Early Detection of Censorship Events with Psiphon Network Data

Simin Kargar
Psiphon
Washington, D.C.
email: s.kargar@psiphon.ca

Keith McManamen
Psiphon
Toronto, Canada
email: k.mcmanamen@psiphon.ca

Jacob Klein
Psiphon
Washington, D.C.
email: j.klein@psiphon.ca

***Abstract*—Over the past decade, circumvention tools have had a significant impact in ensuring access to censored content and preserving user privacy online. In addition, circumvention network data can be used to detect early indicators of Internet censorship and identify population-level effects of changes in the network environment. Monitoring network traffic for key indicators provides an opportunity to diagnose, analyze, and respond to online censorship events in real time. This paper examines the performance of Psiphon, a free and open source circumvention tool, during blocking events that occured over the past year in Iran, Iraq, and Turkmenistan. The study also offers insight into how Psiphon network data detected early signs of blocking in these examples. Through three case studies, we explore detailed data that were leveraged to improve Psiphon network resiliency during socially and politically critical times in various contexts.**

Keywords-information controls; online censorship; Internet shutdown; circumvention tools; social media blocking; psiphon.

I. INTRODUCTION

This study presents analysis of three major censorship events that occurred in 2018 in the context of observable anomalies in discrete time series data from Psiphon network. Psiphon offers free, open source tools that are accessible, easily operated, and trusted worldwide. Psiphon provides recourse to online censorship by routing a user's Internet connection via a distributed global network of servers. Like other Virtual Private Network (VPN) software, an encrypted tunnel is established between the user's device and a Psiphon server, allowing traffic to be transmitted securely and thereby circumvent filtering on censored networks. Although encrypted, VPN traffic tends to have identifiable characteristics and traffic patterns increasingly vulnerable to blocking by deep-packet inspection (DPI) and traffic fingerprinting. Psiphon is designed to mitigate the risk of direct attempts to disrupt network traffic by using sophisticated traffic obfuscation techniques that disguise and vary readily-identifiable features in Internet traffic and provide resilience to fingerprinting. Moreover, a multi-protocol architecture of transports ensures network resiliency in the event that censors successfully fingerprint and block a subset of those protocols. Amid intensifying censorship against VPNs and circumvention tools, the reliability of the Psiphon network has driven widespread adoption in countries that continuously censor the Internet as well as in response to spontaneous censorship events.

Consequently, both in regions where the use of circumvention tools is a persistent need, and where politically-motivated, isolated, and unexpected censorship and network attack events occur, Psiphon has consistently provided a statistically significant snapshot of circumvention tool usage patterns. Disruptions in network performance typically follow social and political contours. They also offer an opportunity to investigate blocking events in real time. Given that the dynamics and internal workings of Internet censorship are highly opaque to media and civil society, this network vantage point provides unique insight into the technical context behind these critical events.

By reviewing case studies from three different contexts, this paper offers a baseline for targeted and strategic blocking events that occurred in response to emerging Internet policy developments and critical socio-political events. The remainder of the paper comprises of the following:

Section II provides an overview of related work in this space. Section 3 explores Psiphon network data of three blocking events from 2018 that occurred in Iran, Iraq, and Turkmenistan with a population-level effect. Section IV discusses how this approach can contribute to the accurate identification of periods of anomalous Psiphon usage as an early warning sign of censorship and targeted Psiphon blocking. Finally, Section V concludes by discussing the implications of anomalies and early detection of online blocking events for Psiphon's ability to rapidly scale and reach populations at the height of critical times. It also offers some direction for future work in this space.

II. RELATED WORK

While circumvention network data remains an underutilized point of analysis, past research in this area has used metrics from the Tor network and quantitative statistical models. The anomaly-based censorship detection system developed by Danezis analyses time series connection data over seven-day periods, flagging an anomaly whenever total Tor connections from a country deviate from the normal distribution of the top 50 Tor-using countries [1]. Wright, Darer, and Farnan refine this methodology to create a multivariate anomaly detection system using principal component analysis, to allow ongoing per-country detection of more nuanced internet

 ISBN: 978-1-61208-695-8

filtering events [2]. The latter emphasize the applicability of this approach to usage data of other services, including Psiphon.

While quantitative approaches are robust, one of their limitations is a tendency to be passive towards the changing social and political conditions on the ground. Two noteworthy studies have analyzed Psiphon network data using an events-based methodology. First, in 2013, Psiphon collaborated with the civil society organization ASL19 on an analysis of information controls in Iran during the 2013 Presidential elections, where censors actively endeavoured to disrupt Psiphon network traffic [3]. This study conducted a detailed examination of Psiphon data over a six-month period in the context of evolving developments in Iranian Internet policy and in the political cycle, and effectively formalized this mixed-methods approach to examining the impacts of information controls. Second, in a recent paper using data provided by Psiphon, Deibert, Oliver, and Senft build on the previous study by conducting a comparative analysis of Iranian information control regimes, contrasting tactics used to disrupt the Psiphon network during the 2016 Parliamentary elections with those employed during the prior election blocking in 2013 [4]. Likewise following this mixed-methods approach, the analysis in this study couples network analytics with the evolving sociopolitical dynamics of online censorship to enhance the blocking resilience of Psiphon tools in the unfolding local contexts.

III. CASE STUDIES

Over the past year, Psiphon registered the scale and impact of many online blocking events. Among these, the cases of Iran, Iraq, and Turkmenistan stand out due to their scope and population-level effects. The unprecedented blocking of Telegram and Instagram in Iran in late 2017 and early 2018, and the ostensibly permanent blocking of Telegram in May 2018, brought about a surge in the use of circumvention tools, in particular Psiphon [5]. A crackdown on VPN usage in Turkmenistan between January and April 2018 [6] involved intensified traffic fingerprinting that degraded the general performance of VPNs and other circumvention tools, and shifted the protocol distribution of Psiphon traffic. The government-imposed Internet [7] and social media shutdown in Iraq in July 2018 [8] led to similar surges in the Psiphon usage. Psiphon network data captured noteworthy intricacies of these events.

The following will investigate these cases in further detail to address two main research questions: (1) to what extent does data-based analysis of Internet censorship correspond to the social and political contours of a given society, and (2) how can Psiphon data be applied to develop narratives of Internet censorship in adversarial environments?

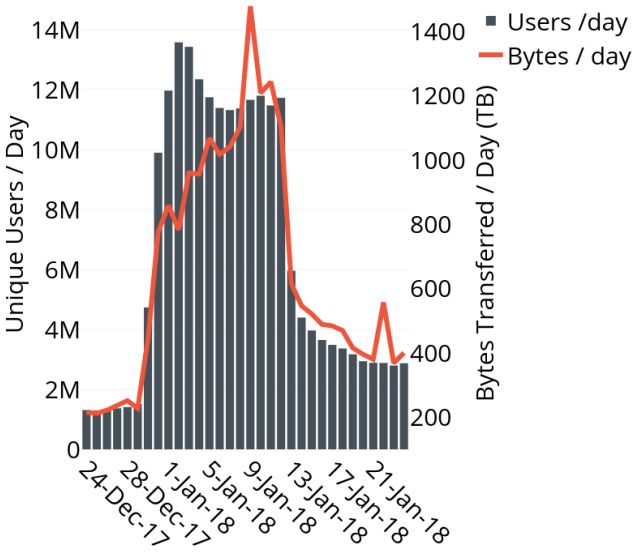

Figure 1. Iran Telegram and Instagram Blocking (Dec 2017-Jan 2018)

A. Iran

For those circumventing Iran's filtering apparatus, Psiphon has been a popular tool since its inception in 2006. Between late December 2017 and the second week of January 2018, anti-government demonstrations broke out across Iran as a reaction to economic grievances. Protesters effectively utilized Telegram and Instagram to organize, which precipitated a temporary ban on both platforms [9]. The government of Iran lifted the ban as the protests subsided [10], but reinstated the ban on Telegram four months later. As Figure 1 indicates, the December 31 disruption of international Internet traffic and the blocking of two popular communication tools resulted in a 600%

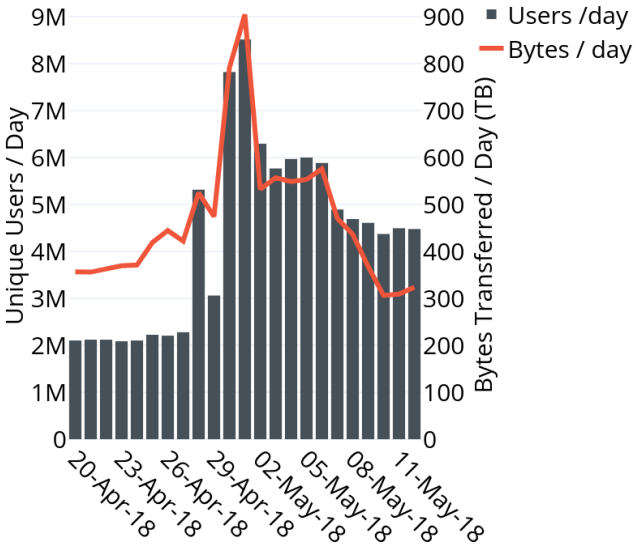

Figure 2. Iran Ban on Telegram Messenger (Apr-May 2018)

 ISBN: 978-1-61208-695-8

surge in Psiphon unique users and network bandwidth usage within 24 hours, and a 900% increase from baseline usage over the next seven days.

In late April 2018, as the permanent blocking of Telegram became imminent, Telegram servers actually faced a major outage that affected users across the UK, Europe, Russia and the Middle East [11][12]. However, concerned users in Iran attributed this problem to Iran's censorship apparatus and turned to Psiphon to restore access to the Telegram network. As Figure 2 indicates, this caused a surge in the Psiphon network on April 28, two days before Telegram was officially blocked in Iran. At the time, Telegram was the most popular messaging application with an estimated 40 million users in Iran [13]. When Iran's judiciary officially announced the ban on April 30, it drove unprecedented adoption of Psiphon on all platforms. The surge peaked at 8.5 million daily unique users, transferring 900 TB across the network. As Iranian authorities confirmed, the broad-scale adoption of circumvention tools, including Psiphon, helped mitigate the intended effects of the blocking orders [14].

B. *Iraq*

On July 9, 2018, protests broke out in the southern Iraqi city of Basra. Citizens took to the streets to demonstrate against widespread unemployment, corruption, and inadequate public services. In the days that followed, the protests spread to several other cities, making this the country's longest and most widespread protest period in recent history [15]. The government responded by declaring a state of emergency and censoring access to major social media platforms Facebook and Twitter, and messaging apps WhatsApp and Viber. Subsequently, reports of complete Internet shutdowns were received from several Iraqi cities,

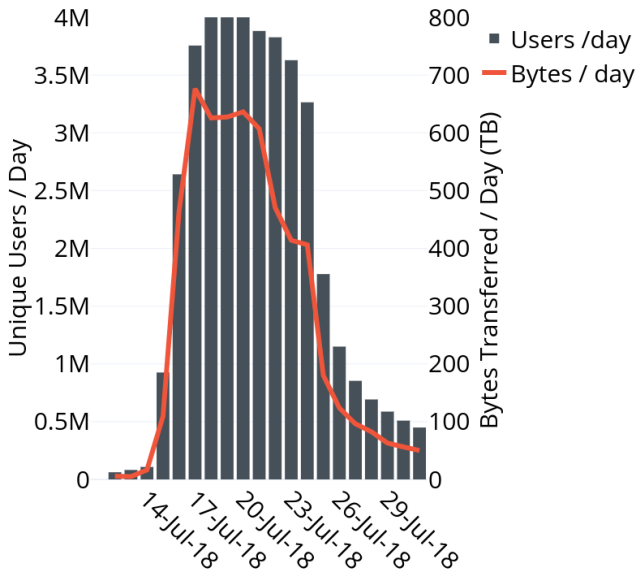

Figure 3. Iraq Social Media Shutdown (Jul 2018)

including the capital of Baghdad, on July 14 [16]. Psiphon connections from Baghdad were observed to drop from a rate of 500,000 connections per hour to zero, simultaneously across all ISPs, for the hours the shutdown persisted. This trend was reflected across 15 other Iraqi cities, indicating that a widespread Internet shutdown had been implemented. However, in regions where Internet access was not entirely blocked, such as in the Kurdistan region where Internet Service Providers (ISPs) remain moderately autonomous from central Iraqi authorities, data transfer reflected users circumventing app or site-specific blocking. A second shutdown occurred on July 19, when Psiphon connections from Baghdad decreased by 98% and network bandwidth transfer fell to nearly zero. Initially unconfirmed by news media covering the story, Psiphon data registered a second nationwide Internet shutdown in near-real time after the termination of traffic at the ISP-level, consistent with an intentional service blackout.

Soon after the onset of the first nationwide shutdown, Psiphon experienced the beginning of a surge in users as Iraqis turned to the Psiphon network to circumvent the ongoing blocking. Though the nationwide Internet shutdowns were lifted, blocks on specific social media and messaging platforms remained in effect until July 26 [17], driving up demand for circumvention tools. Following the July 19 shutdown, eight of the top ten apps in Iraq's Google Play store were VPNs, with Psiphon holding the top spot [18]. As indicated in Figure 3, Psiphon's user base grew from 50,000 to over 4 million between July 12 and July 20, and elevated usage persisted until the social media blocking was lifted. Since these events, the baseline number of users connecting to Psiphon from Iraq has increased 2.9% on the pre-blocking monthly average.

C. *Turkmenistan*

Beginning in early 2018, the state-owned and only operating ISP in Turkmenistan, TurkmenTelecom, initiated a crackdown on VPNs. Media sources reported that TurkmenTelecom was using newly acquired high-speed DPI filtering technology at scale to identify and block circumvention traffic [19]. As Radio Free Europe's Turkmen service reported, the ISP targeted individual Internet users and notified them that continued use of VPNs or proxy tools would result in disconnection from the Internet [20]. According to research conducted by the OpenNet Initiative, DPI technology has been in use in Turkmenistan since at least 2010 to maintain an extensive blacklist of websites and keywords [21]. More sophisticated traffic fingerprinting based on protocol type was not previously observed at national scale.

Psiphon network data corroborated these early reports and anecdotal claims. Beginning January 23, Psiphon's daily unique users and overall network bandwidth usage consistently decreased over the next 30 days, as indicated in

 ISBN: 978-1-61208-695-8

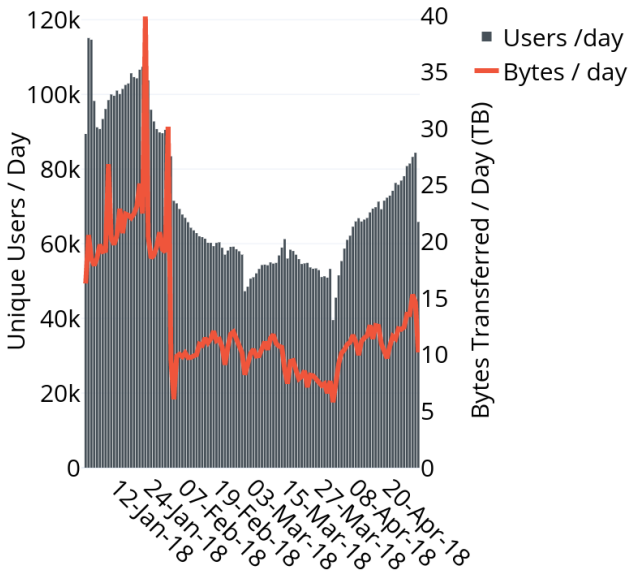

Figure 4. Turkmenistan VPN Filtering (Jan-Apr 2018)

Figure 4. The degradation of directly-connecting protocols in Turkmenistan was also evident in fluctuations in the normal Psiphon network protocol distribution. As shown in Figure 5, direct connections in blue and purple gradually became less viable, resulting in network tactics shifting the balance of traffic to more resilient transport protocols. While redundancy in Psiphon's protocol architecture allowed the network to adapt to enhanced filtering measures, the interference observed against direct connections corroborates reports that general VPN performance was effectively disrupted.

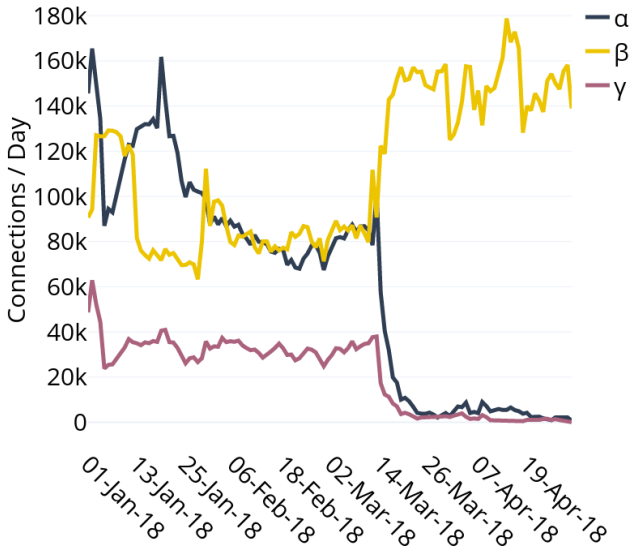

Figure 5. Turkmenistan Connections by Protocol Type (Jan-Apr 2018)

Normal network performance appeared to be restored by August 2018, but similar network interference against direct connections was observed again throughout September and November 2018, and developments remain ongoing.

IV. Discussion

Based on the case studies reviewed herein, our approach can contribute to the accurate identification of periods of anomalous Psiphon usage as an early warning sign of censorship events and, specifically, interference with Psiphon network traffic. Anomalies detected in the Psiphon network data correspond to other indicators of Internet interdiction in countries with a record of policies and tactics adversarial toward Internet freedom [22].

While this analysis demonstrates the strength of a mixed-methods appreach, it is important to acknowledge some future directions for information controls research of this nature. First, technical, quantitative analyses still remain largely decoupled from granular social and political case studies, though the dynamics of Internet censorship involve vast and inextricable dimensions of each. Certainly, the computational methodologies discussed in Section II provide important macro-scale insights that can serve as a focal point for in-depth social scientific research, but often are not intrinsically actionable intelligence for media and civil society advocacy. Second, the event-mapping methodology as applied to selected case studies here can benefit from integration with systematized, automated anomaly-detection on data feeds to allow precise real-time alerting of such events across a broader spectrum of censored countries. Third, looking forward, exploring the application of machine-learning approaches in order to more comprehensively identify the various indicators, even precursors, of critical censorship events to facilitate rapid detection and response is seen as a valuable direction for further research.

As Crete-Nishihata, Deibert, and Senft explain, the study of information controls is a multidisciplinary challenge [23]. Technical measurements are essential but will lead to greater insights into online censorship if we interpret such data with contextual knowledge and social science methods. Performing analysis on real-time filtering events as well as historical filtering behavior provides an opportunity for collaboration with academic researchers, advocacy groups, and the media. This can, in particular, offer insights into the unfolding events in places that do not often receive sufficient media coverage and international attention.

Additionally, partnerships between circumvention tool providers and other stakeholders can support consistent methods of comparing approaches taken by authoritarian regimes to their previous actions in order to further analyze their learning in the realm of online censorship [24]. This will provide a consistent baseline for comparative scholarship and investigations of online censorship cases by academic researchers, advocacy groups, and the media.

 ISBN: 978-1-61208-695-8

V. CONCLUSIONS

Detecting anomalous events within Psiphon data enables us to identify anomalies in the status of Internet freedom globally, and more specifically, in countries with a poor record of securing freedom of expression and access to information. Anomalies in multiple variants such as the number of users, bytes transferred, session duration, and length of establishing connections demonstrate the seasonality in online censorship events. Such data coupled with contextual narratives from users of circumvention tools, media, advocacy groups, and other researchers can significantly enhance our understanding of network disruptions worldwide. Through these examples, we have demonstrated how Psiphon data correspond to imminent, potential, and actual online censorship events on a national or local level. In addition, combining multiple network metrics helps to identify anomalies in Psiphon network performance as an indicator of both degraded domestic Internet performance and direct interference against Psiphon traffic. Applying this knowledge can result in a customized experience of Psiphon services, which is tailored for the unique needs of specific censorship environments, both known and emerging. Comprehensive analysis of anomalies and early detection of online blocking events enhance Psiphon's ability to rapidly scale and reach populations at the height of critical times.

Beyond the technicalities of this approach, the analysis presented herein focused on two types of state actors: (a) those that are known to engage in active filtering, and (b) states that often do not receive significant attention from the media and Internet freedom community. Partnerships between circumvention tool providers and more diverse actors will be conducive to detailed investigations of these cases and will ultimately serve a broader spectrum of stakeholders.

REFERENCES

[1] G. Danezis, An Anomaly-Based Censorship Detection System for Tor", 2011. Retrieved 2019.02.26 from: https://censorbib.nymity.ch/pdf/Danezis2011a.pdf.

[2] J. Wright, A. Darer, and O. Farnan, On Identifying Anomalies in Tor Usage with Applications in Detecting Internet Censorship, Association for Computing Machinery, 2018. Retrieved 2019.02.26 from: https://doi.org/10.1145/3201064.3201093.

[3] ASL19 and Psiphon, Information controls: Iran's presidential elections, 2013. Retrieved 2019.02.26 from: https://asl19.org/cctr/iran-2013election-report/.

[4] R. Deibert, J. Oliver, and A. Senft, Censors Get Smart: Evidence from Psiphon in Iran. Review of Policy Research, e0001, 2019. Retrieved 2019.02.26 from: https://doi.org/10.1111/ropr.12333.

[5] S. Kargar and K. McManamen, Censorship and Collateral Damage: Analyzing the Telegram Ban in Iran, September 2018, Berkman Klein Center Research Publication No. 2018-4. Retrieved 2019.02.26 from: https://dx.doi.org/10.2139/ssrn.3244046.

[6] RFE/RL (Azat Habar), Users of proxy servers in Ashgabat are denied access to the Internet, January 29, 2018. Retrieved 2019.02.26 from: https://rus.azathabar.com/a/29004792.html.

[7] NetBlocks, Study shows extent of Iraq internet shutdown and social media restrictions during protests, July 2018. Retrieved 2019.02.26 from: https://netblocks.org/reports/study-shows-extent-of-iraq-internet-shutdown-and-social-media-restrictions-during-protests-zPyXjzAE.

[8] T. Rami and L. Taha, The Iraqi government turns off the Internet in response to protesters demanding water and electricity, August 2018. Retrieved 2019.02.26 from: https://asl19.org/ar/blog/2018-08-01-iraqi-government-shuts-down-the-internet-in-response-to-protestors-demanding-water-and-electricity.html.

[9] A. Filastò and M. Xynou, Iran Protests: OONI data confirms censorship events (Part 1), January 2018. Retrieved 2019.02.26 from: https://ooni.torproject.org/post/2018-iran-protests/.

[10] Deutsche Welle, Iran unblocks Telegram messenger service shut down during country-wide protests, January 2018. Retrieved 2019.02.26 from: https://www.dw.com/en/iran-unblocks-telegram-messenger-service-shut-down-during-country-wide-protests/a-42141829.

[11] D. Snelling, Telegram DOWN - Popular messaging app not working as major outage confirmed, April 2018. Retrieved 2019.02.26 from: https://www.express.co.uk/life-style/science-technology/952670/Telegram-down-messaging-app-not-working-outage-confirmed-WhatsApp-rival.

[12] Status overview of problems at Telegram, Retrieved 2019.02.26 from: https://downdetector.com/status/telegram/news/212777-problems-at-telegram-2.

[13] A. Vahdat, Iran orders internet providers to block Telegram, April 2018. Retrieved 2019.02.26 from: https://apnews.com/22e81a82289745a49b991bae413e9b71.

[14] R. Faghihi, Iran's conservatives return to Telegram after failed ban, November 28, 2018. Retrieved 2019.02.26 from: https://www.al-monitor.com/pulse/originals/2018/11/iran-telegram-ban-conservative-media-rejoin-tasnim-fars.html.

[15] P. Cockburn, Iraq protests: Demonstrators blame 'bad government, bad roads, bad weather, and bad people', July 17, 2018. Retrieved 2019.02.26 from: https://www.independent.co.uk/news/world/iraq-protests-bad-government-roads-weather-people-haider-abadi-sadr-oil-a8451736.html.

[16] D. Madoury, Internet in Iraq Returns After Two-Day Blackout, July 18, 2018. Retrieved 2019.02.26 from: https://blogs.oracle.com/internetintelligence/internet-in-iraq-returns-after-two-day-blackout.

[17] Middle East Monitor, Iraq lifts ban on social networking sites, July 27, 2018. Retrieved 2019.02.26 from: https://www.middleeastmonitor.com/20180727-iraq-lifts-ban-on-social-networking-sites.

[18] Appbrain analytics dashboard, Retrieved 2019.02.26 from https://www.appbrain.com/.

[19] RFE/RL (Azat Habar), Expert: Turkmen authorities buy spyware for Internet control, March 12, 2018. Retrieved 2019.02.26 from: https://rus.azathabar.com/a/29091514.html.

[20] RFE/RL (Azat Habar), Users of proxy servers in Lebap are faced with the shutdown of the Internet, February 2, 2018. Retrieved 2019.02.26 from: https://rus.azathabar.com/a/29024861.html.

[21] R. Deibert, J. Zittrain, R. Rohozinski, and J. Palfrey, Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, Cambridge, MA: MIT Press, p 244, 2010.

[22] A. Shahbaz, Freedom on the Net 2018; The Rise of Digital Authoritarianism, Freedom House, 2018. Retrieved 2019.02.26 from: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

[23] M. Crete-Nishihata, R. Deibert, A. Senft, Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls, IEEE Internet Computing, vol. 17, no. 3, pp. 34-41, May-June 2013.

 ISBN: 978-1-61208-695-8