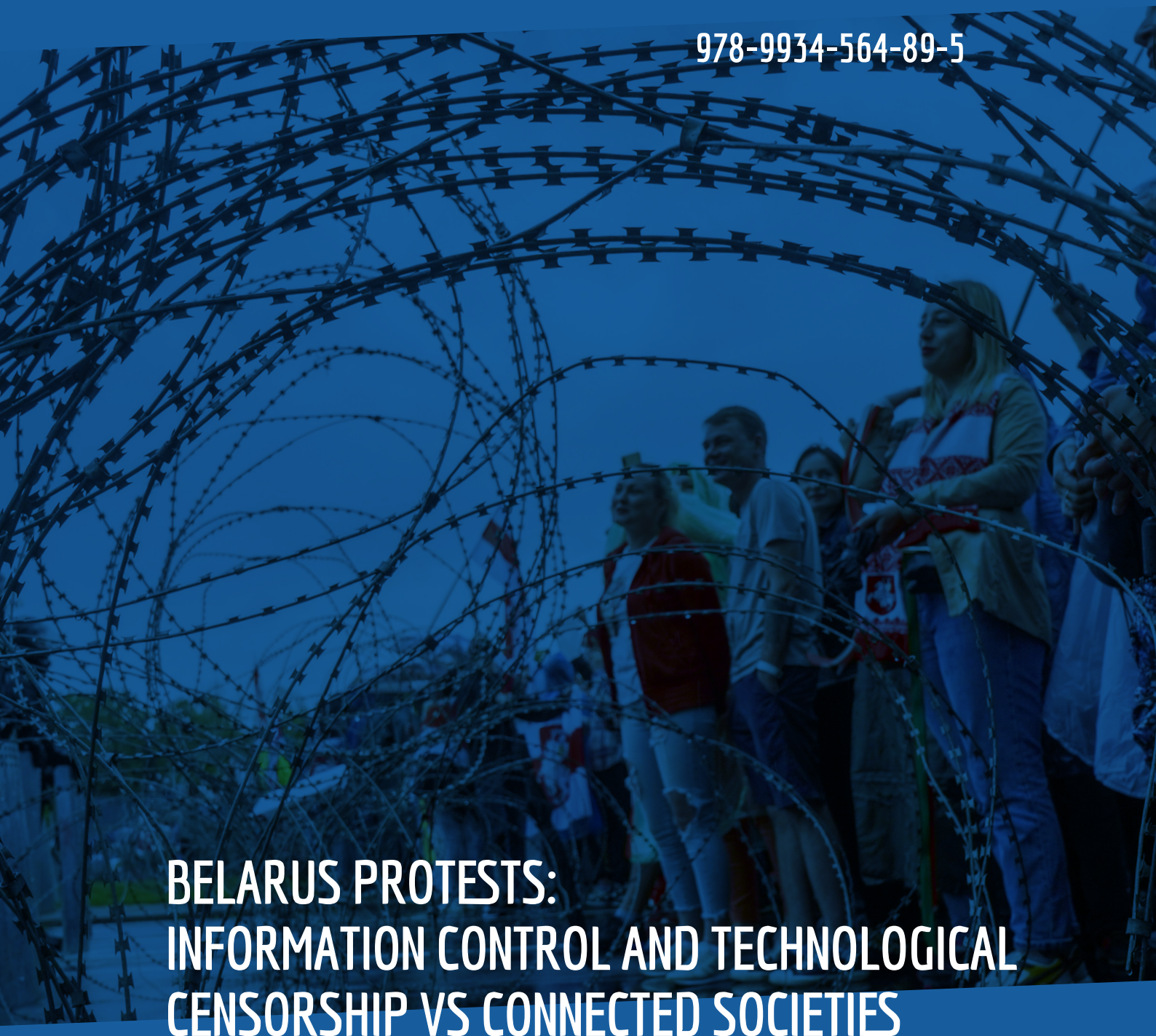
978-9934-564-89-5



BELARUS PROTESTS: INFORMATION CONTROL AND TECHNOLOGICAL CENSORSHIP VS CONNECTED SOCIETIES

Published by the
NATO Strategic Communications
Centre of Excellence

Authors: The report is prepared by the International Strategic Action Network for Security (iSANS). iSANS is an international expert initiative established in 2018 aimed at detecting, analyzing and countering hybrid threats against democracy, rule of law and sovereignty of states in Europe and Asia. The initiative's attention is focused on hostile networks of influence within Central and East Europe and former Soviet countries.
Project Manager: Marius Varna
Language Editing: Annie Geisow
Special thanks to Amanda Rivkin
Design: Linda Curika

Riga, 8 December 2020
NATO STRATCOM COE
11b Kalnciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

Introduction

The Belarusian presidential election on 9 August 2020 was a turning point in the history of modern Belarus. Disagreeing with the apparently falsified results of the vote, protesting Belarusian citizens flooded the cities around the country. Lukashenko's response was lightning fast and brutal. In order to conceal any information about the brutality of the law enforcement structures against peaceful protesters, Lukashenko attempted to take control of the information environment and restrict access to all information channels - especially Internet resources.

At the height of the protests, the internet and digital media became a window for Belarus onto the world, to speak about what is happening in Belarus and hear a response.

Unlike traditional media, the internet is harder to control. Most Belarusians have access to the internet and therefore during the protests in Belarus, many were not only consumers but sources and creators of information.

The government's attempts to restrict access to online sources of information was likely linked to the idea that Belarusians would opt for more easily accessible sources - television, radio and print media (most of which are state-controlled). Paradoxically, however, this provoked the opposite reaction as people began to look for opportunities to access unbiased news in online resources.

Telegram messenger, due to its encrypted messaging, has become the most important information channel and in a short time turned into the most influential news agency. In all the attempts by the Belarusian government to disconnect consumers from Internet resources, e.g. by instructing telephone companies to disconnect digital internet or block social media platforms, Belarusians were increasingly finding ways to circumvent these barriers. To access the internet, Belarusians used free anonymizers, VPNs (i.e. Psiphon and Tachyon) and proxy servers.

This paper explores the events in Belarus and how Lukashenko's loyal structures sought to secure control of the information space.

The Belarussian government has almost full control over traditional media. Such long-lasting focus on one part of the media has created the conditions for the development of a strong IT sector and internet infrastructure, simultaneously allowing the public to adapt to these unfiltered information channels.

This paper provides an analysis of how the Belarussian government was preparing for possible protests. What internet traffic control equipment and software was purchased and tested? What solutions did the protesters use to avoid traffic restriction and gain access to the internet?

August 2020 event timeline

Post-election protests against Aliaksandr Lukashenka have been ongoing in Belarus for many months. The situation inside the country is becoming increasingly turbulent as it enters the most severe political and economic crisis since the late 1980s when the country broke away from the USSR.

The dramatic gap between the population of the country and the Belarusian leadership is increasing. The president Lukashenka, who is not recognized neither by the European Union nor other democratic countries, aims to do everything possible to target his main enemy, the Internet, and its power to supports and mobilise the energy of protest.

The internet blackout of August 9-12 left most Belarusians in an information vacuum for 4 days and was, beyond any doubt, a violation of the international legal ban on arbitrary Internet disconnections. The vast majority of independent online media was unavailable for the duration. Whilst newspaper delivery was suspended during the first few days after election day, state TV and radio remained the main sources of information. However, they did not contain much information about the largest and longest protests in the post-war history of Belarus.

On the day of the Belarusian presidential elections, August 9, the blackout started with slower speeds for services like YouTube and Google, and poor delivery of Telegram without proxies. Then foreign websites stopped downloading almost completely, and finally local websites ceased to respond. Virtual Private Network (VPN) services ceased to operate over time, while proxies required Wi-Fi connection to operate with minimum speeds. 3G and 4G internet 'dropped' closer to 1800-2100 local time depending on location within Belarus.

The connection varied from one Internet service provider (ISP) to another, but overall they were only able to re-establish their regular service provision by the morning of August 12. A week later, some 50 news websites were banned in the territory of Belarus[1]. More followed[2]. Between August 1 and September 3, the authorities blocked at least 86 websites related to political news, human rights, and peaceful activism, as indicated by OONI Web Connectivity analysis.[3]

Pre-requisites and instruments

For many years, Belarusian state has had a complete monopoly on incoming and outbound internet traffic via two state-owned organizations which control Border Gateway Protocol connectivity in Belarus: National Traffic Exchange Center (NTEC, НЦОТ, Национальный центр обмена трафиком, ncot.by) and Beltelecom (state-owned telecommunications operator with cross-border gateways into and out of the country and ownership of most fixed communication channels in Belarus). No other ISPs in Belarus have direct access to any foreign Internet traffic without peer-to-peer channels established with either Beltelecom or NTEC.

Since late 2019, Telegram has become the driving instrument of mobilization and the main political media tribune in Belarus.[4] Despite repeated attempts to oppose pro-democratic media and Telegram channels in particular (for instance, by arresting their administrators), neither Lukashenka nor his security forces were able to limit the influence of their challengers. On the contrary, Telegram channels have become the most influential 'news agencies', setting up the daily agenda for non-governmental press and Lukashenka himself.

Whilst it was technically impossible to halt the work of Telegram channels alone (which have become the real fourth power in Belarus by early 2020), the state officials attempted to stop them at any cost. State bureaucracy understood the potential of Telegram with regards to post-election protest activity long before August 9. An internet blackout was likely chosen as a tool that was supposed to quickly stop Telegram and cut the protests just as happened in December 2010. Neither heavy collateral damage (coinciding with the launch of the Belarus Nuclear Power Station whose personnel are dependent on 'civil' mobile and internet connection), nor economic costs (that were later estimated at up to $ 170 million)[5], nor subsequent stability of the acting authorities were important enough to choose another weapon to crack down on Telegram.

The results were the opposite of those desired. After four days of silence, Telegram exploded. Instead of shutting down, pro-democratic Telegram channels grew their audiences by hundreds of thousands of subscribers, and turned into more than just coordination tools. They became nationwide media outlets with loyal audiences of at least 2.5 million readers daily. However, the remainder of the digital media and news websites fared worse.

Between around 1600 on August 9, 2020 and early morning on August 12, 2020, most websites, social networks (including Facebook, Instagram, Twitter, YouTube), instant messengers (WhatsApp, Telegram, Viber), search engines (Google, Yandex, Mail.Ru), application (AppStore!), and online taxi services were virtually inaccessible to most people within Belarus – including even basic Google services[6]. A major independent news outlet, tut.by was able to find out that its ISP, Beltelecom, capped its bandwidth at 25%[7] of its normal capacity with no explanation and no information on when it would return to normal capacity.

ATMs, payment terminals and all internet-connected real-life services and financial instruments

ceased to operate, but so did two major grassroots platforms created by the opposition IT experts to collect information about fraudulent and genuine votes (Онлайн-платформа Голос and ZUBR); these were quickly banned by the acting authorities.[8] Additionally, most websites located in the '.by' domain zone attributed to the Republic of Belarus, were not available from overseas.

Secret services also blocked numerous Virtual Private Network (or VPN) services that were widely used by the protesters to bypass the internet blackout. Nevertheless, many of them remained accessible even when the internet was almost completely shut down nationwide – and new ones popped up. This added capacity to upload materials onto social media and share them with foreign journalists. Often at very low speed, but the VPNs worked – especially during daytime and using wired Wi-Fi connections (unlike mobile 3G and 4G Internet).

To sustain the connectivity of protesters[9] and journalists[10] in the streets, the administrators of popular Telegram channels urged the residents of lower floors at multi-stored buildings to remove passwords from their Wi-Fi routers.

It has to be highlighted though that the blackout did not affect the entire Internet infrastructure across Belarus. A recent RIPE Atlas[11] report shows that a limited number of users remained connected throughout 9-12 August, 2020. This is further corroborated by OONI Probe measurements[12].

Within 4 days, millions were kept in the dark until access to Internet services was returned to full capacity. Then thousands of images and videos of unprecedented police brutality popped up on digital screens across the country. The outrage fuelled even larger-scale protests and sparked strikes in major state enterprises across Belarus. An avalanche of information about a state-run machine of violence, torture and lethality became the driving force behind the protests demanding that Aliaksandr Lukashenka resign.

The demands of protesters and people on strike remained generally unchanged since early August:

1. Lukashenka must resign;
2. All political prisoners must be released;
3. New and fair elections;
4. End of political violence;
5. All abusers of power must face justice[13].

Since none of these was fulfilled, the protesters and Coordination Council became more straightforward and proactive in applying the pressure on the bureaucracy and law enforcement agencies. So too did the countries of the West. Russia kept tightening the national legal framework for Internet use.

Internet shutdown: testing and practice

The internet shutdown in Belarus was rumoured long before August 9; thousands of digital activists, journalists, bloggers and IT professionals conducted advance preparations. Members of Lukashenka's team confirmed public fears by indicating their readiness to block the Internet. For instance, on July 30, just a week before the election, the Secretary of State Security Andrei Raukou (formerly the defence minister of Belarus) announced that the acting authorities will consider complete shutdown of the Internet if they identified any source as a threat to national security.[14]

The first likely tests of internet blackouts were reported by Belarusian human rights group Human Constanta as early as June 2020[15]. In July, a few Belarusian digital activists and IT professionals reported complete unavailability of internet connection on their devices between 0200 and 0400[16]. A few similar cases followed in July 2020.[17]

Following a public threat to shut down the Internet by the high-ranking state official A. Raukou as well as the Ministry of Interior[18], 40 international human rights groups (who were also aware of alleged shutdown tests) urgently called on Aliaksandr Lukashenka to 'ensure that internet access in Belarus remains open, accessible, and secure during the presidential elections on August 9, 2020'. They sent an open letter on August 6, 2020 – just three days before election day.[19]

In the early voting week, the first reports about Internet instability appeared in the early morning of August 9[20]. Belarus state officials claimed a foreign DDOS attack at approx. 2200 on August 8[21] (this wasn't confirmed by independent agencies like NetBlocks).

On August 9, when an almost complete blackout was imposed, all search engines, social media, as well as independent media and online taxi services ceased to operate.

The first reports of issues with internet accessibility were recorded around 0800.[22]

It is most likely that the state security (acting upon direct orders from Aliaksandr Lukashenka and his most loyal people), aimed to achieve three core goals:

1. Limiting coordination and exchange of information among the protesters;
2. Preventing journalists from sending footage of the extensive and disproportionate violence;
3. Preventing the protesters from sharing their photo and video materials of violent clashes with law enforcement (primarily to prevent them from sending to popular Telegram channels).

On the day of the election and for the next three days, the vast majority of citizens of Belarus experienced severe disruption of Internet access due to a nationwide block of SSL traffic[23]. Simply put, the whole population was unable to access websites, instant messengers, social media platforms, email providers, VPNs, proxy servers or many other services. For a few days, Telegram remained the only

> So far, the only method to completely block Telegram is to switch off the Internet across the country. Belarus managed to run the economy without an Internet connection for 61 hours.

source of connection with the outside world for many people. The technology used by Telegram, domain fronting, allows the application to connect to a so-called "front" domain (which may be acknowledged as safe by automated state security software), but it then leads to connection with actual Telegram infrastructure.[24] It makes this application very resilient to restrictive measures. So far, the only method to completely block Telegram is to switch off the Internet across the country. Belarus managed to run the economy without an Internet connection for 61 hours[25]. Iran kept its longest Internet blackout for around two weeks, but had to refrain from this practice due to the economic burden.

To bypass restrictions, many users turned to pre-installed Internet-privacy apps and tools[26]. A precaution considered an overkill before August 9 proved to be a matter of life safety in cases when the protesters were exposed to very high risk of extremely severe or even lethal injuries if captured by law enforcement on election night or thereafter.

An explosion in the use of Psiphon[27] (an open-source Internet censorship circumvention tool that uses a combination of VPN, SSH, and HTTP Proxy) on mobile devices enabled its users to evade the Internet blockade. The number of Psiphon users in Belarus exceeded 1.76 million over the first four days of the Internet blackout. Whilst the national economy was paralyzed, active Internet audience quickly learned how to bypass the blackout. It rendered the limitations futile.

The cost of the blackout was unbearable for the 'Belarusian IT miracle': according to a Netblocks COST[28] estimation, Belarus was losing over 56 million dollars a day due to Internet shutdown.[29]

After the third day of the Internet blockade, 500+ IT businessmen and senior managers addressed the acting authorities to return Internet connection due to the intolerable economic and reputational costs that Belarus was suffering internationally following August 9, 2020 events.

GSM and landline connection were reportedly available through the blockade time in all towns except Pinsk (where the city council building was captured by the protesters and extremely violent clashes with the police took place). One of possible reasons for the state to keep phone and mobile connection available is very prosaic – the state's own dependency on these means of communication in all fields, including state security coordination.

Blackout tools and official version

Lukashenka and his team blamed unidentified 'foreign puppeteers' in Poland, Lithuania, Ukraine, Czech Republic, the UK and elsewhere for problems with Internet connection. However, NetBlocks reported there were no DDOS attacks on Belarus from abroad[30] when the internet collapsed across the whole country.

A month after the blackout, Bloomberg published its investigation. They named a U.S. company Sandvine Inc.[31] as the provider of Deep Packet Inspection (DPI) technology for Belarusian state security.

The Deep Packet Inspection technology is the same instrument as is being deployed by China to sustain the 'Great Chinese Firewall', and by Iran to filter out 'unwanted' websites and platforms from the West. In August 2020, DPI was reportedly used by Belarusian state security to implement internet-censorship and digital blackout.

With $2.5-million-worth of Sandvine equipment and software, all traffic was routed by Belarus officials through a single DPI node. This caused damage to nationwide Internet connectivity and paralyzed the country's digital economy and business (since data flow exceeded the capacity of the DPI). Along with the lack of a proper firewall, this is probably why connectivity collapsed to most websites and online services on most devices. Although there were rumours[32] of Chinese experts[33] brought in to build 'Chinese firewall mini'[34], no evidence of this was provided.

Although Sandvine[35] management initially denied sales of its equipment to Belarusian state security, it was later forced to condemn the constraints on the freedom of information under public pressure. The company acknowledged that its equipment was sold to Belarusian state security by a Russia-based distribution company. Sandvine announced that it would cancel the contract for any equipment or services sold to Belarus (these potentially violated the US embargo on similar goods).

State control of Internet and information environment

Is the Belarusian state able to gain full control of the information environment? As of mid-November 2020, the short answer is no. Although Belarusian authorities have a de-facto monopoly on [politically-related] print press, TV and radio, the rise of Telegram channels[36] flipped the position of the state in setting up the media agenda[37]. For as long as it will remain impossible to block Telegram without simultaneously harming the national economy, the Belarusian Telegram community will likely remain the actual "fourth power". The interconnectivity of digital business solutions (such as digital payments) and real-life trade and services has become so vital for the economy that Internet blackout cannot be the weapon of choice for the acting officials.

In August 2020, official releases by three major state-owned organizations involved in Internet-control (National Center for Response to Computer Incidents[38], the National Traffic Exchange Center / NTEC[39], and Beltelecom[40]) claimed that all Internet disruption resulted from foreign DDOS[41]-attacks on Belarusian Internet infrastructure and websites of state institutions, causing subsequent equipment failure. Later, Lukashenka officially claimed that the Internet was being switched off from abroad to cause public unrest.[42]

> For as long as it will remain impossible to block Telegram without simultaneously harming the national economy, the Belarusian Telegram community will likely remain the actual "fourth power".

Nevertheless, no private ISPs reported any DDOS-attacks from abroad between 9 and 12 August. Moreover, two major mobile Internet providers, A1 Belarus and MTS Belarus, regularly inform their users that Internet connection is being restricted during political manifestations against Lukashenka 'upon the request' of undefined 'authorized state institutions' which are likely to be state security bodies, such as KGB or OAC.[43]

State bodies claimed the use of UDP Flooding, UDP Fragment, UDP0 (Port 0) Flooding, DNS Flooding, ICMP Misuse and NTP Flooding attacks from abroad. However, it is more likely that this is a complete list of types of attack algorithms that was gradually used by the Belarusian state to silence all dissident voices and avoid dissemination of uncomfortable videos and photos.

The state in Belarus has control of external Internet traffic to such an extent that all incoming Internet is de-facto dependent on NTEC as centralizing institution. Thus, it seems almost impossible to shut down national Internet service for 4 days from overseas due to the complexity of such a mission. A nefarious non-state actor would need to engage numerous operators from all states connected to the Belarusian part of the Internet network to halt the exchange of data with the republic – on a global level. Even within the region, this would have required the joint efforts of countries as different and hostile to each other as Ukraine and Russia. Reaching a global agreement to shut down the internet in Belarus would have been even more difficult – and there is no clear motivation for such a mission organized from abroad.

Foreign attack could have limited the bandwidth, but it would not have put national Internet infrastructure on its knees to do this. The Belarusian Internet network is indeed more vulnerable to external attacks (due to centralization of in-and-out Internet traffic) compared to countries with distributed networks and border protocols. A larger number of distributed domestic networks and Internet service providers makes the national system a lot more secure since it leaves more options for communication with international networks within the global Internet infrastructure, and thus minimizes the risk of system collapse against hypothetic external attacks. However, centralization does not provide an open door to a complete shutdown of Internet connectivity within the whole state.

Protesters solutions to access Internet

Although the acting authorities under the command of Aliaksandr Lukashenka have orchestrated the Internet blackout, there were a number of relatively effective instruments that enabled the use of Internet-driven software at limited capacity and circumvented the limitations: such as free anonymizers, VPNs and proxy servers.

In some cases, people used Bridgefy and Firechat instant messaging apps that help communicate without mobile or Internet connection by building Bluetooth-empowered network of devices. Although popular in Hong Kong during 2020 protests in similar circumstances, these networks were not used in Belarus as much as VPNs.

The most effective and popular VPN service to circumvent the blackout was Psiphon (it was especially effective with iPhone devices). To a certain extent, the wide spread of Psiphon and proxies is a credited to 100,000 high tech industry workers who were sharing the knowledge with their relatives, neighbours and friends. The self-organization of IT specialists within their communities bore unpredicted results: people shared this software via USB flash memory sticks, as well as by sharing posters and leaflets with direct download links to VPN and proxies printed on them.

Psiphon was developed at the University of Toronto in 2006, and uses over 3,000 international and local servers to circumvent state-imposed shutdowns of the Internet. In only a few days, the number of Psiphon users in Belarus grew from a few thousand (ahead of the election) to more than a million according to the company's records[44]. Belarusians became the second largest group of Psiphon users in the world – with first place belonging to inhabitants of Iran.

Another VPN app – Tachyon – was less popular due to its poorer productivity in Belarusian circumstances. However, it sometimes worked when Psiphon did not. Depending on the time of day (with no clear correlation to timing rather than random pickup), various applications and technologies operated better than others, so it was often necessary to check a few VPN options before one of them provided access to Internet connection.

Although Telegram was the main instrument for encrypted messaging and coordination of protesters when and where Internet was available, it often required VPN and Wi-Fi connection to work properly. In most cases, Telegram, Signal, and Facebook Messenger were the only services to remain accessible. During the protests, Telegram substantially expanded[45] its proxy capacity for Belarus and organized a method for Belarus-based users (with SIMs registered in Belarus) to cross-check the results of the election. Sviatlana Tsikhanouskaya gained a lot more votes than was reported in official results. It was further evidence of the fact that the elections were rigged and was welcomed by audiences and people motivated to continue the struggle for fair elections.

Most popular Telegram channels on Belarus and its political life are built on user-generated content: instant messaging and very basic editing allow the moderators of Telegram communities to update audiences in what is one step away from a live broadcast format. In some cases, the groups of protesters coordinated precautionary measures via SMS when a person who remained at home with VPN/proxy-sponsored Wi-Fi reported on police and OMON presence / movements in live mode – which was then updated on Telegram channels.

Russia's reaction to protests - uncontrolled information becomes a threat

Just a few days after post-election protests erupted in Belarus, Russia's former President Dmitry Medvedev, who now serves as Deputy Chairman of the Russian Security Council, urged the imposition of greater Internet control by Russia.[46]

The Kremlin has been actively involved in influence operations against Belarus through the use of Telegram over the last few years, and uses this tool to impose aggressive propaganda narratives and misinformation.[47] Whilst the Kremlin is using Telegram to grow its influence in Belarus and other foreign countries (including EU member states),[48] it is nervous about foreign access to its Internet space and prefers to limit it as much as it can afford.

In February 2019, Russia's government adopted a resolution that banned the use of satellite Internet without ground stations.[49] This document was a logical extension to the FSB position[50] on the micro-satellite Internet providers – OneWeb - in particular. Russia's primary security and intelligence agency assumes that "Space Internet" companies pose an espionage threat.

In November 2019, Russia's "sovereign internet" law came into effect causing fears of growing control and censorship of domestic Internet. The law essentially allowed Russia to operate its own internal networks independently from the rest of the World Wide Web.[51] The new legislation was immediately labelled an "online Iron Curtain", and in the worst case scenario it enables Russia to rapidly block Internet traffic.

Food for thought for the future

Three months after the elections, the Internet connection in Belarus is still regularly being limited on state orders. However, the protests are continuing and becoming more distributed across communities and show no signs of decrease. After the acting ministry of the interior labelled the protests 'a terrorist threat' it is possibly time to consider whether Belarusians will again need VPN and proxies on a scale comparable to early August 2020.

Continuing arrests have once again reached the level of mid-August and it is therefore essential for peaceful protesters and journalists to maintain a stable and safe connection. This is the case for Belarus as much as it is for all post-Soviet countries (except for the Baltic States) or anywhere in the world where journalism may face similar limitations and such recommendations constitute useful preparation measures.

After the first full-fledged Internet blackout by the Belarusian authorities, it is clear that all users in authoritarian countries must have early access to proxies and have VPNs at their disposal (most preferably – VPS / VDS) to be prepared for possible Internet blackouts by the state during instances of civil disturbance.

One immediate priority is to ensure further dissemination of information by independent journalists and further support of Telegram-type channels and their teams; including nationwide promotion of advanced VPN, SSH, and HTTP Proxies for all members of professional community.

Another contingency plan lies in supporting further development of low earth orbit (LEO) Satellite Internet constellation projects and lobbying for a test launch of these services in the airspace over Belarus (including Project Kuiper (Amazon), OneWeb (UK Government & Bharti Enterprises Limited), and StarLink (SpaceX)). This may help solve issues with future Internet blackouts if state-sponsored repression continues to increase.

Endnotes

1. Time.com, Belarus Blocks News Websites during the Protests, Retrieved from November 1, 2020.
2. Belarus: Internet Disruptions, Online Censorship. (2020, August 28). Retrieved December 02, 2020.
3. Open Data on Internet Censorship Worldwide. (n.d.). Retrieved December 02, 2020.
4. Sawitsky, J. (2020, April 20). Information sovereignty of Belarus: Old new truncheon or cooperation tool. Retrieved December 02, 2020.
5. Internet disruption hits Belarus on election day. (2020, August 09). Retrieved December 02, 2020.
6. Google. (n.d.). Traffic and Disruptions to Google. Retrieved December 02, 2020.
7. Tut.by новости [@tutby_official]. (2020, August 10). С утра 10 августа по не зависящим от нас причинам TUT.BY столкнулся с ограничениями пропускной способности за пределами нашего оборудования. [Blog post].Telegram. Retrieved December 02, 2020.
8. Tut.by news. (2020, August 21). В Беларуси ограничили доступ к сайтам платформ "Голос" и Zubr.in. Retrieved December 02, 2020.
9. Hexta Live [@nexta_live]. (2020, August 11). Жители нижних этажей — снимайте пароль со своих WiFi. Это поможет людям лучше ориентироваться в ситуации. [Blog post]. Telegram. Retrieved December 02, 2020.
10. 10 Hexta Live [@nexta_live]. (2020, August 10). Наши уже на Якуба Коласа! Кто живёт в центре — снимайте пароли с домашних WiFi, чтобы протестующие и журналисты имели доступ [Video attached]. [Blog post]. Telegram. Retrieved December 02, 2020.
11. Davies, A., Manojlovic, V., & Wilhelm, R. (2020, August 12). Our First Glance at the Belarus Outages. Ripe NCC. Retrieved December 02, 2020.
12. Open Data on Internet Censorship Worldwide. (n.d.). Retrieved December 02, 2020.
13. Тихановская, С. [@tsikhanouskaya]. (2020, October 16). Требования Народного Ультиматума должны быть выполнены. Иначе – народная забастовка 25 октября – день Народного Ультиматума. Мы заявили 3 требования, и выполнение каждого. [Blog post]. Telegram. Retrieved December 02, 2020.
14. Настоящее Время. (2020, July 30). Власти Беларуси заявили, что могут отключить в стране интернет при "угрозе безопасности" – кандидат в президенты. Retrieved December 02, 2020.
15. Goncharova, Y. (2020, June 20). Что происходило с интернетом в Беларуси 19 июня. Retrieved December 02, 2020.
16. Tut.by news. (2020, July 16). Читатели сообщают, что ночью возникли проблемы с VPN в Беларуси. Что они заметили. Retrieved December 02, 2020.
17. 17 Euroradio news. (2020, July 16). Telegram "falls" during street protests in Belarus. Retrieved December 02, 2020.
18. Belta news. (2020, July 13). При угрозе нацбезопасности МВД может блокировать доступ к интернет-ресурсам - Казакевич. Retrieved December 02, 2020.
19. #KeepItOn: Joint letter on keeping the internet open and secure during the presidential elections in Belarus. (2020, August 06). Retrieved December 02, 2020.
20. Korzun, P. (2020, August 08). Будет, как в Иране? Отвечаем на вопросы об отключении интернета. Retrieved December 02, 2020.
21. State resources under attack. (2020, August 09). Retrieved December 02, 2020.
22. Tut.by news. (2020, August 09). Белорусы сообщают о проблемах с интернетом. CERT. BY: "Государственные ресурсы подверглись атаке". Retrieved December 03, 2020.
23. Secure Sockets Layer (SSL) is a networking protocol designed for securing connections between web clients and web servers over an insecure network (like the Internet).
24. Cimpanu, C. (2020, August 08). DEF CON: New tool brings back 'domain fronting' as 'domain hiding'. Retrieved December 02, 2020.
25. Internet disruption hits Belarus on election day. (2020, August 09). Retrieved December 02, 2020.
26. Guide in case of Internet disconnection. (2020, August 07). Retrieved December 02, 2020.
27. Psiphon will be further discussed in details in one of sections below.
28. NetBlocks is a non-governmental group that monitors cybersecurity, internet governance, and digital rights.

29. Internet disruption hits Belarus on election day. (2020, August 09). Retrieved December 02, 2020.
30. Newman, L. H. (2020, August 10). Belarus has shut down the internet amid a controversial election. Retrieved December 02, 2020.
31. Gallagher, R. (2020, September 11). U.S. Company Faces Backlash After Belarus Uses Its Tech to Block Internet. Retrieved December 02, 2020.
32. Slavius [@slavius]. (2020, August 09). В Беларуси блокируют большое количество интернет-сервисов [Blog post]. Habr. Retrieved December 02, 2020.
33. МотолькоПомоги [@motolkohelp]. (2020, August 14). Нужного пока не нашли, но давайте «поблагодарим» наших китайских братьев за помощь Лукашенко в блокировке интернета в Беларуси 9-13 августа. [Image attached]. [Blog post]. Telegram. Retrieved December 02, 2020.
34. Dudarova, F. (2020, August 11). Белорусско-китайский файрвол: IT-специалист Михаил Климарев объясняет, как Лукашенко отключает интернет во время протестов. Retrieved December 02, 2020.
35. Policy Traffic Switch: Overview. (n.d.). Retrieved December 02, 2020.
36. Information sovereignty of Belarus: Old new truncheon or cooperation tool. (2020, April 20). Retrieved December 02, 2020.
37. Litvinova, D. (2020, August 21). 'Telegram revolution': App helps drive Belarus protests. Retrieved December 02, 2020.
38. State resources under attack. (2020, August 09). Retrieved December 02, 2020.
39. Restoring the Internet. (2020, August 12). Retrieved December 02, 2020.
40. To the attention of Beltelecom subscribers. (2020, August 10). Retrieved December 02, 2020.
41. Distributed denial-of-service
42. Belta news. (2020, August 10). Lukashenko blames poor Internet service in Belarus on foreign parties. Retrieved December 02, 2020.
43. Operations and Analysis Center under the President of the Republic of Belarus, a state security agency in charge of classified information and state secrets.
44. Psiphon Data Engine. (n.d.). Retrieved December 02, 2020.
45. Durov, P. [@durov]. (2020, August 10). We enabled our anti-censorship tools in Belarus so that Telegram remained available for most users there. However, the connection [Tweet]. Twitter. Retrieved December 02, 2020.
46. Tass news. (2020, August 12). Ex-PM Medvedev: US trying to use Internet as its fiefdom. Retrieved December 02, 2020.
47. Russian propaganda in Belarus: Delivery vehicles. (2020, June 12). Retrieved December 02, 2020.
48. Covid-political information from the Kremlin: New mutations of the propaganda virus. (2020, April 23). Retrieved December 02, 2020.
49. Ministry of Digital Development of Russia. (2019, February 29). On changes in the procedure for using foreign satellite communication networks in Russia. Retrieved December 02, 2020, .
50. Kolomychenko, M. (2018, October 24). Exclusive: Russia opposes U.S. OneWeb satellite service, cites security concerns. Retrieved December 02, 2020.
51. Tsydenova, N. (2019, December 19). Russia plans 'sovereign internet' tests to combat external threats. Retrieved December 02, 2020.

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org