access

COMMONWEALTH OF SURVEILLANCE STATES: ON THE EXPORT AND RESALE OF RUSSIAN SURVEILLANCE TECHNOLOGY TO POST-SOVIET CENTRAL ASIA

BY PETER BOURGELAIS

EXECUTIVE SUMMARY

The four post-Soviet Central Asian republics discussed here—Kazakhstan, Tajikistan, Turkmenistan, and Uzbekistan—have problematic records with respect to electronic surveillance with little regard to international norms of due process, privacy, and transparency. While there have been some noteworthy victories with respect to regulating Western companies' exports of surveillance technology to other difficult regions such as the Middle East, a different approach is needed in a region with a large Russian presence such as Central Asia. We begin with an explanation of the Russian System for Operative-Investigative Activities (SORM), a technical framework for electronic surveillance originally developed by the old Soviet KGB in the late 1980s and later copied throughout Central Asia. Then we add the main contribution of this work: a series of profiles, organized by country, of important Russian (and two Western) companies that have exported electronic surveillance equipment to the region, along with some previously undisclosed regional concerns about the security of the SORM system itself. Finally, we conclude with a discussion of possible responses from the global digital rights movement, leaving a more detailed and comprehensive action plan for future work.

METHODOLOGY

All of the information contained here is drawn from three sources: prior published investigative work on the subject, original research involving open sources (e.g. company websites and wikis of relevant marketing literature), and a small handful of confidential sources with experience in the region.

INTRODUCTION

Four of the five post-Soviet Central Asian states—Kazakhstan, Tajikistan, Turkmenistan, and Uzbekistan—have a combined population of 55 million people, all of whom live under regimes that are consistently ranked as some of the most oppressive in the world.[1] Their record regarding the use of wiretapping and internet surveillance is no exception to their pattern of disregard for due process and the human rights to privacy and free expression. However, whereas export controls and political campaigning have been at least somewhat successful against Western companies that sell surveillance technology either directly to similar regimes or through secondary markets, several relevant technology companies in the region are Russian, and are not as easily lobbied or pressured as most Western companies. In this document, we construct profiles of eight companies that have sold electronic surveillance or mobile forensics equipment in Central Asia with their connections to security services and/or telecoms in the region, and in some cases their histories with the Russian security apparatus. While there are few good options in this generally underreported region, some possibilities exist: "naming and shaming" Western investors that conduct business with these companies; international campaigning involving the UNHCR and the OSCE; direct action focusing on security training; an appeal for balanced lawful intercept policy in Tajikistan; and the pursuit of possible legal action against some companies.

Whereas export controls and political campaigning have been at least somewhat successful against Western companies that sell surveillance technology either directly to similar regimes or through secondary markets, several relevant technology companies in the region are Russian, and are not as easily lobbied or pressured as most Western companies.

1 For example, the 2011/2012 Press Freedom Index published by Reporters Without Borders ranks Tajikistan at 122nd, a 3-way tie with Algeria and Malaysia. Kazakhstan is tied at 154th with post-Gaddafi Libya, Uzbekistan is ranked 157th, and Turkmenistan is ranked at 177. This places the country below China, Iran, and Syria, and above only North Korea and Eritrea (source: Various authors (2011). *PRESS FREEDOM INDEX 2011/2012*. [ONLINE] Available at: http://en.rsf.org/press-freedom-index-2011-2012,1043.html. [Last Accessed 1 December 2012].)

BACKGROUND

To begin, a small amount of background on the global struggle against electronic surveillance in authoritarian regimes elsewhere can illustrate what has been successful in similar contexts. For example, Area SpA, an Italian company specializing in electronic intercept technology, was found to be building a surveillance system that "would have given Syrian President Bashar al-Assad's regime the power to intercept, scan and catalog virtually every email that flows through the country".[2]

After this project was reported independently by Bloomberg and Privacy International coupled with pressure from civil society, Area SpA eventually abandoned the project. More recently, in late April of 2012, President Obama signed an executive order that places sanctions on entities that export IT equipment that aids "computer or network disruption, monitoring or tracking that could assist in or enable serious human rights abuses" by the governments of Syria and Iran. Some non-Western countries have also scaled back their operations in the region to varying degrees. For example, the Chinese firm Huawei began to expand its already significant role in the Iranian telecom sector just as Western companies such as Nokia Siemens Networks and Ericsson withdrew after the 2009 election protests. The company partnered with UK-based Creativity Software to provide the 51% state-owned telecom MTN Irancell with a service that enables "mobile-phone operators to 'comply with lawful-intercept government legislation,' which gives police access to communications and location information."[3] Two years later, amid growing concerns in the U.S. and Europe over Huawei's ties with Iran, the company announced that it would "voluntarily restrict its business development there by no longer seeking new customers and limiting its business activities with existing customers".[4] However, it is important to note that the company did not completely cease its operations in Iran, stating that "For communications networks that have been delivered or are under delivery to customers, Huawei will continue to provide necessary services to ensure communications for Iran's citizens."[5]

- Area SpA, an Italian company specializing in electronic intercept technology, was found to be building a surveillance system that "would have given Syrian President Bashar al-Assad's regime the power to intercept, scan and catalog virtually every email that flows through the country".
- In late April of 2012, President Obama signed an executive order that places sanctions on entities that export IT equipment that aids "computer or network disruption, monitoring or tracking that could assist in or enable serious human rights abuses" by the governments of Syria and Iran.
- Nokia Siemens Networks and Ericsson withdrew after the 2009 election protests in Syria and Iran.
- Amid growing concerns in the U.S. and Europe over Huawei's ties with Iran, the company announced that it would "voluntarily restrict its business development there by no longer seeking new customers and limiting its business activities with existing customers"

2 Vernon Silver (2011). *Italian Firm Said to Exit Syrian Monitoring Project*. [ONLINE] Available at: http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html . [Last Accessed 15 July 2012].

3 STEVE STECKLOW, FARNAZ FASSIHI and LORETTA CHAO (2011). *Chinese Tech Giant Aids Iran*. [ONLINE] Available at: http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html. [Last Accessed 1 July 2012].

4 LORETTA CHAO, STEVE STECKLOW, and FARNAZ FASSIHI (2011). *Huawei to Scale Back Business in Iran*. [ONLINE] Available at: http://online.wsj.com/article/SB10001424052970204319004577088001900708704.html. [Last Accessed 1 July 2012].

5 Ibid.

All of this is of very little help to civil society groups in much of Central Asia, where monitoring of internet traffic and phone conversations is conducted with Russian technology. Furthermore, Russia has a far more developed IT sector than much of the Middle East and North Africa, and Russian companies export this technology to post-Soviet Central Asia, where it is used by the local security services for similar purposes.[6] In addition, Russian technology companies are far more indifferent to negative press coverage. One illustrative case is that of Speech Technology Center (STC), a St. Petersburg-based company specializing in audio forensics and facial recognition that was profiled in the Spy Files database of surveillance companies compiled jointly by Wikileaks, Privacy International, and Bugged Planet.[7] [8] When Sergei Koval, a leading analyst at STC, was asked about the Spy Files publication, he was completely dismissive to the potentially repressive uses of the technology. "All this talk about technology catching dissidents is just bull****! [sic] It's typical of the kind of psychological warfare the Americans use against their opponents. I think all of these arguments about human rights are completely hypocritical. The Americans just use them for their own purposes."[9]

The act of intercepting phone conversations, is conducted by the local security services, who often have an office in the main building of the local telcos (as was shown repeatedly in the below referenced documentary on Teliasonera). This surveillance is conducted via the System for Operative-Investigative Activities (SORM), a primarily Russian system that has been copied throughout Central Asia.

Despite some pushback from STC Moscow, it is exactly this kind of technology that is being used by Russian security services against political opponents.[10] There are also many well-established ties between the Russian tech sector and the Federal Security Service (FSB), the successor to the old Soviet KGB. With the collapse of the Soviet Union, many researchers working on surveillance technology within the intelligence community left for the private sector, as "the KGB's R&D budget was cut to a tenth of its original size and Koval's department was liquidated...And while they can no longer distribute work among 40 different state agencies, as once was the case, the Centre has many opportunities to outsource particularly difficult work. 'We have friends in all the special agencies who are only too keen to help', Koval says."[11] For these reasons, Russian technology companies have no qualms about cooperating with the local security services, and the economic incentives that motivate that seeming indifference extend to Central Asia as well.

The act of intercepting phone conversations, is conducted by the local security services, who often have an office in the main building of the local telcos (as was shown repeatedly in the below referenced documentary on Teliasonera). This surveillance is conducted via the System for Operative-Investigative Activities (SORM), a primarily Russian system that has been copied throughout Central Asia. Originally designed as a KGB research project in the mid-1980s to intercept landline communications, newer versions of the system are now capable of targeted surveillance of specific individuals across the whole range of internet and telephone communications. There are three versions of the system operating in Russia:

6 Andrei Soldatov and Irina Borogan (2012). *Just business: how Russian technology provides the eyes and ears for the world's Big Brothers*. [ONLINE] Available at: http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/just-business-how-russian-technology-provides-eyes-and-ears-. [Last Accessed 1 June 2012].

7 The original database is maintained by Privacy International, Bugged Planet, and the Bureau of Investigative Journalism.

8 More specifically, the company has developed technology that can "store many millions of items of biometric data (voice samples and photo images) and match to individuals by searching all of the world's communication channels (including in video files). The voice recognition technology that they have developed can identify the speaker, regardless of the language, accent or dialect that is used (they identify voices by the physical parameters of the sound produced alone). They also have the means to use fingerprint and IRIS recognition technology as additional applications." (source: see footnote 6)

9 See footnote #6

10 When openDemocracy Russia contacted Dmitry Dyrmovsky, the head of the STC Moscow, "he asked us not to publish anything that Koval had told us. 'Sergei Lvovich Koval has no right to represent the company and he had no right to talk to you, even though I have no idea what he might or might not have told you', said Dyrmovsky. He refused point blank to show us any of STC's products, even those commercial products that are openly advertised on the company's website." from the source in footnote #6

11 See footnote #6

> "SORM-1 intercepts telephone traffic, including mobile networks, while SORM-2 is responsible for intercepting Internet traffic, including GPRS. The interception producers' advertisements suggest that SORM-3 will serve to gather information from all communication media, will offer long-term storage (three years), and provide access to all data on subscribers. In addition, the SORM system enables the use of mobile control points, for example a notebook with a special mobile block that can be plugged directly into communication hubs and immediately intercept and record the operator's traffic. A single notebook of this kind has the capacity to simultaneously tap the lines of 1,024 subscribers." [12]

SORM-2 was initially introduced to Central Asia as part of a program associated with the Russian Interior Ministry (MVD), and according to confidential sources, the security services in these countries have struggled to find adequate staff to operate the equipment,[13] which raises considerable suspicion as to who does in fact operate it.

In Central Asia, these companies have struggled continually to stay in the good graces of local authoritarian strongmen like Uzbekistan's Islam Karimov and Turkmenistan's Gurbanguly Berdymuhamedov, and therefore have no choice but to cooperate with the national security services.

In addition to these long-standing connections between the FSB and the Russian tech sector, it is useful to name those Western companies who have conducted significant business in the region and have partly helped to enable the surveillance state. The Swedish-Finnish company Teliasonera, through several subsidiaries and joint-stock ventures, was recently shown to have cooperated with the security services in Kazakhstan, Uzbekistan, and Tajikistan in the interception of various journalists' and opposition figures' phone calls.[14] The company has recently partnered with the Danish Institute for Human Rights (DIHR) to review its policies with respect to electronic intercept requests in the region.[15] In addition, it has become one of the leading members of the Telecommunications's Industry Dialogue on Freedom of Expression and Privacy,[16] and a representative of the company even participated in a panel on rights respecting telecoms at the recent Internet Governance Forum in Baku, Azerbaijan.[17] However, this too is of little help to users in a region dominated largely by state-owned and Russian telecommunications companies. In Central Asia, these companies have struggled continually to stay in the good graces of local authoritarian strongmen like Uzbekistan's Islam Karimov and Turkmenistan's Gurbanguly Berdymuhamedov, and therefore have no choice but to cooperate with the national security services.[18]

12 ANDREI SOLDATOV and IRINA BOROGAN (2012). *Project_ID: Who's bugging the Russian opposition?. [ONLINE] Available* at: http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/project-id-who%E2%80%99s-bugging-russian-opposition. Last Accessed 1 July 2012].

13 This is somewhat suggested as well by the OpenNet Initiative's profile of the digital rights situation in Tajikistan. See Various authors (2010). *Country profiles: Tajikistan.* [ONLINE] Available at: http://opennet.net/research/profiles/tajikistan. [Last Accessed 1 June 2012].

14 Uppdrag Granskning (2012). *How Teliasonera Sells to Dictatorships | Uppdrag Granskning : The Black Boxes | Mission Investigation.* [ONLINE] Available at: http://vimeo.com/41248885. [Last Accessed 1 July 2012].

15 Katrina Kaiser (2012). *This Week in Internet Censorship: Expanding Anti-Blasphemy Laws in Saudi Arabia, Deporting Activists from the UAE, Chinese Video Sites to Pre-Censor, and Sweden's TeliaSonera to Submit for Human Rights Review.* [ONLINE] Available at: https://www.eff.org/deeplinks/2012/07/week-internet-censorship-china-saudi-arabia-sweden-UAE. [Last Accessed 1 August 2012].

16 Teliasonera (2012). *Telecommunication's Industry Dialogue selects five host organisations as potential addresses.* [ONLINE] Available at: http://www.teliasonera.com/en/newsroom/news/2012/telecommunications-industry-dialogue-selects-five-host-organisations-as-potential-addresses/.

17 Access (2012). IGF 2012 Workshop Proposal :: (No: 98) A Plan for Rights-Respecting Telecoms . [ONLINE] Available at: http://www.intgovforum.org/cms/mag/116-workshop-proposals/1034-igf-2012-workshop-proposal-no-98-a-plan-for-rights-respecting-telecoms. [Last Accessed 1 August 2012].

18 Joanna Lillis (2012). *Uzbekistan: Tashkent's Sticky Fingers Spoiling Foreign Investors' Appetites.* [ONLINE] Available at: http://www.eurasianet.org/node/65735. [Last Accessed 15 August 2012]. and "UPDATE 1-Russian mobile operator MTS returns to Turkmenistan", and Maria Kiselyova (2012). *UPDATE 1-Russian mobile operator MTS returns to Turkmenistan.* [ONLINE] Available at: http://www.reuters.com/article/2012/07/26/mts-turkmenistan-idUSL6E8IQJSV20120726. [Last Accessed 30 July 2012].

AN OVERVIEW OF RUSSIAN SURVEILLANCE COMPANIES AND THEIR CLIENTS

A significant number of companies that develop and sell implementations of SORM and other surveillance measures are Russian, and so are several important regional telcos. An overview of these companies will give us an idea of what technology these companies produce and what kinds of surveillance we may see in the region in the coming years. A quick reference table in the Appendix at the end of this document briefly profiles each company described here, its relevant products, and in which countries we can show that they have conducted business.

UZBEKISTAN

> The Uzbek state security services are capable of interception of landline telephone communications, internet traffic, semi-structured data such as SMS, MMS, and forum posts, and automated voice and facial recognition. They also possess some mobile forensics capability.

The state security services in Uzbekistan have access to a variety of sources for SORM components, and it appears that there are some companies providing audio and mobile forensics software. The Russian company MFI-Soft, which has offices in Nizhny Novgorod and Moscow, produces a complete implementation of all three versions of SORM, including SORM-2 or "SORMovich". The SORMovich system as described by MFI-Soft on their website is designed to be scalable to a network of any size, and several remote intercept points can be connected to this system, which provides the ability to share information from the same network across multiple security agencies.[19] MFI-Soft has exported this equipment to Central Asia through an intermediary, ALOE Systems,[20] to Uzbekistan's state-owned Uzbektelecom.[21] In addition, ALOE Systems markets SORM-3 to customers outside the region under the name Netbeholder from its offices in Toronto, Canada.

Another Russian company that offers similar electronic intercept equipment is PROTEI, originally a division of the Leningrad Research and Development Institute of Communications (LONIIS) attached to the Russian Ministry of Communications before becoming a separate company in 2002. Despite pushback from PROTEI management similar to the aforementioned statement from the head of STC Moscow,[22] PROTEI sells several SORM components, as well as a Deep Packet Inspection (DPI) platform.[23] PROTEI DPI "is a traffic management platform with deep packet inspection capabilities allowing to [sic] effectively manage utilization of network resources and provide new value generating services. The main functions of PROTEI DPI are: dynamic policy enforcement, traffic charging and value-added traffic manipulation."[24] In non-technical language, the DPI platform is capable of monitoring network traffic and continuously updating the kinds of traffic that it blocks or logs, right down to specific web pages and services (e.g. Skype and IM clients). The company has contracts with Uzbekistan.[25]

19 MFI-Soft (2012). *СОРМ2 | МФИ СОФТ.* [ONLINE] Available at: http://www.mfisoft.ru/products/sorm/sorm2/sormovich. [Last Accessed 15 July 2012]. (in Russian) and the source in footnote #12.

20 See footnote #6

21 ALOE Systems (2012). *Clients | ALOE Systems VoIP Softswitch Solutions.* [ONLINE] Available at: http://www.aloe-systems.com/company/clients#cis. [Last Accessed 10 December 2012].

22 When the CEO of Protei was contacted about his company's inclusion in the Spy Files, he said "'I didn't pay it any attention...We work with mobile networks in many different countries, so that's how they must have got information about us. I didn't really look into it because the whole thing doesn't bother me. In fact we don't sell that kind of technology – surveillance bugs and that kind of thing. We aren't the only ones producing such applications for mobile anyway'." from the source in footnote #6. In any case, Protei did make an appearance at the 2009 ISS World trade show in Dubai, where they described themselves as Lawful Intercept (LI) specialists. According to the event description on their website, they described an LI solution called "Beyond LI" which "allows system operators to trace calls, detect patterns and relationships among suspects, identify potential accomplices and much more, all at the click of a button". See Protei (2012). Telecommunication Solutions - PROTEI. [ONLINE] Available at: http://www.protei.com/events/past/. [Last Accessed 1 November 2012].

23 Protei (2012). *Конвертер СОРМ XSM - Оборудование СОРМ - Обзор - НТЦ ПРОТЕЙ.* [ONLINE] Available at: http://www.protei.ru/products/xsm/. [Last Accessed December 11 2012].

24 Protei (2012). *DPI Platform - Traffic Management - Overview - PROTEI.* [ONLINE] Available at: http://www.protei.com/products/dpi/. [Last Accessed 11 December 2012].

25 See footnote #6

Electronic surveillance and analysis systems are not the only platforms of concern here produced by Russian companies. Oxygen Forensics and its parent company Oxygen Software were also profiled in the Spy Files. Oxygen Forensics sells a suite of mobile forensics tools that law enforcement agencies can use to retrieve practically any information stored on a confiscated phone.[26] One of Oxygen's resellers, Softline, has offices in all four of the countries discussed here, including four offices in Kazakhstan alone.[27]

Softline directly markets Oxygen's Forensics Suite on Allsoft.uz, the Uzbek version of one of its subsidiaries' websites.[28] Finally, according to a promotional document in the Spy Files, Speech Technology Center (STC), the audio forensics company based in St. Petersburg discussed in the previous section, has conducted business in Uzbekistan.[29]

One of the two cases of Western companies that have at least attempted to export surveillance or digital forensics technology to Central Asia is that of Lindon, Utah based AccessData. AccessData has developed a range of digital forensics platforms, including its SilentRunner network surveillance line. SilentRunner Mobile, for example, "allows you to monitor, capture, analyze and graphically visualize network traffic to see exactly what is happening on your network during a proactive audit or cyber investigation."[30]

AccessData lists both Softline and Moscow-based Ester Solutions as its resellers for Russia, and while it does not offer them as of January 2013, an archived version of the relevant page shows that Softline's subsidiary Axoft lists four of the company's products—including SilentRunner—on its Russian website.[31] Axoft.uz does not maintain its own list of software products, instead linking back to its Russian counterparts' catalog.[32] With respect to Ester Solutions, the reseller lists several regional telecoms that it has conducted business with, including MTS and Megafon.[33] However, as far as can be determined from Ester's website as of this writing, those services are unrelated to electronic surveillance and/or digital forensics. Any information with respect to the resale of mobile forensics equipment is unavailable at this time. The Uzbek state security services are capable of interception of landline telephone communications, internet traffic, semi-structured data such as SMS, MMS, and forum posts, and automated voice and facial recognition. They also possess some mobile forensics capability.

KAZAKHSTAN

> The Kazakh state security services are capable of interception of landline telephone communications, internet traffic, semi-structured data such as SMS, MMS, and forum posts, and automated voice and facial recognition. They also possess some mobile forensics capability as well as sophisticated data analysis software.

26 Oxygen Software (2012). *The Spy Files - Mobile forensic analysis for smartphones.* [ONLINE] Available at: http://www.wikileaks.org/spyfiles/docs/oxygen/34_mobile-forensic-analysis-for-smartphones.html. [Last Accessed 1 August 2012].

27 Softline (2012). ***Softline - информация о компании и корпоративная презентация.*** [ONLINE] Available at: http://softline.ru/about. [Last Accessed 15 July 2012].

28 Allsoft (2012). Allsoft - ***интернет магазин лицензионного софта.*** [ONLINE] Available at: http://allsoft.uz/search_result.php?words=oxygen&p=2. [Last Accessed 1 December 2012]. and Allsoft.kz (2012). Allsoft - **интернет магазин лицензионного софта**. [ONLINE] Available at: http://allsoft.kz/search_result.php?words=oxygen&p=2. [Last Accessed 1 December 2012].

29 Ilya Oparin (2009). *Complex Identification Decision Based on Several Independent Speaker Recognition Methods.* [ONLINE] Available at: http://www.wikileaks.org/spyfiles/files/0/52_200906-ISS-PRG-STC.pdf. [Last Accessed 1 December 2012].

30 AccessData (2012). *SilentRunner Mobile Network Forensics Software.* [ONLINE] Available at: http://accessdata.com/products/digital-forensics/silentrunner-mobile. [Last Accessed 1 December 2012].

31 AccessData (2012). *Partners | AccessData.* [ONLINE] Available at: http://www.accessdata.com/partners/partners. [Last Accessed 1 December 2012].and the European section of its reseller directory, as well as Axoff (2012). AccessData: **обзор**. [ONLINE] Available at: http://web.archive.org/web/20120701144310/http://axoft.ru/software/AccessData/. [Last Accessed 1 December 2012].

32 Axoff.uz (2012). **Главная | «Аксофт» — дистрибуция программного обеспечения.** [ONLINE] Available at: http://axoft.uz/. [Last Accessed 1 December 2012].

33 Ester Solutions (2012). **Клиенты. Эстер Солюшнс** (Ester Solutions) - **Разработка программного обеспечения, управление SIM-картами, системная интеграция, сервисные приложения для мобильных операторов.**. [ONLINE] Available at: http://www.estersolutions.ru/ru/clients/. [Last Accessed 1 December 2012].

In Kazakhstan, the authorities have similar capabilities as Uzbekistan with respect to SORM. MFI-Soft, through its intermediary ALOE Systems, lists the Kazakh telecoms Astel OJSC, JSC Nursat, and the 51% state-owned KazakhTelecom on its list of customers.[34] STC, the audio forensics company based in St. Petersburg discussed in the "Background" section, has conducted business in Kazakhstan.[35] Oxygen Software, the mobile forensics company discussed in the above subsection on Uzbekistan, through its reseller Softline directly markets Oxygen's Forensics Suite on Allsoft.kz, the Kazakh version of one of its subsidiaries' websites.[36]

SORM-3, which encompasses an even greater variety of communications such as SMS, MMS, forums, blogs, and social networks, also requires significant logging and automated analysis capabilities.[37] The "Semantic Archive" system developed by Moscow-based Analytical Business Solutions (ABS) is used for exactly this purpose.[38] Systems like Semantic Archive are designed to draw together all of these sources of information into one easily searchable database. The FSB and KazakhTelecom both make use of this system. Promotional literature for ABS also lists several important telecoms in the region, such as MTS and the Vimpelcom brand Beeline.[39] Similar products include the "Xfiles" system produced by Russian company i-Teco, which lists the Kazakh Ministry of Justice as one of its partners as well as several regional telecoms.[40]

The Kazakh state security services are capable of interception of landline telephone communications, internet traffic, semi-structured data such as SMS, MMS, and forum posts, and automated voice and facial recognition. They also possess some mobile forensics capability as well as sophisticated data analysis software.

TAJIKISTAN

> The Tajik state security services are capable of interception of landline telephone communications, internet traffic, and possibly semi-structured data such as SMS, MMS, and forum posts.

A much smaller number of companies provide SORM components in Tajikistan. MFI-Soft and PROTEI (both profiled in the above discussion of Uzbekistan) have conducted business in this country. MFI-Soft's intermediary, ALOE Systems lists the Tajik subsidiary of the multi-national telecom Beeline on its list of customers.[41] PROTEI also lists the Tajik subsidiary of the Russian telecom Megafon as one of its customers.[42]

TURKMENISTAN

> The Turkmen state security services possess some automated voice and facial recognition capabilities, and have acquired at least a demo version of Gamma International's mobile surveillance platform.

Speech Technology Center (STC), the audio forensics company based in St. Petersburg discussed in the previous "Background" section, has also conducted business in Turkmenistan.[43] In addition, British-German company Gamma

34 See footnote #21

35 See footnote #29

36 See footnote #28

37 MFI Soft (2012). ***СОРМ3 | МФИ Софт.*** [ONLINE] Available at: http://www.mfisoft.ru/products/sorm/sorm3/yanvar. [Last Accessed 1 December 2012].

38 See footnotes #6 and Andrei Soldatov and Irina Borogan (2012). *The Russian state and surveillance technology.* [ONLINE] Available at: http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/russian-state-and-surveillance-technology. [Last Accessed 1 November 2012].

39 Denis Shatrov, Vitaly Kuzin, and EugeneChubrov (2011). *e.g. Training and certification.* [ONLINE] Available at: http://www.slideshare.net/lp1009/abs-invest. [Last Accessed 1 December 2012].

40 i-Teco (2012). "*i-Teco*". [ONLINE] Available at: http://www.i-teco.ru/company_eng.html. [Last Accessed 1 August 2012].

41 See footnote #21

42 PROTEI (2012). *Telecommunication Solutions - PROTEI.* [ONLINE] Available at: http://www.protei.com/company/customers/. [Last Accessed 15 August 2012].

43 See footnote #29

International has exported what is at least a demo version of its Mobile software to Turkmenistan. According to documents obtained by the German news program ZAPP,[44] Gamma sought out a contract with the Turkmen authorities in collaboration with Swiss company Dreamlab AG. FinSpy Mobile is a surveillance system developed by Gamma that targets specific users using techniques similar to traditional malware. With the aid of specialized equipment installed in the server room of the targeted user's ISP, the user is presented with what appears to be a standard update to a commonly used mobile or desktop application (e.g. iTunes), but this "update" is actually a program that will transmit any kind of external communication, including data from the onboard microphone and camera, back to a command and control server run by the agency conducting surveillance. This system completely circumvents any and all encryption or other security measures. When samples of the Mobile spyware were analysed by security experts at the University of Toronto Citizen Lab, scans of the public internet for command and control servers revealed an installation at an IP address associated with the Turkmen Ministry of Communications.[45]

The reaction from civil society to this discovery has been helpful, but it is only one development in the broader problem of Western export controls with respect to Central Asia. The British Treasury Solicitor did issue a statement clarifying that it considers FinSpy to be "dual-use technology" and therefore subject to EU export controls, and that Gamma will have to apply for an export license to sell FinSpy outside of the EU. However, it remains to be seen how this decision will be enforced, whether the license requirement will be retroactively applied, and whether or not Gamma initially applied for a license to export FinSpy to Turkmenistan. It is also unclear how Gamma may attempt to circumvent these controls.[46]

BROADER TRENDS

Beyond this mapping of companies to specific countries, there are several broader trends that hold for the entire region that merit an extended discussion, specifically with respect to connections between the Russian surveillance companies and the Russian security establishment and the problem of tracing companies through resellers to end consumers.

For example, MFI-Soft has well-established ties to the Russian security services. The company's president, Alexander Ivanov, was Deputy Minister for Communications responsible for satellite and radio communications in the Soviet Union from 1989 to 1992, and served in the Russian Armed Forces for several years afterwards.[47] When the company was created in 2007, Ivanov stated that "we do not deny and do not see anything wrong with the use of administrative resources, [and] relationships with federal agencies and entities," and he specifically mentioned the FSB.[48]

> Because of these well-established connections, some of the countries discussed here have been hesitant to rely solely on Russian technology. For example, according to confidential sources contacted in the course of researching this document, the Kazakh National Security Council does not use the semantic database component of SORM-3 and has developed its own equivalent components due to suspected Russian backdoors in the system. It is also worth noting that civil society groups in Kyrgyzstan have expressed similar concerns regarding their country's implementation of the system.[49]

44 ZAPP (2012). *German Spyware for Dictators.* [ONLINE] Available at: http://www.ndr.de/fernsehen/sendungen/zapp/media/zapp4923.html. [Last Accessed 1 December 2012].

45 Morgan Marquis-Boire, Bill Marczak and Claudio Guarnieri (2012). *The SmartPhone Who Loved Me: FinFisher Goes Mobile?.* [ONLINE] Available at: https://citizenlab.org/wp-content/uploads/2012/08/11-2012-thesmartphonewholovedme.pdf. [Last Accessed 1 September 2012].

46 Privacy International (2012). *British government admits it has already started controlling exports of Gamma International's FinSpy.* [ONLINE] Available at: https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma. [Last Accessed 1 October 2012].

47 MFI-Soft (2012). ***Руководство | МФИ Софт.*** [ONLINE] Available at: http://www.mfisoft.ru/about/managment. [Last Accessed 1 December 2012].

48 Inna Erokhina and Alexander Malakhov (2007). ***Экс-глава Госкомсвязи решил торговать коммутаторами.*** [ONLINE] Available at: http://www.kommersant.ru/doc/751197. [Last Accessed 10 October 2012].

49 n/a (2012). *Kyrgyzstan: Bishkek Snoops Relying on Russian Spyware.* [ONLINE] Available at: http://www.eurasianet.org/node/66150. [Last Accessed 8 November 2012].

Finally, wikis of surveillance companies such as BuggedPlanet, Blue Cabinet, and the Spy Files have only exposed so much of the global surveillance industry. Due to the vast global network of software distributors and resellers of which this paper has taken a miniscule snapshot, and the multinational nature of modern telecom companies, it is sometimes far from clear, when relying solely on these wikis, where an arbitrary surveillance company's products are exported. Establishing the linkages from the companies that make this technology to the resellers who distribute it to the end users, whether they are telecoms installing electronic intercept equipment or security services buying digital forensics software is difficult even with the vast amount of open sources currently available.

TOWARDS A PLAN OF ACTION

Post-Soviet Central Asia is one of the most neglected regions in the global movement for a free, safe, and open internet where the right to privacy is universally respected. The seeming lack of options and allies with respect to surveillance technology in the region is a symptom of a broader problem that extends beyond this one issue: the lack of engagement by the international internet freedom community with what few civil society groups do independently operate in the region. However, there are a few general strategies that civil society groups in the region and elsewhere can pursue to begin to counteract the use of surveillance technologies to spy on dissidents and journalists. *The author would like to emphasize, however, that there are no easy solutions to this problem and leaves it to further work to fully realize what will be casually discussed here.*

1. WESTERN "NAMING AND SHAMING."

The multinational character of a few of these surveillance companies may expose a pressure point for digital rights activists, whether through shareholder and investor advocacy or public campaigns and government sanctions. It is worth noting that STC does have wholly-owned subsidiaries in the U.S., Germany, and Mexico. From another angle, the Russian government has made some effort to attract foreign investment in the tech sector. While most investment in the government-backed Skolkovo tech park outside Moscow has been concentrated on unrelated companies such as Yandex or Mail.ru, more investigative work is needed to determine if some Western investors have partnered with any of the companies profiled in this document.[50] MFI-Soft has an office in Skolkovo,[51] along with a spinoff of Speech Technology Center.[52] Some of the press surrounding Skolkovo and foreign investment in Russian IT in general reveals that investors are already somewhat uneasy about these investments, a result of endemic corruption in the Russian economy. Some bad press over the companies they do business with may be especially effective in persuading these investors to withdraw. Of course, this strategy does pose a potential problem of retreat. If a Western investment firm ends its partnership with a Russian surveillance company, that same opportunity could be picked up by a Russian firm.

2. INTERNATIONAL CAMPAIGNING.

There are some limited options with respect to highlighting human rights abuses in this area on the international stage. Frank La Rue, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, has already released a statement discussing threats to freedom of speech online. The Rapporteur's report talks directly about threats to privacy, referencing Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[53] The complaint procedure associated with the Rapporteur's office could be helpful in some cases. The Rapporteur's recent country visits (which, admittedly, require an invitation by the government being visited) have also mentioned freedom of expression online (the best example

50 The Economist (2012). *Russia aims to create a new Silicon Valley.* [ONLINE] Available at: http://afr.com/p/technology/russia_aims_to_create_new_silicon_A8ANhJkb1zBaV2Aiu16jbP. [Last Accessed 1 August 2012].

51 sk.ru (2012). ООО "*МФИ Софт*". [ONLINE] Available at: http://community.sk.ru/net/1110043/. [Last Accessed 1 December 2012].

52 See footnote #6

53 UNHRC (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue**. [ONLINE] Available at: https://s3.amazonaws.com/access.3cdn.net/61561d24e3a5fd6e47_yzm6bno8i.pdf. [Last Accessed 1 December 2012].

being the visit to South Korea two years ago), but none of the recently visited countries are of interest here. As Access has recommended elsewhere, if analyses of the rights to freedom of expression and privacy online are incorporated into the UN Human Rights Council's Universal Periodic Review (UPR) process, it could go a long way towards raising awareness as these countries come up for review in the coming years.[54] The OSCE Representative on Freedom of the Media, Dunja Mijatovic, has also made many statements regarding digital rights specifically in Central Asia.[55]

3. DIRECT ACTION AND SPECULATIVE RESEARCH

A wide range of technical work is needed to begin to address the problem of surveillance technology in Central Asia and beyond. It may be possible to detect the presence and activities of many of these surveillance systems using the Layer8 system under development by Freedom House, but more exploratory research and development is needed before these systems can be deployed in a meaningful way with respect to surveillance. There may also be some possibilities for direct action by means that Access should not and would never directly engage in. For example, Collin Anderson, an independent researcher specializing in digital rights issues in the Middle East, described a 50GB log obtained by the activist group Telecomix from a poorly secured file server at Syria Telecom that yielded valuable information about the use of censorship and monitoring systems created by Blue Coat Systems, a Silicon Valley web security firm.[56] The author hastens to add that neither he nor Access endorses any attempt to compromise the security of any Central Asian security services, but it is not an endorsement of these acts to note that the information obtained from similar agencies has been useful to civil society groups.

4. CAPACITY BUILDING, AND SECURITY EDUCATION.

As Access has learned in discussions with civil society organisations representing some of the most at-risk users around the world, there is a general need for capacity building and education with respect to tools for secure and private communication (e.g. encrypted phone communications and text messaging and secure IM clients). Users need to understand the threats and risks associated with an environment where pervasive electronic surveillance exists, and how best to mitigate those risks.

5. FURTHER INVESTIGATIVE WORK.

One of the main reasons this document has focused on the role of Russian surveillance companies is the significant amount of open sources on their operations in the region. According to confidential sources, the role of Western, Israeli, and Chinese companies could be just as important, if not more. Note that a leaked cable from Wikileaks from the U.S. embassy in Ashgabat, Turkmenistan dated July 2009 described Siemens AG as "reportedly...a major supplier of surveillance equipment for Turkmen secret services."[57] This cable was written four months after Siemens spun off its monitoring/lawful intercept unit to create Trovicor GmbH.[58] It is possible that Trovicor could still be maintaining this equipment, but to the author's knowledge this has yet to be openly proven.

With respect to Chinese companies, Huawei and ZTE have both conducted significant business in Tajikistan, Turkmenistan, and Uzbekistan. Given the case of Huawei in Iran briefly discussed at the outset of this document, it is highly possible that these companies have sold dual-use technology in the region as well. However, we have not been able to find any open or confidential sources that conclusively prove links between these companies and surveillance tech in the region.[59]

54 Peter Micek (2012). *UN Human Rights Council adopts resolution affirming human rights on internet.* [ONLINE] Available at: https://www.accessnow.org/blog/un-human-rights-council-adopts-resolution-affirming-human-rights-on-interne/. [Last Accessed 1 December 2012].

55 OSCE (2012). *OSCE media representative asks Tajikistan to unblock YouTube and to ensure free flow of information.* [ONLINE] Available at: http://www.osce.org/fom/92477. [Last Accessed 1 August 2012].

56 Collin Anderson (2012). *BlueCoat and Syria: Indicators and Culpability.* [ONLINE] Available at: http://b.averysmallbird.com/entries/bluecoat-and-syria-indicators-and-culpability. [Last Accessed 1 December 2012].

57 U.S. Embassy in Ashgabat (2011). *GERMAN BUSINESS IN TURKMENISTAN.* [ONLINE] Available at: http://wikileaks.org/cable/2009/07/09ASHGABAT859.html. [Last Accessed 1 December 2012].

58 Vernon Silver & Ben Elgin (2011). *Torture in Bahrain Becomes Routine With Help From Nokia Siemens.* [ONLINE] Available at: http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html. [Last Accessed 1 November 2012].

59 Deirdre Tynan (2012). *Central Asia: Are Chinese Telecoms Acting as the Ears for Central Asian Authoritarians?.* [ONLINE] Available at: http://www.eurasianet.org/node/65008. [Last Accessed 1 September 2012].

6. BALANCED LAWFUL INTERCEPT POLICY.

It is worth pointing out that all of the technologies described here have perfectly legitimate uses. Nothing in this document should be construed as a condemnation of the general practice of lawful intercept, as long as that interception is truly lawful and conducted in accordance with international norms ensuring basic human rights to privacy and due process. However, given the chronically poor human rights record of all but one of the four countries profiled here and the dominance of the executive branch, any real reform of their legal and regulatory system in the near future is unlikely at best. The one possible exception is Tajikistan, which has had the most viable civil society of these four countries and even a local digital rights advocacy group in the Dushanbe-based Civil Internet Policy Initiative. A serious effort to create balanced LI policy in this country may be a practical option, and it is perhaps all the more urgently needed given the increasingly difficult situation faced by local NGOs.[60] The recent Draft International Principles on Communications Surveillance and Human Rights, a developing framework for balanced lawful intercept policy, could be a good starting point here.[61]

7. A NOTE ON SANCTIONS, EXPORT CONTROLS, AND REPORTING.

The case of Finspy and Turkmenistan is one positive development in the use of export controls to address the export of surveillance equipment to Central Asia, and there is a movement, led in part by Dutch MEP Marietje Schaake, to require the European Commission "to provide a regularly updated list of restricted products and countries."[62] However, any similar efforts in the U.S. would be far less likely to succeed, given that Kazakhstan, Uzbekistan, and Tajikistan are all on the Northern Distribution Network (NDN), a crucial supply route for operations in Afghanistan, in addition to an important refueling station in Ashgabat.[63] In any case, any Western sanctions could potentially shift the demand to the Russian companies profiled here or any Chinese companies that have or could conduct business in the region. It is worth noting that China is not a participating state in the Wassenaar Arrangement, one of the few international treaties dealing with the export of so-called "dual-use" technologies. Nevertheless, some people say that digital rights groups have a moral imperative to call for greater sanctions.

8. LEGAL ACTION AGAINST SURVEILLANCE COMPANIES.

All of these companies have at least some knowledge of where their products are sold, the above discussion of AccessData notwithstanding. Litigation against these companies is a rarely discussed but potentially highly useful means of bringing to the public attention where these technologies have been used and the people affected by them.

Given the chronically poor human rights record of all but one of the four countries profiled here and the dominance of the executive branch, any real reform of their legal and regulatory system in the near future is unlikely at best. The one possible exception is Tajikistan, which has had the most viable civil society of these four countries and even a local digital rights advocacy group in the Dushanbe-based Civil Internet Policy Initiative.

60 Eurasianet.org (2012). *Tajikistan: NGOs Feeling Heat in Winter.* [ONLINE] Available at: http://www.eurasianet.org/node/66177. [Last Accessed 15 November 2012].

61 See http://necessaryandproportionate.net and Raegan MacDonald (2012). *Trending: Rise of 'lawful access' requests pose challenge for user rights.* [ONLINE] Available at: https://www.accessnow.org/blog/2012/11/28/lawful-access-challenge-for-rights. [Last Accessed 1 December 2012].

62 Leila Nachawati (2012). *EU to Tighten Rules on Surveillance Technology Exports.* [ONLINE] Available at: http://advocacy.globalvoicesonline.org/2012/11/01/eu-to-tighten-the-rules-on-surveillance-technology-exports/. [Last Accessed 1 December 2012].

63 BenPiven(2012).*Map:USbasesencirclelran.*[ONLINE]Availableat:http://www.aljazeera.com/indepth/interactive/2012/04/2012417131242767298.html. [Last Accessed 1 September 2012].

CONCLUSION

The struggle for digital rights in post-Soviet Central Asia is greatly hindered by the fact that much of the necessary technology used to eavesdrop on online communications is available from Russian companies, thereby bypassing a wide variety of successful tactics that have been used against Western companies that export similar technologies to repressive regimes. The kinds of potential surveillance range from traditional wiretapping of analog communications all the way to sophisticated monitoring systems backed by massive databases designed to handle data from blogs and social networks. While there are no easy solutions, there are some potential advocacy avenues in the area of "naming and shaming" at the level of Western foreign investment, drawing attention to these abuses in the international arena, and, most importantly, on-the-ground collaboration with local civil society groups. If recent victories in the area of internet censorship can provide any example, the most successful campaigns in this area are the ones where local groups are "in the driver's seat." When these groups are appropriately aided and advised by the global digital community, we can begin to push back against this threat to civil society in an all too ignored region of the former Soviet Union.

ACKNOWLEDGEMENTS

The author would like to acknowledge the invaluable input of Brett Solomon and Jochai Ben-Avie in the creation of this document. He also thanks Rafal Rohozinski, Masha Feiguinova, Erik Johnson, Eric King, Artem Goryainov, and Collin Anderson for their input.

Appendix: Table of Companies Profiled

Company Name	Product	Short Description	Based in	KZ	UZ	TJ	TM
MFI-Soft	SORM Components (SORM 1, 2 and 3)	Interception of landline telephone communications (SORM 1), internet traffic (SORM 2), and semi-structured data such as SMS, MMS, and forum posts with long-term storage and equipment for remote operation (SORM 3)	Nizhny Novgorod/ Moscow, Russian Federation	X	X	X	
Speech Technology Center (STC)	Audio Forensics/ Biometric recognition	Voice and facial recognition, automated recognition based on other biometric data (e.g. fingerprints)	St. Petersburg, Russian Federation	X	X		X
Protei	SORM Components	See MFI-Soft	St. Petersburg, Russian Federation (Middle East/North Africa branch in Amman, Jordan		X	X	
Analytic Business Solutions (ABS)	SORM-3 Database Components	Analysis of diverse sources of information (forum posts, MMS, social networks) for data mining and intelligence analysis	Moscow, Russian Federation	X			
iTeco	SORM-3 Database Components	See ABS		X			
AccessData	Dual-Use Network monitoring technology	Can intercept network traffic, potential use in SORM 2 or 3	Lindon, UT, USA		X		
Gamma International	Spyware	Extracts data (including live microphone and camera data) from mobile phones in use by targeted users via traditional Trojan malware techniques	Andover, United Kingdom				X
Oxygen Software	Mobile forensics	Extraction of all data from confiscated mobile phones	Moscow, Russian Federation	X	X		