokia Siemens confirmed it sold telecommunication monitoring equipment to Iran; and Italian firm Area SpA assisted Syria with the development of a surveillance system. See "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, April 30, 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/; 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; Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html; Helmi Noman and Jillian C. York, "West Censoring East, The Use of Western Technologies by Middle East Censors, 2010-2011," OpenNet Initiative, March 2011, https://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011; Rory Cellan-Jones, "Hi-Tech Helps Iranian Monitoring," BBC News, June 22, 2009, http://news.bbc.co.uk/2/hi/technology/8112550.stm; "Internet Filtering in China in 2004-2005: A Country Study," OpenNet Initiative, April 14, 2005, https://opennet.net/studies/china; Cindy Cohn and Jillian C. York, "EFF Urges Microsoft and Cisco to Reconsider China," Electronic Frontier Foundation, July 8, 2011, https://www.eff.org/deeplinks/2011/07/eff-urges-microsoft-and-cisco-to-reconsider-china; and Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Ad with US-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.

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

3 Paul Sonne and Steve Stecklow, "US restricts U.A.E. Firm for Web Filter Sale to Syria," *Wall Street Journal*, December 16, 2011, http://online.wsj.com/article/SB10001424052970204844504577100550048032714.html.

study it: many of its products are easily identifiable on networks. This makes it possible for academic researchers and hacktivist groups like Telecomix to identify Blue Coat appliances in countries like Syria and Burma. The Citizen Lab, for example, documented specific country implementations in *Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma* (2011). We have since employed more refined methods and signatures that have enabled global-scale scanning for Blue Coat appliances, as documented in *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools* (2013). This work has highlighted a trend: Blue Coat devices appearing on public networks in countries with dubious human rights records, concerns over the rule of law, or that are ruled by authoritarian regimes.

IMPLICATIONS: Structural Problems with Dual-Use Markets

There are underlying structural problems with existing regulations, export control compliance, re-export and distribution practices, and aftermarket provision of services for dual-use technologies. Blue Coat is just one company in the marketplace for dual-use technology, albeit one with substantial notoriety. The global spread of its products documented in this report is thus only a slice of a much larger market. Yet more than a year of scrutiny of Blue Coat highlights the extent to which the sale of dual-use technology has become increasingly "normalized," if not ubiquitous.

Western technologies capable of surveillance and censorship now serve as standard network building blocks for Internet service providers (ISPs) around the world. Amidst this global technology transfer, evidence continues to emerge of unanticipated impacts on human rights. Yet these consequences are not well addressed either through regulatory, or self-regulatory mechanisms in the dual-use market. Even in cases where restrictions are explicit, or part of formalized sanctions and export control regimes, devices still make their way to governments in countries like Iran, Sudan, and Syria. Many more devices are present in countries with questionable records on human rights, surveillance, and the rule of law.

The market for dual-use technology lacks effective mechanisms for external accountability and transparency to civil society or export control regimes. This conclusion is reinforced by recent developments in export control and enforcement. In April 2013, the Office of Export Enforcement of the Bureau of Industry and Security (BIS) and the US Department of Commerce, after investigating the 2011 discovery of Blue Coat devices in Syria, obtained a US$2.8 million settlement from the UAE-based distributor of the Blue Coat devices in question, Computerlinks FZCO, for alleged violations of US Export Administration Regulations (EAR).[4] Blue Coat Systems has maintained that it lawfully sold its devices to Computerlinks FZCO only after which point the devices were unlawfully diverted and transshipped to Syria.[5]

4 "Order Relating to Computerlinks FZCO," US Department of Commerce, Bureau of Industry and Security, http://www.bis.doc.gov/news/2013/Computerlinks%20FZCO.pdf.

5 "Update on Blue Coat Devices in Syria," Blue Coat, December 15, 2011, http://www.bluecoat.com/company/news/update-blue-coat-devices-syria. In December 2011 the BIS added the two parties involved in purchasing the devices from Computerlinks FZCO and transshipping them to Syria to the BIS Entity List. That listing indicates that any license applications to export products to the two entities will be presumptively denied. See "BIS Adds Two Parties to Entity List for Sending Internet Filtering Equipment to Syria," Bureau of Industry and Security US Department of Commerce, http://www.bis.doc.gov/news/2011/bis_press12152011.htm; and "Supplement No. 4 to Part 744 - ENTITY LIST," Bureau of Industry and Security, US Department of Commerce, March 28, 2013, http://www.bis.doc.gov/policiesandregulations/ear/744_supp4.pdf.

The BIS concluded, based on its investigation, that Computerlinks FZCO was aware that the devices were destined for end-users in Syria, but provided false information on destination and end-user when placing the orders with Blue Coat.[6] The shipment ran contrary to a distribution agreement with Blue Coat that required Computerlinks FZCO to comply with US export laws and "additional safeguards specially applicable to Computerlinks FZCO." Additionally, according to the BIS, Computerlinks FZCO provided support in connection with the devices sold to Syrian entities that was "designed to help the end-user of the devices monitor the Web activities of individual Internet users and prevent users from navigating around censorship controls."[7] Meanwhile, further highlighting systemic issues of distributor malfeasance, Dell computer equipment was discovered in May 2013 to "have been sold to the Syrian government through a Dubai-based distributor," with arrangements for such sale reportedly made in late 2012.[8]

How should we address the sale of these tools to locations where the implementation of such technology has not been publicly debated or shaped by the rule of law? Cases like Computerlinks FZCO, the presence of Blue Coat in Iran, Sudan, and other countries with dubious human rights records illustrate the widely-recognized need for smarter, multilayered control of dual-use technologies. Industry, civil society, and the public sector all have a stake, and should all be consulted in the development of new control methods and export regimes. Multi-stakeholder discussion regarding distribution channels and compliance programs for dual-use technologies is crucial, as is an emphasis on corporate social responsibility, human rights due diligence, and enforcement of standards among partner entities. The issues raised by this latest report go beyond one company and its products and services, and underscore the need to address the global policy implications of internationally-marketed communications infrastructure and services.

REPORT STRUCTURE

The report is divided into three sections. Parts I and II explain our methods and report on the findings of our scanning for Blue Coat devices. In addition, Part II highlights cases of pressing concern given their significant human rights implications, including findings of devices in sanctioned countries (Iran, Sudan and Syria) as well as countries like Côte d'Ivoire and Thailand where we believe further investigation is warranted in light of the policy and rights context. Part II also contains a map of the locations of devices on public networks worldwide. Part III lays out the legal and policy considerations of our findings, and reiterates specific questions to Blue Coat Systems and its major investor, the Ontario Teachers' Pension Plan.

6 "Order Relating to Computerlinks FZCO," US Department of Commerce, Bureau of Industry and Security.

7 Ibid.

8 Ron Nixon, "Outwitting Sanctions, Syria Buys Dell PCs," *New York Times*, May 3, 2013, http://www.nytimes.com/2013/05/04/technology/dell-products-make-their-way-circuitously-to-syria.html?_r=2&.

PART I: METHODOLOGY

In *Planet Blue Coat*, Citizen Lab researchers utilized the Shodan Computer Search Engine,[9] network scanning, and manual investigation to enumerate the global distribution of Blue Coat devices. In addition to these methods, this new research draws on the anonymously published "Internet Census 2012."[10] We developed and refined a series of queries conducted against the Internet Census data that enabled us to identify Blue Coat devices of interest.

As with *Planet Blue Coat*, we focused primarily on Blue Coat ProxySG and PacketShaper appliances. ProxySG devices enable content filtering based on categories of content and work in conjunction with another Blue Coat technology called WebFilter, which Blue Coat markets as offering a highly granular degree of content blocking based on 82 categories.[11] The categories range from uncontroversial categories like "malicious sources" and "spam" to topics like "alternative spirituality/belief" or "religion."[12] To remain current, URL lists for each content category are regularly updated from Blue Coat servers. Blue Coat has sometimes attracted criticism for these categories, given the kind of control they offer to network administrators. Recently, for example, Blue Coat announced it would remove the "LGBTQ" category from its URL list after pressure from advocacy groups.[13] ProxySG also offers "SSL inspection" of users' encrypted sessions, which Blue Coat explicitly states solves "issues with intercepting SSL for your end-users."[14] PacketShaper devices provide a wide range of traffic classification management functions, including identifying and monitoring traffic generated by hundreds of common applications and traffic types and allowing a network administrator to filter or block them.[15]

9 "Shodan," http://www.shodanhq.com/

10 Carna Botnet, "Internet Census 2012: Port Scanning /0 Using Insecure Embedded Devices," 2012, http://internetcensus2012.bitbucket.org/paper.html.

11 "Blue Coat WebFilter Whitepaper," Blue Coat, http://www.bluecoat.com/sites/default/files/editor_files/BlueCoat_WebFilter_wp_v1c.pdf.

12 "Blue Coat Category Descriptions," Blue Coat, https://sitereview.bluecoat.com/catdesc.jsp.

13 "Blue Coat: Stop Allowing Department of Defense and Other Customers to Block LGBT Websites," GLAAD, http://www.glaad.org/lgbtwebfilter.

14 Tim Chiu, "The Growing Need for SSL Inspection," Blue Coat, June 18, 2012, https://www.bluecoat.com/security/security-archive/2012-06-18/growing-need-ssl-inspection.

15 "Blue Coat PacketShaper Application List," Blue Coat, http://www.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf.

SCANNING THE INTERNET CENSUS

The primary method used in this report was to search the Internet Census dataset for indicators of Blue Coat equipment of interest. We conducted a series of searches for text strings commonly found in Blue Coat device banners (*See Table 1*). The nine terabytes of scanning results that make up the Internet Census dataset are organized within that dataset by scan type, followed by the target network block or port.

TABLE 1 - This table specifies the strings we searched for that are associated with ProxySG and PacketShaper devices.[16]

PROTOCOL	PORT	QUERY[1]
TCP (FTP)	21	"BlueCoat", "ProxySG", "Packeteer", "PacketShaper"
TCP (Telnet)	23	"Using telnet exposes your password"
SNMP (v1, v3)	161	"BlueCoat", "ProxySG", "Packeteer", "PacketShaper"
TCP (HTTP)	80	"BlueCoat", "ProxySG", "Packeteer", "PacketShaper"
TCP (HTTP)	8081	"BlueCoat", "ProxySG", "Packeteer", "PacketShaper"
TCP (HTTPS)	8082	"BlueCoat", "ProxySG", "Packeteer", "PacketShaper"

1 Case sensitive.

We then validated the search results through a combination of manual and automated network investigation, including nmap, telnet, netcat, WhatWeb,[17] and Shodan.

The methodology of the Internet Census 2012 is controversial.[18] Data was gathered by scanning the technologies, networks, and devices that make up the Internet using a vast network of unsecured, publicly-connected devices. Owners neither consented to these scans, nor were they informed that the scanning was taking place, although the project included some efforts to mitigate certain adverse effects.[19] We have made use of the Internet Census dataset in this research because the data is in the public domain and provides an as of yet unreplicated high-level view of the Internet. However, the

16 These signatures were derived from publicly-accessible support documentation produced by the manufacturer, our own testing and experiences with live Blue Coat devices, and the work of independent network assessment tools, such as the open source scanner nmap.

17 "Urbanadventurer/WhatWeb," GitHub, https://github.com/urbanadventurer/WhatWeb/wiki.

18 Robert McMillan, "Botnet-Generated Map of Internet Gathered Data 'Unethically'," *Wired*, May 16, 2013, http://www.wired.co.uk/news/archive/2013-05/16/internet-census.

19 Judith Horchert and Christian Stöcker, "Mapping the Internet: A Hacker's Secret Internet Census," *Spiegel Online*, March 22, 2013, http://www.spiegel.de/international/world/hacker-measures-the-internet-illegally-with-carna-botnet-a-890413.html.

Citizen Lab does not condone research methods that may be unethical or illegal.[20] While we have drawn on the information contained within that dataset, we have run our own queries of publicly-accessible devices to confirm the network presence of Blue Coat ProxySG and PacketShaper appliances, resulting in independently verifiable findings.

RESULTS DATASET

https://citizenlab.org/wander-data

This dataset includes both the initial addresses derived from the Internet Census and the results of our verification process. The last octet of IP addresses have been removed in order to respect privacy and the security of networks.

DATASET CATEGORIES

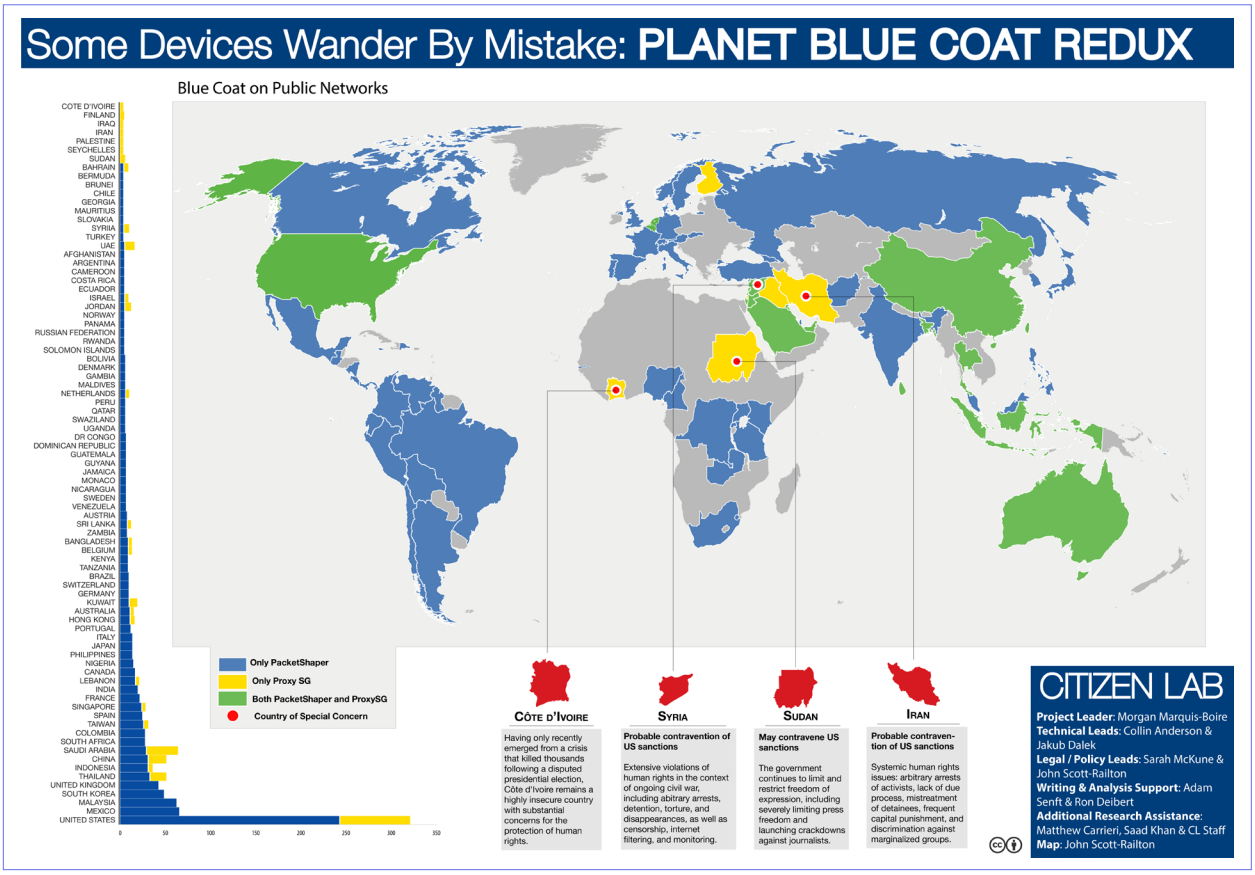
We developed three dataset categories, **Public, Public-Infrastructure**, and **Non-Public**, to facilitate analysis of the networks where we identified Blue Coat devices. The categories are derived from manual classification to differentiate between networks available to the general public and networks that do not meet this criterion. Our categories are meant to help determine implementations of interest. They should be considered a best guess or working categorization, not exhaustive statements of the activities of a particular ISP or network. Public networks include residential ISPs, and ISPs with mixed commercial and residential services. Public-Infrastructure networks include Tier 1 providers, Internet transit, international Internet gateways, peering facilities, Internet exchanges and so on. Non-Public networks include ISPs offering business services (but not residential service), educational networks, internal government networks, commercial networks, and so on.

20 For a further discussion of issues surrounding use of shared measurement data, see Mark Allman and Vern Paxson, "Issues and Etiquette Concerning Use of Shared Measurement Data," Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, 2007: 135-140. For a discussion of methods and ethics for Internet research generally, see Ronald Deibert and Masashi Crete-Nishihata, "Blurred Boundaries: Probing the Ethics of Cyberspace Research," *Review of Policy Research* 28, no. 5 (2011): 531-537.

PART II: FINDINGS

Citizen Lab found Blue Coat devices of interest (PacketShaper and ProxySG) on public networks in a wide range of countries (*See Figure 1*), and was able to confirm their presence in 83 countries (*See Table 2*).

FIGURE 1 - Global map of Blue Coat devices on public networks



To view a high resolution version of this map, please go to https://citizenlab.org/storage/bluecoat/fig1.jpg

TABLE 2 - Countries with verified Blue Coat devices on public networks

BOTH PROXYSG & PACKETSHAPER	PACKETSHAPER			PROXYSG
AUSTRALIA	AFGHANISTAN	GUATEMALA	QATAR	COTE D'IVOIRE
BAHRAIN	ARGENTINA	GUYANA	RUSSIAN FEDERATION	FINLAND
BANGLADESH	AUSTRIA	INDIA	RWANDA	IRAN
BELGIUM	BERMUDA	ITALY	SLOVAKIA (Slovak Republic)	IRAQ
CHINA	BOLIVIA	JAMAICA	SOLOMON ISLANDS	PALESTINE
HONG KONG	BRAZIL	JAPAN	SOUTH AFRICA	SEYCHELLES
INDONESIA	BRUNEI DARUSSALAM	KENYA	SPAIN	SUDAN
ISRAEL	CAMEROON	KOREA, REPUBLIC OF	SWAZILAND	
JORDAN	CANADA	MALAYSIA	SWEDEN	
KUWAIT	CHILE	MALDIVES	SWITZERLAND	
LEBANON	COLOMBIA	MAURITIUS	TANZANIA, UNITED REPUBLIC OF	
NETHERLANDS	CONGO, THE DRC	MEXICO	TURKEY	
SAUDI ARABIA	COSTA RICA	MONACO	UGANDA	
SINGAPORE	DENMARK	NICARAGUA	UNITED KINGDOM	
SRI LANKA	DOMINICAN REPUBLIC	NIGERIA	VENEZUELA	
SYRIAN ARAB REPUBLIC	ECUADOR	NORWAY	ZAMBIA	
TAIWAN	FRANCE	PANAMA		
THAILAND	GAMBIA	PERU		
UNITED ARAB EMIRATES	GEORGIA	PHILIPPINES		
UNITED STATES	GERMANY	PORTUGAL		

The installations highlighted in this section are a subset of the cases where we identified Blue Coat Systems filtering and monitoring products on public networks. We have highlighted Iran, Sudan, and Syria as three cases where Blue Coat devices are in operation despite sanctions and export control regimes. In addition, we highlight two 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: Côte d'Ivoire and Thailand.[21]

The Citizen Lab's focus is chiefly on devices located within environments that present a considerable potential for abuse of their latent capacity for filtering and surveillance. As *Table 2* indicates, these devices were found on a very wide range of countries that we do not address in detail. We suspect similar concerns apply to several other countries on this list, and we hope that other researchers and civil society groups will pursue these findings further.

It is also important to note that in our data and findings we differentiate between "accessible" and "inaccessible" devices. For the data that we include in the report's analysis, we only describe devices that were initially identified via the Internet Census, and further validated manually (hence "accessible"). In specific cases, however (Iran, Sudan, and Syria) we include tables in the body of the report (*Tables 3, 4, and 5*) that highlight all devices, both accessible and inaccessible to manual verification, and label them as such. Similarly, we include all instances found in the supplemental dataset provided with this report.

CÔTE D'IVOIRE

TYPE: ProxySG

NETWORK(S): Côte d'Ivoire Telecom

A Blue Coat ProxySG installation was found on the ISP Côte d'Ivoire Telecom, a company partially owned by France Telecom.[22] Having only recently emerged from a crisis that killed thousands following a disputed presidential election, Côte d'Ivoire remains a highly insecure country with substantial concerns for the protection of human rights. The country faces ongoing violence, reports of arbitrary detentions, torture, and threats to freedom of expression.[23] Reports have emerged of bloggers being arrested for their online writings, and former president Laurent Gbagbo had targeted critical and independent media websites for censorship.[24]

21 Additional information on countries identified as having Blue Coat which are not covered in detail here can be found in Part 2 and the appendix of "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools," Citizen Lab. For a more detailed examination of national-level Internet filtering practices, the legal and regulatory frameworks under which they are applied and concerns over risks to freedom of expression, transparency and due process, see country profiles produced by the OpenNet Initiative: "Country Profiles," OpenNet Initiative, https://opennet.net/research/profiles.

22 "Group's Activities in Côte d'Ivoire," Orange, http://www.orange.com/en/group/global-footprint/countries/Group-s-activities-in-Cote-d-Ivoire.

23 "Annual Report 2013: Côte D'Ivoire," Amnesty international, 2013, http://www.amnesty.org/en/region/cote-divoire/report-2013; and "World Report 2012: Côte d'Ivoire," Human Rights Watch, 2012, http://www.hrw.org/world-report-2012/c-te-d-ivoire.

24 "Alain Doh Bi," Global Voices Online, http://threatened.globalvoicesonline.org/blogger/alain-doh-bi; "Ivorian Bloggers Under Arrest for Allegedly Interfering with Disaster Recovery While Trying to Help," Global Voices Online, January 4, 2013, http://globalvoicesonline.org/2013/01/04/ivorian-bloggers-under-arrest-for-allegedly-interfering-with-disaster-recovery-while-trying-to-help; and Théophile Kouamouo, Global Voices Online, http://threatened.globalvoicesonline.org/blogger/théophile-kouamouo; and "Gbagbo Camp to Block Access to Independent and Opposition Websites," Reporters Without Borders, March 30, 2011, http://en.rsf.org/cote-d-ivoire-gbagbo-camp-to-block-access-to-30-03-2011,39916.html.

IRAN

TYPE: ProxySG

NETWORKS: Max Net, Information Technology Company (Iranian Ministry of Communication), Datak Telecom, Shahrad Network.

SANCTIONS: http://www.treasury.gov/resource-center/sanctions/Programs/pages/iran.aspx

This report has identified six active Blue Coat devices on a number of networks in Iran, including a ProxySG device on residential ISP Max Net and an additional Blue Coat device on the network of the Information Technology Company, an entity created by the Ministry of Communication and Information Technology to implement filtering nationwide.[25]

Iran is implicated in a myriad of systemic human rights concerns, including arbitrary arrests of activists, lack of due process, mistreatment of detainees, frequent application of capital punishment, and discrimination against marginalized groups.[26] Abuses are reported to have increased in the lead up to the 2013 presidential elections, including a spate of blogger arrests and an increase in censorship.[27] There have been a number of high-profile incidents of surveillance and targeted malware attacks against Internet users. Prior Citizen Lab research has identified compromised versions of Simurgh, a popular censorship circumvention tool, which exfiltrated data and logged keystrokes of unsuspecting users.[28] A number of Western technology companies have also been implicated in the sale of surveillance and tracking systems to Iranian law enforcement and security agencies.[29]

In 2011, an attack was made on Iranian targets using a fraudulent SSL certificate issued by a compromised certificate authority. The objective of the attack appeared to be to intercept the private communications of Gmail users in Iran.[30] The attacker claimed to be an individual Iranian who had chosen to help the government monitor individuals' communications.[31] In light of this, the discovery of devices in Iran which purport to offer "SSL Inspection" capabilities is especially concerning.

Without a specific license, the provision of Blue Coat devices and services to ISPs in Iran may contravene US sanctions.

25 "After the Green Movement: Internet Controls in Iran, 2009-2012," OpenNet Initiative, 2013, https://opennet.net/blog/2013/02/after-green-movement-internet-controls-iran-2009-2012.

26 "Annual Report 2013: Iran," Amnesty International, 2013, http://www.amnesty.org/en/region/iran/report-2013#page.

27 For example, see "Middle East and North Africa CyberWatch - April 2013," Citizen Lab, May 6, 2013, https://citizenlab.org/2013/05/middle-east-and-north-africa-cyberwatch-april-2013; and "Iran: Threats to Free, Fair Elections," Human Rights Watch, May 24, 2013, http://www.hrw.org/news/2013/05/24/iran-threats-free-fair-elections.

28 "Iranian Anti-Censorship Software 'Simurgh' Circulated with Malicious Backdoor (Updated)," Citizen Lab, May 25, 2012, https://citizenlab.org/2012/05/iranian-anti-censorship-software-simurgh-circulated-with-malicious-backdoor-2.

29 "After the Green Movement," OpenNet Initiative.

30 "DigiNotar Certificate Authority Breach, 'Operation Black Tulip,'" September 5, 2011, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf.

31 "Hacker Rattles Security Circles," *New York Times*, September 11, 2011, http://www.nytimes.com/2011/09/12/technology/hacker-rattles-internet-security-circles.html?pagewanted=all.

TABLE 3 - Full list of Blue Coat devices in Iran

IP	ASN	ACCESSIBLE	PRODUCT	LOCATION ASSESSMENT
217.219.227.x	DCI-AS Information Technology Company (ITC)	YES	BlueCoat Generic	Government
81.91.145.x	DATAK DATAK Internet Engineering, Inc	YES	BlueCoat Generic	Residential ISP
92.50.28.x	SHAHRAD-AS Shahrad Net Company Ltd.	YES	BlueCoat Generic	Residential ISP
92.50.28.x	SHAHRAD-AS Shahrad Net Company Ltd.	YES	BlueCoat Generic	Residential ISP
128.140.1.x	MAxNET-AS Bozorg Net-e Aria	YES	ProxySG	Residential ISP
217.218.15.x	DCI-AS Information Technology Company (ITC)	YES		Government
217.219.227.x	DCI-AS Information Technology Company (ITC)	NO		Government
217.219.4.x	DCI-AS Information Technology Company (ITC)	NO		Government
77.237.91.x	RESPINA-AS Respina Networks & Beyond PJSC	NO		Commercial ISP
5.34.200.x	RASANE-AS Samaneh Sama Pishro Persian Communications and Information Development Company PJS	NO		Commercial
194.225.17.x	IRANET-IPM Research Center of Theoretical Physics & Mathematics (IPM)	NO		Education
109.122.208.x	JAHANONLINE Jahan Ruye Khat	NO		Residential ISP
213.217.40.x	PARSONLINE PARSONLINE Autonomous System	NO		Residential ISP

SUDAN

TYPE: ProxySG

NETWORK: Canar Telecom

SANCTIONS: http://www.treasury.gov/resource-center/sanctions/Programs/pages/sudan.aspx

This report has identified the presence of a Blue Coat ProxySG device on the consumer ISP Canar Telecom. Sudan continues to face numerous human rights concerns as a result of ongoing violence and crackdowns against dissidents and opposition political figures. Widespread violence and instability continues on numerous fronts, including Darfur and as a result of ongoing post-independence

negotiations with South Sudan.[32] Sudan's government continues to limit and restrict freedom of expression, including severely limiting press freedom and launching crackdowns against journalists.[33] Online activists, bloggers, and journalists have also been arrested and deported, while reports have indicated that Sudanese ISPs have censored news websites covering sensitive political protests.[34] Unless a specific license was issued, it is probable that the provision of Blue Coat devices and related services to Canar Telecommunications contravenes US sanctions.

TABLE 4 - Full list of Blue Coat devices in Sudan

IP	ASN	ACCESSIBLE	PRODUCT	LOCATION ASSESSMENT
197.254.192.x	KANARTEL	NO		Residential ISP
197.254.192.x	KANARTEL	YES	ProxySG	Residential ISP
197.254.192.x	KANARTEL	YES	ProxySG	Residential ISP
197.254.192.x	KANARTEL	YES	ProxySG	Residential ISP

SYRIA

TYPE: ProxySG

NETWORK: Syrian Telecommunications Establishment

SANCTIONS: http://www.treasury.gov/resource-center/sanctions/Programs/pages/syria.aspx

This report has identified the presence of Blue Coat devices on networks operated by the state-owned Syrian Telecommunications Establishment, confirming past Citizen Lab findings and widespread reports.[35] Syria continues to face substantial human rights concerns as a result of its two year old civil war which is estimated to have killed at least 80,000 people.[36] Tens of thousands of individuals have been subjected to arbitrary arrest, detention, torture, and disappearances, and domestic and international journalists have been killed and detained for their reporting on the crisis.[37]

The ongoing conflict has extended into the online realm on a number of fronts. Previous Citizen Lab

32 "World Report 2013: Sudan," Human Rights Watch, 2013, http://www.hrw.org/world-report/2013/country-chapters/sudan.

33 "Annual Report 2013: Sudan," Amnesty International, 2013, http://www.amnesty.org/en/region/sudan/report-2013.

34 Eva Galperin, "Sudan Revolts, Government Cracks Down on Dissent," Electronic Frontier Foundation, July 10, 2012, https://www.eff.org/deeplinks/2012/07/sudan-revolts-government-cracks-down-dissent; and "Sudanese Blogger Detained Without Charge," *The Guardian*, July 27, 2012, http://www.guardian.co.uk/media/greenslade/2012/jul/27/journalist-safety-sudan.

35 "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 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.

36 "Syria Death Toll At Least 80,000, says U.N. General Assembly President," Reuters, May 15, 2013, http://in.reuters.com/article/2013/05/15/syria-crisis-un-deaths-idINDEE94E0CJ20130515.

37 "World Report 2013: Syria," Human Rights Watch, http://www.hrw.org/world-report/2013/country-chapters/syria; and "Annual Report 2013: Syria," Amnesty International, http://www.amnesty.org/en/region/syria/report-2013.

research has documented the emergence of the Syrian Electronic Army, a group who have targeted opposition activists and compromised a number of high profile international media outlets.[38] Citizen Lab research has also identified the use of remote surveillance software against Syrian activists.[39]

While the highly-publicized installations of Blue Coat ProxySG devices in Syria were found to be a principle mechanism for content filtering, the Citizen Lab has not at this time attempted to determine whether these devices were being used for censorship or surveillance purposes.[40]

Unless a specific license was issued, it is probable that the provision of Blue Coat devices and related services to the Syrian Telecommunications Establishment contravenes US sanctions.

TABLE 5 - Full list of Blue Coat devices in Syria

IP	ASN	ACCESSIBLE	PRODUCT	LOCATION ASSESSMENT?[1]
91.144.8.x	EXT-PDN-STE-AS Syrian Telecommunications Establishment	YES	PacketShaper	ISP*
188.160.1.x	ExT-PDN-STE-AS Syrian Telecommunications Establishment	YES	ProxySG	ISP*
188.160.1.x	ExT-PDN-STE-AS Syrian Telecommunications Establishment	YES	ProxySG	ISP*
82.137.217.x	ExT-PDN-STE-AS Syrian Telecommunications Establishment	YES	ProxySG	ISP*
91.144.44.x	EXT-PDN-STE-AS Syrian Telecommunications Establishment	NO		ISP*
91.144.8.x	EXT-PDN-STE-AS Syrian Telecommunications Establishment	NO		ISP*

1 It is inherently difficult to categorize Syrian IP addresses, because the majority of routable Syrian IPs are assigned a very limited number of ASN names that are not descriptive.

38 Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," Information Warfare Monitor, May 30, 2011, http://www.infowar-monitor.net/2011/05/7349; and Nicole Perlroth, "Hunting for Syrian Hackers' Chain of Command," *New York Times*, May 18, 2013, http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?_r=0.

39 "Syrian Activists Targeted with BlackShades Spy Software," Citizen Lab, June 19, 2012, https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software.

40 "BlueCoat's Presence in Syria Finally Uncovered," Reflets.info, October 29, 2011, http://reflets.info/bluecoats-presence-in-syria-finally-uncovered.

THAILAND

TYPE: ProxySG, PacketShaper, CacheFlow, Reporter

NETWORKS: Communication Authority of Thailand, SheepLink, SiamData, Jastel Network Company Limited, Triple T Internet Co., True Internet, TOT, NTT Communications, Metrabyte, Prince of Songkla University, KSC Commercial Internet, Proen Internet, King Mongkut's Institute of Technology North Bangkok, World Internetwork Co., Jasmine Internet Company, CS LoxInfo, Samart Infonet, Internet Solution and Service Provider, Netway Communications, UniNet Thailand

This report documents a large number of active Blue Coat devices in use in Thailand, including a ProxySG on the network of the state-owned Communication Authority of Thailand. The finding of Blue Coat devices in Thailand is of note as the country has a long history of censoring critical speech and cracking down against critical voices. Oppositional political content has long been censored in the country, often on the basis of lèse-majesté laws that forbid making insulting or defamatory remarks about the monarchy.[41] The same rationale has frequently been used to arrest and punish bloggers for their online postings and intermediaries for content hosted on their sites.[42]

41 "Thailand," in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, eds. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge: MIT Press, 2012).

42 See "Southeast Asia Cyber Watch—May 2012," Citizen Lab, June 8, 2012, https://citizenlab.org/2012/06/southeast-asia-cyber-watch-issue-1/#th; and "Southeast Asia CyberWatch—September 2012," Citizen Lab, September 28, 2012, https://citizenlab.org/2012/09/southeast-asia-cyberwatch-september-2012/#thailand.

PART III: LEGAL AND POLICY CONSIDERATIONS

In *Planet Blue Coat*, the Citizen Lab laid out a number of the legal, policy, and ethical issues that are raised by the global trade of dual-use and other rights-impacting technologies. We also urged Blue Coat Systems, as well as other company participants in this industry, to engage in constructive dialogue around a series of questions related to the human rights impacts of their products and practices. We noted that the time has come "to examine the appropriate course of action for companies that participate in the industry for network surveillance, censorship and other sensitive technologies."

At present that invitation to dialogue remains unanswered. Since the publication of *Planet Blue Coat*, we have also written follow-up letters to, but received no direct response from, Blue Coat Systems and its investor, Ontario Teachers' Pension Plan (OTPP), which as we noted in a February 2013 op-ed, holds a significant stake in Blue Coat, as well as a seat on the Blue Coat board.[43] Yet company-driven implementation of corporate social responsibility measures, complemented with action from investors that subscribe to principles of responsible investing, is an essential element of addressing the issues raised. Particularly in an industry such as this in which transparency is sorely lacking, company participants may be the only entities that possess the knowledge required to fully define the scope of the problem and create solutions that work in practice.

Building on *Planet Blue Coat*, this section examines additional legal and policy issues relevant to our latest technical findings which we hope Blue Coat and other stakeholders will build upon in order to engage in dialogue. In particular, we:

- Summarize the US sanctions provisions applicable to the discovery of Blue Coat devices in certain countries;
- Assess the ramifications of current US export control regulations for exports of Blue Coat devices and other dual-use technologies to countries that are not sanctioned yet still present human rights concerns;
- Explore the question of why the products of an industry leader like Blue Coat Systems, which employs a global trade compliance team as well as in-house and outside legal counsel, would appear in sanctioned countries – raising significant concerns surrounding the global distribution of dual-use technology and resulting human rights violations.

43 Ron Deibert and Sarah McKune, "Teachers' Pension Plan Invests in Internet Surveillance Firm," *Toronto Star*, February 6, 2013, http://www.thestar.com/opinion/editorialopinion/2013/02/06/teachers_pension_plan_invests_in_internet_surveillance_firm.html.

Blue Coat Systems may yet take steps toward engaging on these issues, and we encourage them to do so, including with respect to the recommendations outlined in the conclusion section below. It is noteworthy that in a February 2013 commentary, "Enabling a Safe and Productive Internet," Blue Coat Systems stated:

> Blue Coat respects and supports freedom of expression, which the U.N. has declared to be a universal human right for all people. We do not design our products or condone their use to suppress human rights. . . . Throughout 2013 we will continue to engage key stakeholders, including our channel partners, to review what further steps we can take to limit misuse of our products. As we do so, we will continue to evaluate policies and processes that support our principles and further our mission to provide products that enable an open, safe and more productive Internet.[44]

If undertaken in a transparent manner, such action could serve as a welcome and necessary catalyst for an industry-led solution to the control of rights-impacting technologies.

BLUE COAT DEVICES IN COUNTRIES IN CONTRAVENTION OF US SANCTIONS

Citizen Lab found evidence of Blue Coat devices operating in Iran, Sudan, and Syria, all of which are subject to comprehensive US sanctions. It appears that the presence of these devices are in contravention of sanctions provisions, raising questions regarding Blue Coat Systems' compliance measures, and the ease of access by authoritarian regimes to Western-made dual-use technologies despite extensive US sanctions regimes.

Sanctions, as foreign policy instruments, are not typically limited to targeting the sale and transfer of dual-use technologies. However, they are often the primary control measure to which companies in this industry respond, as they present relatively bright-line standards – violations of which may result in serious monetary and other penalties. Sanctions are thus one of various methods to prevent the provision of devices capable of network surveillance and content filtering to authoritarian regimes.

The effectiveness of sanctions in properly limiting sales of rights-impacting technologies remains a subject of debate, given their potential for over- or under-inclusiveness.[45] The public and private sectors have struggled with how to properly balance the nuanced goals of limiting the export of potentially infringing technologies with securing individual access to vital personal communications services in

44 David Murphy, "Enabling a Safe and Productive Internet," Blue Coat, February 15, 2013, http://www.bluecoat.com/company-blog/2013-02-15/enabling-safe-and-productive-internet.

45 For example, see Access Now, The Center for Democracy and Technology, Collin Anderson, The Committee to Protect Journalists, and The New America Foundation's Open Technology Institute, "Comments to the U.S. Department of State in response to Public Notice 8086, the State Department Sanctions Information and Guidance, issued on November 8, 2012," January 12, 2013, http://newamerica.net/sites/newamerica.net/files/profiles/attachments/SensitiveTechnologiesComments.pdf.

sanctioned countries.[46] Regulators and private entities retain the difficult responsibility of distinguishing between problematic cases, and situations that may serve socially beneficial purposes. A chilling effect has at times resulted from concern over potential ramifications of enforcement actions by authorities, such that companies often overregulate services that fall within existing legal exemptions and serve a significant public good. Hence, export controls, compliance policies, and the public discourse surrounding dual-use technologies require nuance in language itself and in adherence. In the absence of specific attention to the proliferation of such technologies within export control frameworks, however, comprehensive sanctions are one of the few legal impediments to the provision of devices capable of surveillance and censorship to some of the world's most authoritarian regimes.

In line with these pressing concerns, our findings include evidence of Blue Coat devices active on public networks in Iran, Sudan, and Syria. These countries are subject to comprehensive US sanctions programs with which Blue Coat Systems, a US company, must comply. More limited US sanctions also apply with respect to other countries in which we have found Blue Coat installations, namely, to specially designated nationals[47] of Côte d'Ivoire,[48] Iraq,[49] Lebanon,[50] Liberia,[51] and Zimbabwe.[52] However, these provisions do not appear to preclude the export of Blue Coat products to network providers in these countries.

46 Licensing of personal communications technologies for use by individuals in Iran is a case in point. On May 30, 2013, the Office of Foreign Assets Control, US Department of the Treasury, issued a new "General License with Respect to the Exportation and Re-exportation of Certain Services, Software, and Hardware Incident to the Exchange of Personal Communications," which supplemented the items authorized for export to Iran in prior general licenses with fee-based personal communications services and software, as well as consumer-grade Internet connectivity services and a variety of mobile, personal computing, and computer security-related equipment. This action was taken in light of concerns raised by activists and others that, because of existing sanctions, the Iranian people were unable to obtain essential technologies that would support their ability to securely access information and communicate online. See US Department of the Treasury, "United States Takes Action to Facilitate Communications by the Iranian People and Targets Iranian Government Censorship," May 30, 2013, http://www.treasury.gov/press-center/press-releases/Pages/jl1961.aspx; and Terry Atlas, "US to Ease Iran Sanctions on Laptops, Mobile Phones," *Bloomberg*, May 29, 2013, http://www.bloomberg.com/news/2013-05-29/u-s-to-ease-iran-sanctions-on-laptops-mobile-phones.html. Similar action was taken in Canada: on May 29, 2013, Minister of Foreign Affairs John Baird announced "Regulations Amending the Special Economic Measures (Iran) Regulations," which included an exemption for "equipment, services and software that facilitate secure and widespread communications via information technologies, or the provision or acquisition of financial services in relation to such equipment, services and software, provided that an export permit has been issued in respect of any goods listed in the Guide." See Foreign Affairs and International Trade Canada, *Regulations Amending the Special Economic Measures (Iran) Regulations*, May 29, 2013, http://www.international.gc.ca/sanctions/iran developments-developpements iran3.aspx, at Amendment 5.

47 "SDN Search," US Office of Foreign Assets Control, http://sdnsearch.ofac.treas.gov/default.aspx.

48 Executive Order no. 13,396, 31 CFR Part 543 blocks the property of persons and entities identified as contributing to the political and social unrest in Côte d'Ivoire.

49 As implemented in the Iraq Stabilization and Insurgency Sanctions Regulations at 31 CFR Part 576, the US 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 US 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.

50 Executive Order no. 13,441, 31 CFR Part 549 blocks the property of persons and entities identified as having undermined Lebanon's democratic processes or institutions or rule of law, or supported Syrian interference in Lebanon.

51 Executive Order no. 13,348, 31 CFR Part 593 blocks the property of persons identified as family members of Charles Taylor or senior officials or associates of the former regime led by Charles Taylor, and related entities.

52 Executive Orders no. 13,288, 13,391, and 13,469, 31 CFR Part 541, block the property of persons identified as officials of the government of Zimbabwe, having undermined Zimbabwe's democratic processes or institutions, or having engaged in human rights abuses, including President Robert Mugabe and those associated with him, as well as related entities.

IRAN

A broad US sanctions regime exists with respect to Iran, covering a myriad of transactions and multiple industries. Of particular relevance to trade in dual-use technology products are the Iranian Transaction and Sanctions Regulations.[53] According to 31 CFR § 560.204:

> Except as otherwise authorized pursuant to this part, and notwithstanding any contract entered into or any license or permit granted prior to May 7, 1995, the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran is prohibited, including the exportation, reexportation, sale, or supply of any goods, technology, or services to a person in a third country undertaken with knowledge or reason to know that:
>
> (a) Such goods, technology, or services are intended specifically for supply, transshipment, or reexportation, directly or indirectly, to Iran or the Government of Iran; or
>
> (b) Such goods, technology, or services are intended specifically for use in the production of, for commingling with, or for incorporation into goods, technology, or services to be directly or indirectly supplied, transshipped, or reexported exclusively or predominantly to Iran or the Government of Iran.

Accordingly, unless an exception or license applies, US companies such as Blue Coat Systems cannot export products to Iran or to a distributor that the company has reason to know may transship to Iran.

As for the general licenses available pursuant to Subpart E of 31 CFR Part 560,[54] none appear applicable to the products and services offered by Blue Coat Systems. The most relevant of these licenses is contained in § 560.540: "Exportation of certain services and software incident to Internet-based communications." This license authorizes the export "to persons in Iran of services incident to the exchange of personal communications over the Internet" when such services "are publicly available at no cost to the user." It also authorizes export of software necessary to enable such services if that software is publicly available at no cost to the user, and is either (a) not subject to the EAR, (b) designated as EAR99, or (c) classified as mass market software under ECCN 5D992 of the EAR (*See Appendix A for further information*).[55] However, the Blue Coat product at issue would not meet these criteria, given that it is fee-based, was provided to an ISP in Iran rather than for personal

53 Parts 535 and 560-562 of Title 31 of the CFR implement provisions of legislation and executive orders enacting sanctions against Iran, including the *Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA) and the Iran Threat Reduction and Syria Human Rights Act of 2012. See Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010*, http://www.treasury.gov/resource-center/sanctions/Documents/hr2194.pdf, and *Iran Threat Reduction and Syria Human Rights Act of 2012*, http://www.treasury.gov/resource-center/sanctions/Documents/hr_1905_pl_112_158.pdf.

54 31 CFR § 560.501 et seq.

55 See also 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.

communications use by individuals, and falls under an ECCN other than 5D992 (*See Appendix A*).[56]

Thus, unless a specific license was obtained by Blue Coat Systems to export the device in use by Max Net, Information Technology Company (Iranian Ministry of Communication), Datak Telecom, and Shahrad Network, it is probable that the provision of that product and related services contravenes US sanctions. No record of a license application from Blue Coat Systems for export of devices to Iran exists in the most up-to-date database released by the US Department of Treasury.[57]

SUDAN

In response to the violent conflict and human rights violations taking place over many years in Sudan, particularly in the Darfur region, and the state's support of terrorism, the US has maintained strict sanctions against the country.[58] According to the Sudanese Sanctions Regulations, "Except as otherwise authorized, the exportation or reexportation, directly or indirectly, to Sudan of any goods, technology (including technical data, software, or other information) or services from the United States or by a United States person, wherever located, or requiring the issuance of a license by a Federal agency, is prohibited."[59] While certain transactions, including to "Specified Areas of Sudan,"[60] are exempted from this prohibition,[61] and a general license exists for services and software incident to the exchange of personal communications over the Internet (identical to the Iran general license described above),[62] the Blue Coat devices at issue do not fit the criteria for such exemptions or license.

The Sudanese Sanctions Regulations also indicate that "exportation of goods or technology (including technical data, software, and information not exempted from the prohibition of this part pursuant to § 538.211, or technical assistance) from the United States to third countries is prohibited if the exporter knows, *or has reason to know*, that the goods or technology are intended for transshipment to Sudan (including passage through, or storage in, intermediate destinations)" (emphasis added).[63] Accordingly, even if companies have no direct knowledge that downstream distributors in other locations will transship goods or services to Sudan, should they have reason to know transshipment may occur at

56 On May 30, 2013, the Office of Foreign Assets Control (OFAC), US Department of the Treasury, issued a new "General License with Respect to the Exportation and Reexportation of Certain Services, Software, and Hardware Incident to the Exchange of Personal Communications," which supplemented the items authorized for export to Iran in prior general licenses with fee-based personal communications services and software, as well as consumer-grade Internet connectivity services and a variety of mobile, personal computing, and computer security-related equipment. However, it appears that Blue Coat devices remain outside the scope of the terms of this license; and, as this general license became effective as of May 30, 2013, it does not apply to the Blue Coat installations documented in this report, which were discovered well before that date.

57 Unlike Department of Commerce records, OFAC activities are subject to Freedom of Information Act requests.

58 "Sudan," US Department of the Treasure Office of Foreign Assets Control, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/sudan.pdf.

59 31 CFR § 538.205.

60 The term "Specified Areas of Sudan means Southern Kordofan/Nuba Mountains State, Blue Nile State, Abyei, Darfur, and marginalized areas in and around Khartoum." The term "marginalized areas in and around Khartoum means the following official camps for internally displaced persons: Mayo, El Salaam, Wad El Bashir, and Soba." 31 CFR § 538.320. Blue Coat devices do not appear to be located in these areas.

61 31 CFR § 538.212.

62 31 CFR § 538.533.

63 31 CFR § 538.411.

some point in the distribution chain, they are still prohibited from engaging in the transaction.

Thus, unless a specific license was obtained by Blue Coat Systems to export the device in use by Canar Telecommunications, the provision of that product and related services contravenes US sanctions.

SYRIA

Three Blue Coat devices were found on networks of the Syrian Telecommunications Establishment, a state-owned entity that is a part of Syria's Ministry of Telecommunications and Technology and controls telecommunications infrastructure in Syria.[64] These installations merit particular scrutiny in light of the BIS investigation of and settlement with Computerlinks FZCO concerning the unlawful export of Blue Coat devices to Syria.

US sanctions covering Syria are quite robust, as reflected in the Syria Accountability and Lebanese Sovereignty Restoration Act of 2003 (SAA),[65] Syrian Sanctions Regulations,[66] the Iran Threat Reduction and Syria Human Rights Act of 2012, and a series of executive orders on Syria. Section 5(a)(1) of the SAA required the president to "prohibit the export to Syria of any item, including the issuance of a license for the export of any item, on the United States Munitions List or Commerce Control List of dual-use items in the Export Administration Regulations (15 CFR Part 730 et seq.)." This effectively prevented export of Commerce Control List (CCL) items such as dual-use information security products (see discussion of classification of Blue Coat products under the EAR below).[67] Moreover, pursuant to sections 5(a)(1) and 5(a)(2)(A) of the SAA, in Executive Order no. 13,338, "Blocking Property of Certain Persons and Prohibiting the Export of Certain Goods to Syria,"[68] then-President Bush extended such prohibition not only to items on the CCL but to all US products with the exception of food and medicine:

> Except to the extent provided in regulations, orders, directives, or licenses that may be issued pursuant to the provisions of this order in a manner consistent with the SAA, and notwithstanding any license, permit, or authorization granted prior to the effective date of this order, (i) the Secretary of Commerce shall not permit the exportation or reexportation to Syria of any item on the Commerce Control List (15 C.F.R. part 774); and (ii) with the exception of food and medicine, the Secretary of Commerce shall not permit the exportation or reexportation to Syria of any product of the United States not included in section 1(b)(i) of this order.[69]

64 "Freedom on the Net: Syria," Freedom House, 2012, http://www.freedomhouse.org/report/freedom-net/2012/syria. ("The Syrian government regulates and controls the internet via the state-owned Syrian Telecommunication Establishment (STE), which owns all telecommunications infrastructure. The STE is a government body established in 1975 as a part of the Ministry of Telecommunications and Technology. In addition to its regulatory role, the STE also serves as an ISP.")

65 See "Syria Accountability and Lebanese Sovereignty Restoration Act of 2003," http://www.gpo.gov/fdsys/pkg/PLAW-108publ175/pdf/PLAW-108publ175.pdf.

66 See 31 CFR Part 542, which implements provisions of legislation and executive orders pertaining to Syria.

67 See 15 CFR Part 774.

68 Executive Order no. 13,338.

69 Section 1(b).

Certain exceptions to this prohibition exist pursuant to the national security waiver elaborated in section 5(b) of the SAA and section 7 of Executive Order no. 13,338, which are detailed in Department of Commerce's General Order No. 2 to Supplement No. 1, 15 CFR Part 736.[70] However, the items included in that General Order[71] do not appear to cover Blue Coat devices (*see discussion of classification of Blue Coat products under the EAR below*). As such, the Blue Coat products at issue remain subject to the general policy of denial that the BIS has in place for licensing of exports to Syria.[72]

Subsequent legislation and executive orders have further tightened the sanctions regime applicable to Syria. These include measures to block property and interests in property of the Syrian government[73] and other persons or entities identified as linked to human rights abuses (as represented on the Specially Designated Nationals List),[74] as well as a prohibition on "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."[75]

Thus, unless Blue Coat Systems obtained a specific license from the BIS—which appears highly unlikely given the BIS general policy of denial on exports to Syria, its recent findings concerning the unlawful export of other Blue Coat devices to Syria, and the links between the Syrian Telecommunications Establishment and the Syrian government—the provision of Blue Coat devices and related services to the Syrian Telecommunications Establishment contravenes US sanctions.

70 15 CFR Part 736.

71 "Items in support of activities, diplomatic or otherwise, of the United States Government (to the extent that regulation of such exportation or reexportation would not fall within the President's constitutional authority to conduct the nation's foreign affairs); medicine (on the CCL) and medical devices (both as defined in Part 772 of the EAR); parts and components intended to ensure the safety of civil aviation and the safe operation of commercial passenger aircraft; aircraft chartered by the Syrian Government for the transport of Syrian Government officials on official Syrian Government business; telecommunications equipment and associated computers, software and technology; and items in support of United Nations operations in Syria."

72 See 15 CFR § 746.9(c). Additionally, an OFAC general license exists for "services incident to the exchange of personal communications over the Internet." See Office of Foreign Assets Control, General License No. 5, "Exportation of Certain Services Incident to Internet-Based Communications Authorized," http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_gl5.pdf. However, that license contains similar parameters as the general licenses applicable to such services in Iran and Sudan, which as noted above do not cover Blue Coat devices.

73 Defined as "the Government of the Syrian Arab Republic, its agencies, instrumentalities, and controlled entities." See Executive Order no. 13,582, at Sec. 2(b), http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_eo_08182011.pdf.

74 It should be noted that OFAC has issued a general license authorizing "exportation or reexportation of items to Syria from the United States or by a US person, wherever located, to any person, including the Government of Syria, whose property and interests in property are blocked" under these measures, "provided that the exportation or reexportation of such items to Syria is licensed or otherwise authorized by the Department of Commerce." Office of Foreign Assets Control, General License No. 4A, "Exports or Reexports to Syria of Items Licensed or Otherwise Authorized by the Department of Commerce Authorized; Exports or Reexports of Certain Services Authorized," April 27, 2012, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_gl4a.pdf. However, the effect of this license is simply to reiterate that the licensing of exports to Syria is pursuant to the BIS rather than OFAC authorization—and as explained above, the BIS maintains a general policy of denial regarding licenses for exports to Syria, with a few narrow exceptions.

75 Executive Order no. 13,582, at Sec. 2(b).

LIMITATIONS ON CONTROL OF DUAL-USE TECHNOLOGIES SUCH AS BLUE COAT DEVICES THROUGH EXPORT REGULATIONS

Controlling the spread of dual-use technologies for end-uses that may compromise human rights is a more difficult problem when the final destination of the product is a country that is not subject to US sanctions, yet still presents significant human rights concerns. Those concerns may be due to government crackdowns, a lack of robust rule of law, or lack of protections for freedoms of expression and association, privacy, or other rights. In such a scenario, export regulations are one of the few applicable control methods. Yet, existing export regulations do not fully address the goal of controlling certain technologies for human rights reasons, and application of such export controls is inadequate to prevent potentially harmful sales Blue Coat devices, for example, are exported on the basis of a license exception that broadly permits exports to non-sanctioned destinations without requiring license approval from the BIS. In order to rely on export regulations to curb the spread of dual-use technologies used to compromise human rights, export control reforms as well as greater company transparency are required.

In addition to compliance with US sanctions regimes, US companies such as Blue Coat Systems must also comply with broader US export control regulations, which in turn incorporate international commitments under the Wassenaar Arrangement.[76] Exports of US products that are dual-use (having both military/strategic and commercial applications) or occasionally civil use in nature are primarily governed by the US Export Administration Regulations, 15 CFR Chapter VII, Subchapter C, with licensing carried out by the Bureau of Industry and Security at the US Department of Commerce. Pursuant to the EAR, items designated on the Commerce Control List—Supplement No. 1 to § 774.1 of the EAR—may require a license to export depending on their destination and, in some instances, their end-use or end-user.[77] As these are the main provisions governing corporate export practices in the US, and are buttressed by existing enforcement mechanisms and bodies, much debate has centered around the extent to which such regulations can be employed to prevent harmful sales of dual-use technologies to destinations around the world.

Ascertaining whether the current export regulations can in fact be used to effectively control dual-use technology sales requires consideration of multiple factors, including: whether the products in question would be controlled under the EAR, and if so pursuant to which Export Control Classification Number (ECCN); whether those controls would trigger a licensing requirement (as opposed to qualifying for a license exception or "no license required"); and, if a licensing requirement is triggered, how the BIS would evaluate the probability of harm resulting from the export in deciding on the license application, including whether a mandated presumption of license denial or approval applies. However, determining whether a particular product would require a license to export under the EAR, and if so, pursuant to which provisions, is a complex process that depends heavily on the technical specifications of the

76 The Wassenaar Arrangement is a multilateral export control regime covering conventional arms and dual-use goods and technologies, which currently includes 41 countries as members. Participating countries—including the US, Canada, a number of European countries, and Russia—commit to maintain national export controls on Wassenaar-listed items, which include items related to "telecommunications" (Category 5, Part 1) and "information security" (Category 5, Part 2). "How Does the Wassenaar Arrangement Work?," Wassenaar Arrangement, http://www.wassenaar.org/introduction/howitworks.html.

77 See 15 CFR § 736.2(a).

item and the location and entity to which the item is exported. This information is typically within the exclusive purview of the exporting company, which submits license applications to the BIS on a confidential basis[78] after engaging in its own internal evaluation and compliance processes. As a result, determining with certainty the scope of regulations and licensing requirements that govern the export of a particular product is generally not possible without some disclosure from the company itself.

In the case of Blue Coat devices, Blue Coat Systems released an export control product matrix[79] in May 2013 detailing the classification of its products under the EAR. Companies may maintain export control product matrices to assist in internal evaluation and classification of items for export. Making those matrices publicly available enhances the transparency surrounding the export of dual-use technologies, and we encourage other companies in the industry to take similar steps.[80] The Blue Coat Systems matrix indicates that the CacheFlow, PacketShaper, and ProxySG devices are classified under ECCN 5A002, which covers "information security" systems, while the operating system software for these devices is classified under ECCN 5D002, which covers software related to 5A002 items.[81] Blue Coat Reporter software is classified under ECCN 5D992, which covers software related to "information security" equipment other than 5A002 items.

We provide a further explanation regarding treatment of technology exports such as Blue Coat devices under the EAR in Appendix A, where we present an overview of EAR provisions most relevant to the export of rights-impacting technologies. As detailed as that explanation is, however, significant limitations exist to relying on the EAR for the control of dual-use technology sales to prevent human rights compromises – a purpose the EAR does not adequately accommodate in its current iteration.

The EAR control policy articulated in 15 CFR Part 742 includes only two sections specifically linking export controls to human rights: in support of US policy to "promote the observance of human rights throughout the world," § 742.7 requires licensing for crime control and detection equipment, related technology and software, and § 742.11 requires licensing for specially designed implements of torture.

78 See 15 CFR § 748.1(c) ("Consistent with section 12(c) of the Export Administration Act, as amended, information obtained for the purpose of considering license applications, and other information obtained by the US Department of Commerce concerning license applications, will not be made available to the public without the approval of the Secretary of Commerce or of the Under Secretary for Industry and Security.")

79 "Product Matrix," Blue Coat, May 2013, http://www.bluecoat.com/documents/download/623ffdcd-15da-44ae-ba7c-cd9fd6f6c67b/c40ac45a-4bc1-4cd0-8411-f76f578941f3.

80 Other companies such as Microsoft and Apple have likewise made export control information regarding their products publicly available. See "Exporting Microsoft Products," Microsoft, http://www.microsoft.com/en-us/exporting/eccn.aspx; and "Global Trade Compliance," Apple, https://www.apple.com/legal/more-resources/gtc.html.

81 Reports filed with the US Securities and Exchange Commission pre-2012, when Blue Coat Systems was still publicly traded, confirm that Blue Coat "products are subject to US export controls and may be exported outside the US only with the required level of export license or under an export license exception, *because we incorporate encryption technology into our products*" (emphasis added). See 10-Q March 2009, http://www.sec.gov/Archives/edgar/data/1095600/000119312509050706/d10q.htm. See also 10-Q December 2011, http://www.sec.gov/Archives/edgar/data/1095600/000119312511328772/d246506d10q.htm. ("Our products contain encryption technology and various countries regulate the import or export of certain encryption technology and have enacted laws that could limit our ability to distribute our products or could limit our customers' ability to implement our products in those countries."). Additionally, with respect to the Blue Coat devices discovered in Syria in 2011, the BIS settlement agreement with Computerlinks FZCO indicates that those "items included equipment and software designed for use in monitoring and controlling Web traffic that are classified under [ECCNS] 5A002 and 5D002, respectively, controlled for National Security and Anti-Terrorism reasons and as Encryption items."

These items are controlled within the CCL for crime control (CC) reasons.[82] The CC category is one of the "foreign policy controls" established under the Export Administration Act of 1979,[83] which authorizes control of exports, *inter alia*, "to the extent necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations,"[84] and, as such, is the type of control most amenable to incorporation of human rights concerns. Both § 742.7 and § 742.11 note that in maintaining controls over the designated items, the US "considers international norms regarding human rights and the practices of other countries that control exports to promote the observance of human rights." However, the items currently covered by these CC controls are limited in scope, consisting primarily of equipment that can be used to directly inflict physical harm upon an individual (e.g., law enforcement striking weapons) and related items. They do not include any "telecommunications" (Category 5, Part 1) or "information security" (Category 5, Part 2) items, which are the categories of particular relevance to dual-use technologies (*See Appendix A below for a full explanation*).

Export of Blue Coat products illustrates the limitations of the EAR in controlling dual-use technologies for human rights reasons. As indicated in the Blue Coat export control product matrix, while the devices at issue are classified with "information security" ECCNs that are subject to control for national security (NS), anti-terrorism (AT), and encryption item (EI) reasons, they may still be exported pursuant to license exception "ENC." License exception ENC (15 CFR § 740.1) authorizes the export and re-export of certain encryption commodities, software, and technology pursuant to streamlined procedures that minimize the BIS review and approval requirements, without the need to obtain a license.

The Blue Coat export control product matrix states that the license exception ENC provision applicable to its products is 15 CFR § 740.17(b)(1). Under § 740.17(b)(1), companies may opt to complete encryption registration with the BIS and "self-classify" encryption items that are not otherwise enumerated in § 740.17(b)(2) and (3), which results in immediate authorization of a product for export and simply requires submission of an end-of-year self-classification report to the BIS. As Blue Coat is utilizing license exception ENC (unrestricted) pursuant to § 740.17(b)(1) to export its products, BIS oversight of and input on such exports is limited; the BIS is performing more of an information gathering function regarding, rather than actively controlling, such products. (It is noteworthy, however, that Blue Coat describes its products as covered by § 740.17(b)(1) instead of § 740.17(b)(3) in its export control matrix. § 740.17(b)(3) includes encryption commodities "that provide or perform vulnerability analysis, network forensics, or computer forensics functions characterized by . . . automated network analysis, visualization, or packet inspection for profiling network flow, network user or client behavior, or network structure/topology and adapting in real-time to the operating environment." That description would appear to match the functions of Blue Coat PacketShaper and ProxySG devices). While license exception ENC is still available for such products, a different classification process applies – self-classification is not permitted. (*See Appendix A for a full explanation*).

82 The EAR controls items for export according to the following possible categories of reasons, which are primarily security-related: anti-terrorism (AT), chemical and biological weapons (CB), crime control (CC), chemical weapons convention (CW), encryption items (EI), firearms convention (FC), missile technology (MT), national security (NS), nuclear nonproliferation (NP), regional stability (RS), short supply (SS), United Nations Embargo (UN), significant items (SI), or surreptitious listening (SL). See 15 CFR § 738.2.

83 See Export Administration Act of 1979, as amended, Pub. L. 96-72, 93 Stat. 503, 50 USC. app. 2401 - 2420, at § 6(n), available at http://www.bis.doc.gov/policiesandregulations/ear/legal_authority.pdf.

84 Ibid. at § 6(a)(1).

Blue Coat exports to destinations that are not subject to US sanctions thus appear unlikely to trigger limitations or review under the EAR that would ultimately prevent export, despite the fact that the use of that technology by authorities in many such countries presents substantial human rights concerns.

In light of the limitations of current export regulations in generating changes to industry behavior surrounding rights-impacting technologies, if export regulations are to be relied upon in the future to curb harmful exports, some reforms will be necessary. Within the US, discussions are taking place over how to adapt the export licensing regime to properly control digital equipment for human rights purposes. For example, the draft Global Online Freedom Act (GOFA) introduced in Congress includes a provision that would amend the Export Administration Act to add a foreign policy control over "Certain Telecommunications Equipment."[85] That provision would require the creation of "a list of goods and technology that would serve the primary purpose of assisting, or be specifically configured to assist, a foreign government in acquiring the capability to carry out censorship, surveillance, or any other similar or related activity through means of telecommunications, including the Internet."[86] Export of items on that list would then be prohibited to "government end-users" in "Internet-restricting countries."[87] While developing the proposed list of goods and technology and designating Internet-restricting countries would present challenges, such an approach would have the benefit of addressing the human rights implications of these technologies directly, perhaps resulting in more clear-cut limitations on the dual-use technology trade. Reform within the US would also likely require revisions to certain existing language within the EAR, including license exception ENC (*See Appendix A*).

Efforts to better regulate the dual-use technology trade have also developed internationally. In its December 2012 "Digital Freedom Strategy," the European Parliament 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.[88] It also called for "the inclusion of targeted repression technologies in the Wassenaar Arrangement,"[89] which would extend the effort beyond the EU to the US, Canada, the Russian Federation, and other countries that are members of the multilateral regime. Similarly, the UK government indicated in December 2012 that, with respect to telecommunications equipment that can be used to restrict freedom of expression online, "[w]here this type of equipment is not currently subject to control the Government is committed to working with international partners through the mechanism of the Wassenaar Arrangement in order to agree a specific control list of goods, software and technology. . . . Given the evolving nature of these technologies and the very technical nature of these discussions we expect that this work will continue next year."[90] Addressing the issue multilaterally

85 H.R. 491: Global Online Freedom Act of 2013, 113th Congress, February 4, 2013, http://www.govtrack.us/congress/bills/113/hr491/text, at § 301(a).

86 Ibid.

87 Ibid. Note that the definition of "government end-user" proposed in GOFA is different than the existing EAR definition (see Appendix A below); in particular, the GOFA definition includes "a telecommunications or Internet service provider that is wholly or partially owned by a government of that country."

88 See Paragraph 23 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.

89 See Ibid., at Paragraph 43.

90 http://www.official-documents.gov.uk/document/cm85/8506/8506.pdf, at Paragraph 32.

within the Wassenaar Arrangement could result in more widespread and effective control, and promote international dialogue around the important questions of what technologies and end-uses to control. However, as a state-based institution, whose decisions depend on member state consensus, significant challenges exist to promoting controls for human rights purposes (a topic hotly contested among states) in that forum – particularly if the goal is to develop regulation in a transparent manner that addresses civil society concerns.

SYSTEMIC CHALLENGES TO HUMAN RIGHTS AND THE NEED FOR STRONGER CORPORATE SOCIAL RESPONSIBILITY EFFORTS.

As our latest findings demonstrate, existing measures to limit the provision of dual-use technologies to those who will misuse them are inadequate. This inadequacy is due not only to lack of robust, human rights-based regulation, but also to the dual-use technology industry's lack of transparency and lack of effective compliance with those controls that are in place. In the case of Blue Coat Systems, reliance on unethical distribution partners appears to be one significant element in the overall compliance breakdown. Companies must enhance their corporate social responsibility efforts, including human rights due diligence, in order to rectify these systemic issues and prevent human rights compromise.

The reappearance of Blue Coat devices in sanctioned countries documented in this report, as well as the BIS investigation into Computerlinks FZCO described above, raise important questions surrounding Blue Coat Systems' knowledge of the presence of its devices in those countries, possible diversion of Blue Coat products, and accountability mechanisms applicable to Blue Coat Systems and its distribution partners.

Blue Coat Systems has a global trade compliance program in place, and has developed certain measures to prevent black-letter violations of sanctions and export control regulations, including measures developed specifically for partners. According to the company, "All of our sales are generated through third parties we call channel partners, and we contractually require these partners to comply with applicable laws in connection with their sale of our products to authorized destinations, end-users and end-uses. We also require our channel partners to adhere to high standards of ethical conduct in connection with the sale of our products."[91] These standards include that "[p]artners must be familiar with and comply with all relevant laws and restrictions, including US export laws, when dealing with Blue Coat products. It is critical to such compliance that Partners correctly specify the end-user and destination of any Blue Coat products ordered and that Partners identify any suspicious circumstances with respect to the end-user or transaction."[92]

Such compliance requirements are essential as, pursuant to US export regulations, Blue Coat Systems is prohibited from "[p]roceeding with transactions with knowledge that a violation has occurred or

91 "Enabling a Safe and Productive Internet," Blue Coat.

92 "Ethics Policy for Partners," Blue Coat, http://www.bluecoat.com/company/ethics-policy-partners.

is about to occur."[93] Thus, if Blue Coat Systems has reason to know that its products for export may be diverted or that a distributor may have misrepresented details of the transaction, it is prohibited from proceeding with that transaction. The BIS has developed "know your customer" guidance and red flags to assist company compliance with this knowledge standard, at Supplement No. 3 to 15 CFR Part 732.94. If red flags are present concerning a transaction, companies "have a duty to check out the suspicious circumstances and inquire about the end-use, end-user, or ultimate country of destination," beyond that information initially supplied by a distributor, customer, or others.[95]

It appears, however, that these measures were insufficient to prevent the deployment of Blue Coat devices in the sanctioned countries of Iran, Sudan, and Syria. That deployment could be the result of unlawful diversion, as Blue Coat asserted was the case with respect to the 2011 findings of its devices in Syria; according to the BIS settlement agreement stemming from that investigation, distribution partner Computerlinks FZCO misrepresented destination and end-user details in placing orders for those devices with Blue Coat, willfully violating its distribution agreement with the company. It could also be the result of gray market sales – though Blue Coat Systems maintains that it "only provides support for equipment purchased through an official Blue Coat channel. Blue Coat will not provide support nor make any support contracts available for any equipment purchased through a distribution channel not authorized by Blue Coat."[96] Yet even if unlawful diversion or gray market sales do account for Blue Coat deployment in sanctioned countries, if Blue Coat knew or had reason to know that a distribution partner was engaging in questionable practices, or that its devices were bound for or ultimately utilized in an unauthorized destination or by an unauthorized end-user, Blue Coat would remain responsible for that deployment under US sanctions and export control regulations.

The knowledge standards incorporated in US sanctions language and export regulations also raise certain factual questions about the operation of Blue Coat devices, and the information available to Blue Coat Systems concerning end-use. As noted when logs of Blue Coat devices in Syria were made public in 2011, the appliances in question appeared to "phone home," creating indicators of their location due to requests made back to the company for software updates, registration, and the retrieval of filtering rules.[97] Blue Coat Systems, however, announced in a statement:

> We do not know who is using the appliances or exactly how they are being used. ... These ProxySG appliances are not able to use Blue Coat's cloud-based WebPulse service for real-time URL and malicious threat intelligence or run the Blue Coat WebFilter database. We are not providing support, updates or other services to these appliances. In essence, these ProxySG appliances are operating independently. There is no so-called "kill switch" for Blue

93 General Prohibition Ten provides that a company "may not sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR and exported or to be exported with knowledge that a violation of the Export Administration Regulations, the Export Administration Act or any order, license, License Exception, or other authorization issued thereunder has occurred, is about to occur, or is intended to occur in connection with the item." See 15 CFR § 736.2(b)(10).

94 See Supplement No. 3 to 15 CFR Part 732.

95 Ibid., Paragraph (a)(2).

96 "Gray Market Equipment," Blue Coat, http://www.bluecoat.com/support/support-policies/gray-market-equipment.

97 See Collin David Anderson, "BlueCoat and Syria: Indicators and Culpability," October 11, 2011, http://b.averysmallbird.com/entries/bluecoat-and-syria-indicators-and-culpability.

> Coat ProxySG appliances and Blue Coat cannot connect and remotely shut down or access information of ProxySG appliances that have been deployed.[98]

An experiment conducted by Citizen Lab researchers over a period of three weeks in July 2012 revealed evidence suggesting that devices in Syria were not phoning home to the company's servers in California and that Blue Coat may have blocked traffic on Syrian ISPs from accessing its websites.[99] Further discussion is therefore necessary regarding the means available to Blue Coat Systems to detect and prevent deployment of its products in violation of US sanctions and export regulations, as well as for end-uses that may otherwise compromise human rights.

Finally, regardless of the requirements or limitations in existing export regulations, companies remain obliged at all times to respect human rights. The UN Guiding Principles on Business and Human Rights 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."[100] 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"[101] – which requires proactive efforts to ensure human rights compliance among business partners such as distributors. The UN Guiding Principles further detail how companies should carry out such obligations.

Accordingly, the findings of this report highlight the need for Blue Coat Systems, as well as other companies in this industry, to critically examine why existing control measures are insufficient to prevent the use of its products in sanctioned countries, and what options exist for more effective human rights- and export-related due diligence. An understanding of why safeguards related to information gathering and distribution practices broke down—even after incidents of diversion had already come to light, in the case of Syria—will inform best practices for the future, and should be the basis for constructive dialogue among industry, civil society, and governments. Blue Coat has already announced its intention to "engage key stakeholders, including our channel partners, to review what further steps we can take to limit misuse of our products."[102] It has also reportedly started revamping its channel partner program in significant ways, including reducing the total number of partners and conducting more frequent audits of partners.[103] Now is therefore an opportune time to engage on lessons learned and effective approaches for the future.

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

99 "Update: Are Blue Coat Devices in Syria 'Phoning Home'?," Citizen Lab, January 14, 2013, https://citizenlab.org/2011/11/behind-blue-coat/#update.

100 Principle 11, "UN Guiding Principles on Business and Human Rights," Business and Human Rights Resource Centre, http://www.business-humanrights.org/Documents/UNGuidingPrinciples.

101 Ibid., Principle 13 (b).

102 "Enabling a Safe and Productive Internet," Blue Coat.

103 Christopher Tozzi, "BlueCoat Revamps Channel Partner Program," The Var Guy, September 17, 2012, http://thevarguy.com/var-guy/bluecoat-revamps-channel-partner-program.

CONCLUSIONS AND RECOMMENDATIONS

Our report uncovered Blue Coat devices on public networks in 83 countries, including countries subject to US sanctions, such as Iran, Sudan, and Syria. This work, building on our January 2013 *Planet Blue Coat* report, also follows other recent findings concerning the use of Blue Coat in sanctioned countries. For example, Reflets.info recently announced they had identified 171 Blue Coat devices in Iran,[104] however we suspect that this may be a misinterpretation of the relevant data.[105] Similarly, on May 23, 2013, the hacktivist group Telecomix announced new findings concerning the presence of Blue Coat devices in Syria.[106] These findings paint a picture of the global spread Blue Coat in places with questionable human rights records and key concerns over the rule of law. More generally, we think this indicates continuing failures in the market for dual-use devices, and highlights the substantial need for greater scrutiny. We hope that other researchers will take encouragement from this work, and borrow liberally from our methods.

It is encouraging that companies like Blue Coat Systems have voiced their support for international human rights principles.[107] The critical next step is implementing those principles in business practice. This is a difficult step for many companies, as they must acknowledge the potential of the dual-use technologies they produce to negatively impact human rights, and their own corporate responsibilities. Companies have many potential allies as they consider embarking on this process: a very wide range of civil society, government actors, and other industry participants are committed to addressing the dual-use technology trade and working towards real solutions. Where pressure is strongest, naturally, some progress has been made. Indeed, Blue Coat Systems has already demonstrated its capacity to turn principles into practice by its decision to remove the LGBT category from Blue Coat WebFilter[108] after civil society organizations raised concern over the discriminatory nature of such a category and its use by the Department of Defense, educational institutions, and others.[109]

Citizen Lab calls on Blue Coat Systems, as well as its investor Ontario Teachers' Pension Plan, to open dialogue with our organization regarding (in Blue Coat's words) "further steps we can take to limit

104 "#BlueCoat: tu vas avoir du mal avec ton #spanous©: 171 appliances en Iran, 34 en Syrie,» Reflets.info, May 24, 2013, http://reflets.info/bluecoat-tu-vas-avoir-du-mal-avec-ton-spanous-171-appliances-en-iran-34-en-syrie.

105 The 171 devices found in Shodan and counted as "Blue Coat" by Reflets.info do not, in fact, appear to be Blue Coat devices, but Squid proxies that were attempting to communicate with upstream Blue Coat devices. The number thus reflects unrelated proxies, not Blue Coat devices.

106 "#BlueCoat spotted in #Syria once again," Reflets.info, May 23, 2013, http://reflets.info/bluecoat-spotted-in-syria-once-again.

107 "Enabling a Safe and Productive Internet," Blue Coat.

108 "Removing LGBT Category in Blue Coat WebFilter," Blue Coat.

109 John Aravosis, "Tell Blue Coat to Stop Helping its Customers Ban Gay and Trans Web Sites," America Blog, January 9, 2013, http://americablog.com/2013/01/tell-blue-coat-stop-banning-gay.html.

misuse of [Blue Coat] products."[110] Citizen Lab can also assist Blue Coat Systems in coordinating the participation of other stakeholders such as the Global Network Initiative, NGOs and individual activists, and research and government entities that have expressed interest in developing intelligent control of the dual-use technology trade. Such a process, conducted in a transparent and results-oriented manner, can help advance the protection of human rights in this industry as a whole. Proactive, industry-led corporate social responsibility measures, informed by civil society input, are essential to internalizing human rights considerations in business practice, above and beyond basic regulatory compliance. This is not only a step towards ensuring companies fulfill their moral and human rights obligations, but may also help companies prevent serious public relations problems or other liabilities stemming from knowledge gaps and/or partner malfeasance in global operations.

As an initial basis for discussion, Citizen Lab reiterates the questions presented to Blue Coat Systems and issues for further inquiry raised in our January 2013 *Planet Blue Coat* report (*See Appendix B*).

Citizen Lab also recommends the following action in light of the issues raised by the findings of this report:

- **Greater transparency by dual-use technology companies over export practices**, including the release of export control product matrices identifying the ECCNs applicable to each of their products (which Blue Coat Systems made available in May 2013), as well as the release of reporting related to their use of license exception ENC or other license exceptions.
- **Increased focus on mechanisms for ensuring the accountability and compliance with export regulations as well as human rights principles of distribution partners or other third parties involved in the sale and export of dual-use technologies.** Industry participants such as Blue Coat Systems have longstanding experience and unique knowledge concerning the practices and circumstances of distribution partners and others entities involved in this market. It is important for Blue Coat Systems to share that understanding in constructive discussion with other stakeholders on how to address the challenges of global distribution systems. For example, how might companies better incorporate audits and human rights "background checks" when assessing potential or current partners? In industry experience, what "red flags" above and beyond those enumerated by the BIS tend to signal partner malfeasance?
- **Consideration of new safeguards that might prevent or correct inappropriate end-uses or diversion of a company's product.** For example, what logs are available to Blue Coat Systems and other companies reflecting contact with company servers from devices in the field? Is it possible to audit these logs to verify that the final destination and end-use of its products conform with export regulations and human rights principles? What other sources of information are available or could be sought by Blue Coat and similar companies that might assist its human rights due diligence?
- **Greater industry involvement in discussion of human rights-oriented export control reform efforts, both nationally and internationally.** Bringing together perspectives from industry, civil society, and government will be crucial to determining effective options for intelligent control of dual-use technologies.

110 "Enabling a Safe and Productive Internet," Blue Coat.

APPENDIX A

HOW MIGHT EXISTING US EXPORT REGULATIONS LIMIT SALES OF RIGHTS-IMPACTING TECHNOLOGIES?

Much debate has centered around whether existing export regulations adequately control the sale and dissemination of rights-impacting technologies, or whether reform at the domestic and international levels is necessary to curb the spread of such technologies to authoritarian regimes and other actors that might use them to violate human rights. This debate is complicated by the fact that export regulations are a particularly complex area of law, and understanding their application or potential application is entirely dependent on the circumstances of the export at issue – including its destination, technical specifications, and exchanges concerning licensing between the exporter and the government agency responsible for export control. In an effort to further examine the role of existing export regulations in controlling rights-impacting technologies, we address here the provisions of the US Export Administration Regulations (EAR), administered by the Bureau of Industry and Security (BIS) at the US Department of Commerce, that are most relevant to the technologies at issue. This assessment is not intended to draw definitive conclusions, as we are limited in our analysis to publicly available information concerning the export of these technologies.

At the outset, an item for export is subject to the EAR if it is of US origin,[111] and does not meet the criteria for exclusion from the EAR under 15 CFR § 734.3(b).[112] Technologies subject to the EAR are assigned an export control classification number (ECCN) as laid out in the Commerce Control List (CCL), with items not otherwise listed within the CCL designated as "EAR99."[113] The CCL is broken down into the following categories: nuclear materials, facilities and equipment [and miscellaneous items] (category 0); materials, chemicals, microorganisms and toxins (category 1); materials processing (category 2); electronics (category 3); computers (category 4); telecommunications and information security (category 5); sensors and lasers (category 6); navigation and avionics (category 7); marine (category 8); and propulsion systems, space vehicles, and related equipment (category 9).

The CCL category applicable to any given rights-impacting technology will depend heavily on its technical specifications. In general, category 5, telecommunications and information security, appears to be the most pertinent to the technologies in question, though it is possible that certain products may

111 See 15 CFR § 734.3

112 15 CFR § 734.3(b) excludes from the EAR items that are exclusively controlled for export or re-export by other US departments or agencies; certain printed media; and publicly available technology and software (with the exception of certain encryption software).

113 Items that are designated as EAR99 do not normally require a license to export.

also require inclusion in category 4, computers.[114] Part 1 of category 5 covers "telecommunications" items, while part 2 of category 5, "information security,"[115] covers many products that incorporate encryption in some form.

Certain rights-impacting technologies that are designed to compromise mobile devices and electronic communications might fall within ECCNs of CCL category 5, part 1: telecommunications items, some of which are controlled for surreptitious listening (SL) reasons. According to the BIS, "the purpose of the imposition of surreptitious listening controls is to prevent the unlawful interception of oral, wire, or electronic communications by terrorists and others who may put the information gained through intercepted communications to an unlawful use; to promote the protection of privacy of oral, wire, or electronic communications; and to protect against threats of terrorism around the world."[116] In particular, the following ECCNs include SL items, for which a license is required regardless of destination:

- 5A001.i – "Systems or equipment, specially designed or modified to intercept and process the air interface of 'mobile telecommunications', and specially designed components therefor."
- 5A980 – "Devices primarily useful for the surreptitious interception of wire, oral, or electronic communications, other than those controlled under 5A001.i; and parts and accessories therefor."
- 5D001 – "Software"
  Includes software "specially designed or modified for the 'development', 'production' or 'use' of equipment, functions or features, controlled by 5A001" (a).
- 5D980 – Other "software," other than that controlled by 5D001
  Includes software "primarily useful for the surreptitious interception of wire, oral, and electronic communications" (a), and software "primarily useful for the "development", "production", or "use" of equipment controlled by 5A980" (b).
- 5E001 – "Technology"
  Includes technology for the "'development', 'production' or 'use' (excluding operation) of equipment, functions or features, controlled by 5A001 or 'software' controlled by 5D001.a" (a).
- 5E980 – "Technology," other than that controlled by 5E001.a (for 5A001.i, and for 5D001.a (for 5A001.i)), primarily useful for the "development", "production", or "use" of equipment, functions or features, of equipment controlled by 5A980 or "software" controlled by 5D980.

If a product is controlled for SL reasons, the BIS will generally deny the license application.[117] Two important limitations exist, however, with respect to surreptitious listening controls. First, the item must be "primarily useful for" surreptitious listening in order to fall within the scope of the

114 This category covers, *inter alia*, digital computers "having an 'Adjusted Peak Performance' ('APP') exceeding 3.0 weighted Tera-FLOPS" (4A003) and computers for fingerprint equipment (4A980).

115 "Information security" is defined in the EAR as "all the means and functions ensuring the accessibility, confidentiality or integrity of information or communications, excluding the means and functions intended to safeguard against malfunctions. This includes 'cryptography', 'cryptographic activation', 'cryptanalysis', protection against compromising emanations and computer security." "Cryptanalysis" is further defined as "the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text." See 15 CFR § 772.1.

116 "Chapter 13: Surreptitious Listening (§ 742.13)," Bureau of Industry and Security, US Department of Commerce, http://www.bis.doc.gov/news/2007/foreignpolicyreport/fprchap13_surreplisten.htm.

117 15 CFR § 742.13(b)(2).

control, which will depend on the design of the product and the extent to which it is also capable of permissible functions.[118] Second, the presumption of licensing denial is not applicable to exports by providers of wire or electronic communication services, or by individuals working for the US government and engaged in the normal course of government activities, license applications of which will generally be approved.[119]

Additionally, ECCN 5A001.f, while not controlled for SL reasons, includes items that may affect the security of mobile telecommunications, namely:

> Jamming equipment specially designed or modified to intentionally and selectively interfere with, deny, inhibit, degrade or seduce mobile telecommunication services and perform any of the following, and specially designed components therefor:
>
> f.1. Simulate the functions of Radio Access Network (RAN) equipment;
>
> f.2. Detect and exploit specific characteristics of the mobile telecommunications protocol employed (e.g., GSM); or
>
> f.3. Exploit specific characteristics of the mobile telecommunications protocol employed (e.g., GSM).

Items that fall within this ECCN are controlled for national security reasons, such that a license is required for export to a number of countries. However, the BIS general licensing policy for national security-controlled items is to approve license applications, unless exporting to a country that is included within Country Group D:1 of Supplement No. 1 to 15 CFR Part 740, in which case the licensing policy is to approve license applications only for exports to civilian end-users.[120]

More applicable to technologies such as the Blue Coat devices addressed in this report, however, is CCL category 5, part 2: information security. Category 5, part 2 information security ECCNs relevant to rights-impacting technologies include:

- 5A002 – "Information security" systems, equipment and components therefor
  Includes certain items "designed or modified to use 'cryptography' employing digital techniques performing any cryptographic function other than authentication or digital signature" (a.1), and items "designed or modified to perform cryptanalytic functions" (a.2).
- 5A992 – Equipment not controlled by 5A002
  Includes "telecommunications and other information security equipment containing encryption" (a), and "'information security' equipment, n.e.s., (e.g., cryptographic, cryptanalytic, and cryptologic equipment, n.e.s.) and components therefor" (b).

118 15 CFR § 742.13(a)(2) defines "communications intercepting devices" as "electronic, mechanical, or other devices that can be used for interception of wire, oral, or electronic communications if their design renders them primarily useful for surreptitious listening even though they may also have innocent uses."

119 15 CFR § 742.13(b)(1). "License applications, except for those applications for which a license is required for both SL and AT reasons, will generally be approved for exports or reexports requiring a license for SL reasons when the exporter or reexporter is:

(i) A provider of wire or electronic communication services or an officer, agent, or employee of, or person under contract with such a provider, in the normal course of the business of providing that wire or electronic communication service; or

(ii) An officer, agent, or employee of, or a person under contract with, the United States, one of the 50 States, or a political subdivision thereof, when engaged in the normal course of government activities."

120 See 15 CFR § 742.4(b).

- 5D002 – "Software"
  Includes software that is "specially designed or modified for the 'development', 'production' or 'use' of equipment controlled by 5A002" (a), "specially designed or modified to support 'technology' controlled by 5E002" (b), or "having the characteristics, or performing or simulating the functions of the equipment, controlled by 5A002" (c.1).
- 5D992 – "Information Security" "software" not controlled by 5D002
  Includes software "specially designed or modified for the 'development', 'production,' or 'use' of" (a), or "having the characteristics, or performing or simulating the functions of" (b), that equipment controlled by ECCN 5A992.a or 5A992.b.
- 5E002 – "Technology"
  "Technology" is defined in the EAR as "specific information necessary for the 'development', 'production', or 'use' of a product. The information takes the form of 'technical data' or 'technical assistance.'" Technical data includes manuals, instructions, and engineering designs and specifications, while technical assistance includes "instruction, skills training, working knowledge, consulting services."[121] This ECCN includes technology "for the 'development', 'production' or 'use' of equipment controlled by 5A002 or 5B002 or 'software' controlled by 5D002.a or 5D002.c" (a).
- 5E992 – "Information Security" "technology" not controlled by 5E002
  Includes technology, not elsewhere specified, for "the 'development', 'production' or 'use' of equipment controlled by 5A992.a, 'information security' or cryptologic equipment controlled by 5A992.b or 'software' controlled by 5D992.a or b" (a).

Items that fit the criteria of the 5x992 ECCNs are controlled for anti-terrorism reasons, which according to 15 CFR §§ 742.8, 742.9, 742.10, 742.19 and the Commerce Country Chart[122] triggers licensing requirements for exports to Iran, Syria, Sudan, and North Korea. However, the remaining information security items outlined above are controlled for national security and encryption item reasons as well as anti-terrorism, such that licensing requirements are triggered for exports to *all* countries except Canada. Even so, licensing requirements on these items are limited by the existence of broad license exceptions and "mass market treatment" for encryption products.

Despite the above-mentioned controls, for many encryption products, it is not necessary to engage in full-scale licensing with the BIS; rather, simplified procedures are available for products that qualify for

121 See 15 CFR § 772.1.

122 See Supplement No. 1 to 15 CFR Part 738.

"mass market treatment,"[123] for license exception "ENC,"[124] or for other license exceptions. Over the last few years there has been significant movement towards the streamlining of encryption controls, including related review and reporting requirements, with ongoing efforts to reduce restrictions (given the increasingly ubiquitous nature of encryption) and free up related commerce. Thus, for a significant range of encryption products, emphasis by the BIS appears to be on regular information gathering as opposed to outright restriction on exports. Control of rights-impacting technologies on the basis of their encryption functionality thus does not align well with the parameters of and reasoning behind controls on encryption items, which involve distinct considerations.

License exception ENC deserves particular discussion concerning its potential incompatibility with human rights-based export control. At the outset it should be noted that the streamlined treatment detailed in this license exception is not available for exports to countries listed in Country Group E:1 in Supplement No. 1 to Part 740 of the EAR, namely: Cuba, Iran, North Korea, Sudan, and Syria – all of which are currently subject to US sanctions. This exception does, however, permit streamlined exporting in a variety of other circumstances.

First, exports and reexports of certain encryption items are authorized without the need for submission of *any* application, registration or reporting to the BIS if the export is to a US subsidiary; or to a "private sector end-user" located in one of the "favourable treatment" countries laid out in Supplement No. 3 to Part 740 of the EAR—namely, European countries as well as Australia, Canada, Iceland, Japan, New Zealand, and Turkey—for which the end-use is "internal 'development' or 'production' of new products by those end-users."[125]

123 According to 15 CFR § 742.15(b)(1), many encryption commodities, software and components covered by ECCNs 5A992 or 5D992 may qualify for self-classification and immediate mass market authorization (provided a company has obtained an Encryption Registration Number from the BIS and completes necessary self-classification reporting requirements) if they meet all of the following criteria, laid out in Cryptography Note 3 to CCL Category 5, Part 2:

a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:

1. Over-the-counter transactions;
2. Mail order transactions;
3. Electronic transactions; or
4. Telephone call transactions;

b. The cryptographic functionality cannot be easily changed by the user;

c. Designed for installation by the user without further substantial support by the supplier; and

d. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs (a) through (c) of this note.

Qualifying items are treated as "no license required." The following are noted as examples of mass market encryption products: "general purpose operating systems and desktop applications (e.g., e-mail, browsers, games, word processing, database, financial applications or utilities) designed for use with computers classified as ECCN 4A994 or designated as EAR99, laptops, or handheld devices; commodities and software for client Internet appliances and client wireless LAN devices; home use networking commodities and software (e.g., personal firewalls, cable modems for personal computers, and consumer set top boxes); and portable or mobile civil telecommunications commodities and software (e.g., personal data assistants (PDAs), radios, or cellular products)." 15 CFR § 742.15(b)(6).

Note that mass market treatment is not available for exports to countries listed in Country Group E:1 in Supplement No. 1 to Part 740 of the EAR, namely: Cuba, Iran, North Korea, Sudan, and Syria; nor is it available for the encryption items described in §§ 740.17(b)(2) or (b)(3)(iii) of the EAR (see below). See "Supplement No.1 to Part 740—Country Groups," in *Electronic Code of Federal Regulations*, US Government Printing Office, http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=88273360a10069a57de20e9db4d7970a&rgn=div5&view=text&node=15:2.1.3.4.25&idno=15#15:2.1.3.4.25.0.1.21.28.

124 See 15 CFR § 740.17.

125 See 15 CFR § 740.17(a).

Second, in those circumstances that do not meet the criteria of § 740.17(a) of license exception ENC, while companies do have to submit some information to the BIS, the process is simplified, with wide latitude provided for export of encryption items to end-users in the aforementioned "favourable treatment" countries. Under § 740.17(b) of license exception ENC, companies may opt to complete a basic encryption registration with the BIS.[126] Once that registration is complete, the following processes apply:

- Under §740.17(b)(1), companies may "self-classify" encryption items that are not otherwise enumerated in §740.17(b)(2) and (3), which results in immediate authorization of a product for export and simply requires submission of an end-of-year self-classification report to the BIS.
- Encryption items that are enumerated in §740.17(b)(2) or (3) also qualify for streamlined processing rather than requiring a license application – with provisions of §740.17(b)(2) applicable to specified items to particular end-users, and provisions of §740.17(b)(3) applicable to specified items to any end-user. However, rather than self-classifying, companies submit "classification requests" to the BIS for these items, followed with semi-annual reporting to the BIS regarding the exported items. Export of items submitted for classification in this manner is authorized thirty days after submission of the request,[127] provided that the BIS does not request follow-up during that time; companies are thereafter able to continue exporting those products for which classification was completed, to which Commodity Classification Automated Tracking System (CCATS) numbers are assigned. The BIS as well as NSA review these classification requests.

The following provisions of § 740.17(b) are of particular note with respect to control of rights-impacting technologies that incorporate cryptography.

Under § 740.17(b)(2)(i)(F), a company may engage in this simplified classification review and export to any non-"government end-user" (not located in a "favourable treatment" country) of "encryption commodities and software that provide penetration capabilities that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks."

This provision to the license exception was added in June 2010, to clarify that export of such products to *government* end-users outside of favourable treatment countries still requires licensing by the BIS.[128] Given the offensive capabilities and potential human rights implications of such technology, however,

126 See 15 CFR § 742, Supplement No. 5.

127 Export or re-export is authorized *immediately* after submission of the classification request, without the 30-day wait, in the circumstances outlined in the note to the introductory text of paragraph (b)(2)—which include the export of "[a]ll submitted encryption items described in this paragraph (b)(2), except 'cryptanalytic items,' to any end-user located or headquartered in a country listed in Supplement No. 3 [listing favourable treatment countries] to this part"—as well as in the note to the introductory text of paragraph (b)(3), covering export "of the items described in this paragraph (b)(3) to any end-user located or headquartered in a country listed in Supplement No. 3 to this part."

128 See Department of Commerce Bureau of Industry and Security, "Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility, Submission Procedures, Reporting Requirements, License Application Requirements, and Addition of Note 4 to Category 5, Part 2," *Federal Register*, Vol. 75, No. 122, June 25, 2010, http://www.bis.doc.gov/encryption/75fr36481.pdf, at p. 36484 ("These amendments are consistent with determinations that, for national security reasons, encryption commodities and software that provide penetration capabilities that can be used to attack, deny, disrupt or otherwise impair the use of cyber infrastructure or networks require a license in order to be exported to "government end-users" in countries other than countries listed in Supplement No. 3 to Part 740. This change is implemented in new paragraph section 740.17(b)(2)(i)(F).") See also US Department of Commerce Bureau of Industry and Security, "Update 2011 Conference on Export Controls and Policy: Encryption Workshop Update 2011 (Part 1)," July 21, 2011, http://htc-01.media.globix.net/COMP008760MOD1/BIS_Web/Transcripts/072111_Encryption_Workshop_2011_part1.pdf, at pp. 9-10.

it is unclear why the license exception would cover items with such "penetration capabilities" in the first instance, rather than excluding those items entirely from the scope of the exception and requiring a complete license application for case-by-case review of such exports to both non-government and government end-users.[129] The license exception presents particular concern considering the EAR's approach to "government end-user," which is defined as:

> [A]ny foreign central, regional or local government department, agency, or other entity performing governmental functions; including governmental research institutions, governmental corporations or their separate business units (as defined in Part 772 of the EAR) which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and international governmental organizations. *This term does not include: utilities (including telecommunications companies and Internet service providers)*; banks and financial institutions; transportation; broadcast or entertainment; *educational organizations*; civil health and medical organizations; retail or wholesale firms; and manufacturing or industrial entities not engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.[130]

On its face, this provision suggests that a company exporting attack tools and other penetration capabilities to a telecommunication company, Internet service provider, or educational organization may do so under the simplified classification review procedure without submitting a license application to the BIS – despite the fact that such entities are in many instances effectively controlled by the governments of their home countries.

Additionally, according to 15 CFR § 740.17(b)(3)(iii), a company may engage in the simplified classification review process for export to any end-user of:

> Encryption commodities and software not described by paragraph (b)(2) of this section, that provide or perform vulnerability analysis, network forensics, or computer forensics functions characterized by any of the following:
>
> (A) Automated network analysis, visualization, or packet inspection for profiling network flow, network user or client behavior, or network structure/topology and adapting in real-time to the operating environment; or
>
> (B) Investigation of data leakage, network breaches, and other malicious intrusion activities through triage of captured digital forensic data for law enforcement purposes or in a similarly rigorous evidentiary manner.

129 In a November 2012 meeting of the BIS Information Systems Technical Advisory Committee (ISTAC), a discussion was held regarding trade in security exploits, including "zero-day" exploits. The discussion noted the existence of challenges in this area. According to meeting minutes, "Export control seems unlikely to be effective [for regulation of "zero-day" exploits]. At this stage, reporting for the purpose of informing policy-makers about the scope and nature of the market might be sufficient. . . . Because this presentation was informational, no specific follow-up actions were needed. However, this presentation may help inform the ISTAC's discussions of possible future Wassenaar proposals seeking to implement new controls on 'cybertools' as well as any regulatory proposals to amend Section 740.17(b)(2)(i)(F) of the EAR." Bureau of Industry and Security Information Systems Technical Advisory Committee, Minutes of Meeting, November 7-8, 2012, http://tac.bis.doc.gov/2012/110712istacmin.htm.

130 See 115 CFR § 772.1 (emphasis added).

This category of items potentially covers a wide array of dual-use technologies, including those with deep packet inspection functions, bringing them within the scope of the license exception.

With respect to products covered by license exception ENC, BIS input is relatively limited, consisting primarily of reviewing the requisite end-of-year self-classification report (for §740.17(b)(1) items) or initial classification request and semiannual report (for §740.17(b)(2) and (3) items). Moreover, the semiannual reporting requirement is itself limited: for companies that provide their products through distribution partners (as many in the industry do, including Blue Coat Systems), 15 CFR § 740.17(e)(1)(i) requires only that the company indicate "the name and address of the distributor or reseller, the item and the quantity exported or reexported and, *if collected by the exporter as part of the distribution process*, the end-user's name and address" (emphasis added). Thus, unless end-user information is already collected in the normal course of business (e.g., warranty registration cards, etc.), companies have no obligation to report recipients beyond the first level of the distribution chain.

In sum, while this external assessment is by no means conclusive or exhaustive, it appears that the EAR in its current iteration would not substantially limit export of significant rights-impacting technologies to non-sanctioned countries.

APPENDIX B

QUESTIONS POSED TO BLUE COAT SYSTEMS INC. IN OUR JANUARY 2013 *PLANET BLUE COAT* REPORT

- 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?

- 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?

https://citizenlab.org