How Azerbaijan’s government combines technology and fear to control the internet

Internet shutdown during 2020 Nagorno-Karabakh war as part of the government’s strategy to silence dissent
EXECUTIVE SUMMARY 3
OVERVIEW AND METHODOLOGY 5
BACKGROUND: THE ICT MARKET IN AZERBAIJAN 7
  Control over the ICT infrastructure - key players 7
  The rest of the ICT market is also dominated by state-owned companies. 8
  The market 9
INTERNET SHUTDOWN DURING THE 2020 WAR IN NAGORNO-KARABAKH: CONTEXT AND IMPACT 14
  What is an internet shutdown? 15
  Legal basis for the 2020 internet shutdown 15
  The lack of alternative solutions for internet access and anti-VPN campaign during the 2020 shutdown 17
  The responsibility of providers during the 2020 shutdown 18
  The wider impact and costs of the 2020 shutdown 19
  ICT market 22
  Advertising market 23
  E-commerce 23
  Indirect costs/impact 23
PATTERN OF INTERNET CENSORSHIP, SURVEILLANCE AND ATTACKS ON CIVIL SOCIETY 25
  Restrictions on internet access 25
  Digital surveillance 26
  DDoS and hacker attacks 32
  Trolling 35
  Conclusions 37
RECOMMENDATIONS 39
EXECUTIVE SUMMARY

On 27 September 2020, Azerbaijan’s Ministry of Transport, Communication and High Technologies (MTCHT) announced that internet access would be limited across the country to prevent ‘Armenian provocation’.1 This announcement came the same day as the armed forces of Azerbaijan and Armenia began clashing in the contested region of Nagorno-Karabakh, in relation to which martial law was declared in Azerbaijan.2

The MTCHT did not provide any further information on the nature or duration of the announced internet restrictions. However, as the military operations in Nagorno-Karabakh continued during the next 44 days, residents of Azerbaijan were unable to access social media platforms, communication and video conferencing apps and other online resources. Internet users from across the country also reported difficulties with downloading Virtual Private Networks (VPNs) -- tools used to get around the blocking of online resources. As a result, they could not use VPNs to access neither the platforms that now had become unavailable nor sites already previously blocked in the country, such as popular independent and opposition news sites. Throughout the 44-day war, the MTCHT failed to provide any public update on the internet restrictions, the online resources to which access had been limited, and the grounds on which these resources had been selected. The ministry also did not explain why the government restricted access to entire platforms rather than imposing more limited measures targeting certain online content. Finally, on 11 November 2020, the day after a ceasefire agreement had entered into force in Nagorno-Karabakh, the MTCHT announced that it was lifting the internet restrictions as of 12 November.3

---

2 Martial law was lifted on 11 December 2020.
Thus, this announcement ended the longest internet disruption that Azerbaijan has experienced to date (46 days).4

This report highlights the profound negative impact of the prolonged internet shutdown in Azerbaijan. The fact that access to key online resources were throttled for 46 days deprived residents of the opportunity to use such resources for their everyday communication and activities, including for purposes related to their work and studies. The devastating impact of the shutdown is illustrated by the economic costs associated with it. The report’s authors estimate that Azerbaijan’s economy suffered a USD 243 million loss, including both direct and indirect costs as a result of the shutdown. Our research also shows how plunging the country into digital darkness fits into a broader government strategy of using state-of-the-art digital surveillance technology, repressive legislation and harassment to silence dissent. The report exposes how US, Canadian, Swedish, Italian and Israeli tech companies have helped Azerbaijan’s government to consolidate control over the access, quality and diversity of the internet to an unprecedented degree - violating citizens’ rights to freedom of expression, privacy, and other fundamental rights.

The report’s authors found significant evidence to suggest that Azerbaijan’s government has used sophisticated surveillance technology purchased from foreign companies to spy on civil society representatives since 2009. The technology used for this purpose includes telecommunications surveillance monitoring centres supplied by the US-based Verint company, a Remote Control System (RCS) purchased from the Italian Hacking Team company, Deep Packet Inspection (DPI) technology purchased from the Israeli firm Allot Communications and the Canada-based Sandvine (through the national Bakcell mobile operator in the second case), as well as black boxes installed by the national Azercell mobile company when Swedish telecoms giant TeliaSonera owned a large stake in this company.

The report also highlights how SMS interceptions are common to date, exposing the involvement of mobile companies in attacks targeting journalists, activists and rights defenders.

Distributed denial-of-service (DDoS) attacks have been used frequently against websites reporting critically on the government. Many of these websites have also been rendered inaccessible for long periods or completely blocked – often without any court decision – since 2017.

The ruling party and government institutions have employed trolling networks to attack outspoken critics and independent and opposition media on social networking sites. Pro-government trolls typically leave hundreds of comments under posts for the purpose of derailing the discussion and intimidating dissidents. Trolls and pro-government accounts have also abused mechanisms for reporting violations of community rules and copyright infringements on social media platforms to block access to content critical of the authorities.

Azerbaijan’s government is implementing its digital crackdown on dissent in an environment in which the country’s information and communications technology (ICT) infrastructure is monopolized by allies of the regime, with a lack of competition leading to poor quality and prohibitively high prices for consumers. Although the country’s official internet penetration rate is 80 percent, underinvestment in infrastructure has led to huge disparities in access and speed across the country. These factors have contributed to problems with access to online education resources experienced in particular by students living outside the capital and other larger cities during the COVID-19 pandemic. These problems were further aggravated during the 46-day internet shutdown, when many students were unable to access the Teams application used by the Ministry of Education for online classes.

The MTCHT remains the main internet regulator in the country, although the country’s Strategic Road Map for Telecommunications and Information Technologies for 2016-2020 called for the establishment of an independent regulatory body. Thus, there is currently a lack of independent oversight of the ICT sector. At the same time, national legislation requires telecommunications operators and providers to cooperate with law enforcement authorities on the implementation of surveillance schemes, in particular by installing special equipment that grants officials access to confidential information about their customers, in violation of international data protection standards.

---

OVERVIEW AND METHODOLOGY

This report examines the country-wide internet shutdown that was enforced in Azerbaijan during the renewed hostilities in Nagorno-Karabakh in autumn 2020. While much of the previous and on-going reporting related to these hostilities focuses on the social, political and economic costs of the war between Armenia and Azerbaijan, little research has been done about the internet blackout that Azerbaijan was plunged into during the war.

In order to fully understand the recent shutdown and its human rights implications, a holistic overview of internet freedoms in Azerbaijan is needed. This report, therefore, offers an overview of the existing internet landscape in Azerbaijan, where the use of authoritarian technology and information controls has reached an unprecedented level in recent years. Despite the adoption of government plans and programs aimed at promoting internet development and freedoms, the government continues to fully control the internet landscape, including internet infrastructure, access, and service quality in an environment marred by human rights violations and the state-of-the-art surveillance technology utilized to silence dissent.

The first chapter of this report sets out the background for the following chapters by taking a closer look at the ICT market in Azerbaijan. It looks at how a centralized mechanism of control impacts internet service providers (ISPs) and end users, who are often left with no agency to demand transparency and better-quality services on their behalf. It further explores the legal landscape and corporate accountability of mobile companies and internet providers who are forced to implement government-imposed limits as a result of a deeply opaque system of legal norms and regulations.

The second chapter examines the context and impact of the recent internet shutdown that Azerbaijan experienced during the 2020 war in Nagorno-Karabakh. It highlights how the shutdown was imposed without a clear legal basis and in violation of international standards on the right to freedom of expression. It assesses the significant economic costs of the extended shutdown and discusses its impact on online education opportu-
This chapter also discusses the responsibility of providers and the failure to provide compensation or alternative solutions to internet users who were left without access to key internet resources for a prolonged period of time.

The third chapter shows how the recent shutdown fits into the longer-term pattern of online information controls deployed in Azerbaijan. The chapter offers an overview of how specific technology software has been used since at least 2009 for surveillance purposes and for preventing access to information, social media and popular communication platforms. Combined with less sophisticated methods such as hacking and online harassment, the authorities have used this technology to silence critics, alternative views and opinions.

This report relies on both quantitative and qualitative data. It summarizes research findings by independent experts, as collected and analyzed by the author. It draws on existing legal and international documents, articles and reports, as well as evidence collected by forensic teams at Qurium Media Foundation/Virtual Road, measurements made by the Open Observatory of Network Interference (OONI), and interviews with internet service providers, mobile operators, and experts. When relevant, statistical data and information from the Azerbaijani State Statistical Committee and the MTCHT have been used. In addition, the report draws on investigations carried out by the Organized Crime Corruption Reporting Project (OCCRP); reports published by Freedom House, Human Rights Watch, Reporters Without Borders, the Committee to Protect Journalists, and Azerbaijan Internet Watch; leaked email archives (in the case of the Hacking Team); and reporting by journalists working at national and international media platforms.

We assessed the economic costs of the internet shutdown implemented during the 44-day war in Nagorno-Karabakh based on national and international data sets. We used international formulas for calculating the costs of internet shutdowns (from the Cost of Internet Shutdown tool, Brookings Institute, Global Network Initiative, Access Now, and Deloitte), combined with an analysis undertaken by an independent economist from Azerbaijan.

Finally, the infographics in this report were developed by Mikroskop Media, an independent Azerbaijan-covering news platform based in exile. The data used in the infographics is based on publicly available information and interviews with ISPs and mobile companies operating in Azerbaijan.
BACKGROUND:

THE ICT MARKET IN AZERBAIJAN

Control over the ICT infrastructure - key players

Azerbaijan views the ICT industry as its road to economic diversification and growth. In 2016, the ICT was one of 11 economic sectors identified to be of strategic importance in the country and a strategic roadmap for the development of this sector was adopted.\(^5\) However, the government’s ambitious plan to turn the country into an information communications technology hub for the Caucasus has so far failed.

One of the three key strategic targets outlined in the roadmap from 2016 was to improve governance structures and strengthen the ICT. The priorities under this strategic target were to create an independent regulatory body, liberalize the telecommunications market and increase investment in mobile infrastructure. However, although the period of implementation of this strategic road map expired in 2020, no independent regulatory body has been established. The sole agency responsible for both ICT policy and regulation is the MTCHT. The dominant role of the MTCHT has often been criticized by local experts, who have been calling for decentralization and demonopolization in the ICT sector for years.

Overall, Azerbaijan’s ICT infrastructure is poor and highly monopolized, and the sector’s value of the country’s gross domestic product (GDP) remains low: in 2020, it made up a mere 1.6 percent of the total GDP.

The international connectivity of the broadband network is in need of an upgrade and expansion. Limited competition for fixed broadband infrastructure has led to complacency and slow internet speeds.

Due to the underdeveloped infrastructure, there are also widespread disparities in internet access and quality, although the country’s overall internet penetration rate is 80 percent. According to the Network Readiness Index 2020 report, Azerbaijan’s weakest indicator is the rural/urban divide. Specifically there is a gap in fixed household internet penetration between rural and urban households and across regions of the country due to shortages of fixed infrastructure and lower levels of digital literacy in rural areas. The country’s 4G LTE coverage is mostly available in urban areas.

Two companies have been licensed to provide access to international internet traffic: Delta Telecom and AzerTelekom. Delta Telecom is state-owned, while AzerTelekom is controlled by the state-run Azerfon mobile company. Thus, these two backbone internet providers have monopoly on the provision of international internet access and sell such services to other national ISPs. A 2016 working paper published by the Economic and Social Commission for Asia and the Pacific (ESCAP) emphasizes that: “A monopoly on an international gateway may lead to a loss in quality of service for the end user” especially because “an incumbent operator has by default less incentive to improve its services and keep up with latest technologies due to lack of competition”.

In particular, Delta Telecom, the country’s leading backbone provider which controls the market in the capital, has been widely criticized for selling slow, costly internet services to national ISPs. In a statement issued in 2017, Delta Telecom claimed that the reason for the slow and unreliable internet services was that national ISPs “were not paying their bills”. It claimed that ISP companies had accumulated a 1.8 million USD debt to the government provider.

The rest of the ICT market is also dominated by state-owned companies.

According to a 2019 report from the Asian Development Bank, state-owned companies ultimately control about 50 percent of the national ICT market, while the rest of the country is served by private ISPs. However, taking into consideration that many of the ISPs that are privately owned have ties to people in power, there is even less competition in practice. For example, Aztelekom, one of the country’s two fixed line operators that control all last-mile access to homes, is owned by the family of President Ilham Aliyev. The second one, Baktelecom, is a state-owned company.

The current state dominance of the ICT market in Azerbaijan thwarts open competition and the development of better and faster internet services.

---

The lack of legislation holding providers accountable to users\textsuperscript{16}, as well as independent oversight of their work further aggravate this problem.

### The market

According to the MTCHT’s website, there are 48 ISPs and three mobile phone operators that offer internet access in Azerbaijan. As discussed above, two of the ISPs, Delta Telecom and AzerTelekom provide international traffic, which they also sell to other ISPs. Fourteen of the ISPs are no longer active. The three mobile companies that provide internet access are Azercell, Bakcell and Azerfon/Nar Mobile.

The picture on the left breaks down IP ownership in Azerbaijan. With the two state-owned backbone providers, the rest of the market is shared by 48 regular ISPs and three mobile phone operators.

The average monthly cost of internet packages offered by ISPs varies from 15-18AZN (8.8-10.5USD) to as much as 80 AZN (47 USD), depending on the type of internet connection offered and its speed. Internet services are quite expensive in relation to the monthly average income.

According to the 2020 Inclusive Internet Index, the monthly cost of a fixed internet connection in Azerbaijan is 2 percent of the gross national income (GNI) per capita, while the cost of a mobile data plan offering 1 GB per month is 1 percent of the GNI per capita, leaving Azerbaijan behind countries like Ukraine, Turkey and Russia.\textsuperscript{17}

The state dominance of the ICT sector, which was discussed above, has made it easy for the authorities to control internet traffic as well as to block content online in the absence of effective accountability measures. At the same time, a series of legal acts grant government institutions such as the state security services powers to snoop around internet users.

The practice of arbitrary, government-imposed restrictions on internet access began as early as 2003, when the government requested ISPs to cut access to all Chechen websites, according to a report published by Reporters Without Borders in 2004.\textsuperscript{18} The same year, an official from the Ministry of Communications and High Technologies\textsuperscript{19} said that this ministry “had the right to ask ISPs to block sites containing material ‘contrary to the mentality, traditions, and customs’ of the country.” In 2006, authorities blocked access

---


\textsuperscript{19} In 2017, this ministry was merged with the Ministry of Transportation.

The state control over ISPs and mobile operators is established by the Law on Telecommunications (hereafter “Telecoms Law”)\(^2\), laws related to the activities of law enforcement agencies, presidential decrees, as well as decisions by the Cabinet of Ministers and the MTCHT.

According to the Telecoms Law, state policies in the area of telecommunications is aimed at protecting the equality and legitimate interests of operators, providers, and users; preventing unacceptable monopolies in the telecommunications service market; and ensuring a healthy competitive environment characterized by transparency and openness in decision-making. The Telecoms Law also sets out as a basic principle the separation of state regulatory functions from telecommunications. However, contrary to this basic principle, the law grants the government broad powers with respect to the licensing, registration, and certification of telecommunication activities; the application of tariffs for the use of telecommunication services and radiofrequencies; and the regulation of competition, antimonopoly activity and other aspects of telecommunications.\(^2\)

Currently three categories of telecommunications activities require state authorization through - licensing, registration, and certification. The licensing and registration processes in place are restrictive and non-transparent.

Licenses are issued in accordance with the 2016 Law on Licenses and Permits.\(^2\) Annex 1 to the law lists activities requiring a license in all cases except for those involving issues of state security, while Annex 2 lists activities requiring a license in those cases.

---

27 The Law on Telecommunications specifies the telecommunication services as phone (wired); cellular (mobile); paging; radio trunk and wireless phone; domestic and international telecommunication; Internet service; TV and radio broadcast services; universal telecommunication services; and other telecommunication services set by legislation.
28 The organisation of the use of radiofrequencies; regulation of interconnection among operators; keeping records of operators and providers of internet telecommunication services; organizing the use of number resource; and other priorities for regulation set out by the legislation of the Republic of Azerbaijan (as per article 6 of the Telecommunications Law).

---

The process in which ISPs and mobile operators implement government orders to block specific websites is non-transparent as it is not officially regulated and the companies concerned do not disclose any information about how they handle such orders. The nature of government orders is also problematic, as government institutions fail to disclose any relevant information ahead of time or during the requests to public as well as website owners. In addition, their corporate accountability with respect to the blocking of websites is unclear.

The state control over ISPs and mobile operators is established by the Law to the tinsohbeti.com website\(^1\), a satirical blog posting cartoons making fun of the president. In 2007, a similar measure was imposed against susmayaq.biz\(^2\) because this site had petitioned the authorities to reduce energy prices. The following year, internet users were prevented from accessing shiraslan.info, a website about the presidential election candidacy of an invented “man of the people.”\(^3\) According to a 2008 State Department cable obtained by Wikileaks, Delta Telecom was serving “as an informal mechanism for shutting down select internet sites.”\(^4\) Blocking was not the only measure in place, arrests of people affiliated with online platforms critical of the government were already common at the time. When the author of the pur.gen.az website posted a caricature of the president, the man was arrested.\(^5\) Seventeen years since the first blocking measure, the authorities have effectively blocked access to at least nine online news resources reflecting independent and opposition views.\(^6\) They have also blocked access to social media and communication app platforms in recent years.


---

27 The Law on Telecommunications specifies the telecommunication services as phone (wired); cellular (mobile); paging; radio trunk and wireless phone; domestic and international telecommunication; Internet service; TV and radio broadcast services; universal telecommunication services; and other telecommunication services set by legislation.
28 The organisation of the use of radiofrequencies; regulation of interconnection among operators; keeping records of operators and providers of internet telecommunication services; organizing the use of number resource; and other priorities for regulation set out by the legislation of the Republic of Azerbaijan (as per article 6 of the Telecommunications Law).

---
The licensing process is also regulated by Resolution No. 174 on «additional conditions required for the issuance of special permits (licenses) depending on the nature of the activity», which was adopted by the Cabinet of Ministers on 7 November 2002. This resolution requires telecommunication companies to provide a range of documentation when applying for licenses, including, among others documents proving their right to use the facilities and equipment required for the organization of telecommunications services; information on the technical characteristics of the equipment to be used; and proof of their experience in the field of telecommunications. Applicants are also required to provide a written affirmation of their readiness to install special equipment needed for law enforcement authorities to obtain information from telecommunications networks for reasons of national security. The license fee depends on the nature of the telecommunications services provided.30

According to Resolution No. 427 on the “Rules of registration of operators and providers of Internet telecommunication services”, which was approved by the Cabinet of Ministers on 12 October 2017, operators and providers are required to apply to the MTCHT for registration within 15 days from the start of service.31

These rules also require ISPs to present a guarantee that they will install special equipment needed to access information during search operations conducted by authorities.32 The rules further require operators and providers to submit to the registration authority (MTCHT) copies of the agreements concluded with the first subscribers to their services.33

The State Security Service and the Ministry of Internal Affairs are authorized to carry out search operations targeting communications networks in accordance with a set of rules approved by Presidential Decree No. 638 from 2 October 2015.34 This decree indicates that the rules as such have not been made public. Azerbaijan’s Constitutional Law on Normative Legal Acts requires that laws and presidential decrees officially be published within 72 hours after being signed by the president.35 However, exception is made for normative legal acts that contain provisions concerning state secrets.36 Thus, the relevant rules can be assumed to have been classified.

The MTCHT may reject the registration of operators and providers if the application submitted for registration is not completed in full; if it contains incorrect or distorted information; or if information is missing. The MTCHT may also reject the application if the technical and organizational capacity of the service providers is considered insufficient, and it will not be possible for security and law enforcement authorities to carry out search operations using special equipment to access information on the telecommunications networks of the providers. The technical and organizational capabilities of the service providers, as documented in the application, are reviewed by the ministry with the participation of other relevant agencies. However, domestic legislation does not specify the review procedures or set out any concrete requirements for the technical and organizational capacities of service providers.

In accordance with the Telecoms Law and the government resolution on the conditions of telecom licensing and registration mentioned above, telecom operators and providers must cooperate with the law enforcement authorities and install equipment and software programmes enabling these authorities to access information when needed for law enforcement purposes.37

---

30 Telephone (wired) - 2 500 AZN; radiotrunk and wireless telephone - 2 500 AZN; IP telephony (Internet telephony) - 50 000 AZN; organization of national telecommunication channels- 2 500 AZN; organization of international telecommunication channels- 5 500 AZN; data transmission (Data) - 3 000 AZN; high-speed postal services - 1 250 AZN; creation of biometric technologies and rendering them services-1100 AZN; formation of personal data backups and creation of information systems, rendering them services-1100 AZN; cellular (mobile) communication services (indicating technological standard ) - 1 000 000 AZN.
31 The Rules of registration of operators and providers of Internet telecommunication services Available (in Azerbaijani) at: http://e-qanun.az/framework/36773
32 On this point, the rules refer to Presidential Decree No. 507 on “the division of power of search operations in the implementation of search operations”, dated 19 June 2001, which is available (in Azerbaijani) at: http://e-qanun.az/framework/3569
33 Article 3.3.3 of the Rule of registration of operators and providers of Internet telecommunication services.
34 http://e-qanun.az/framework/30840
36 Article 82.7 of the Constitutional Law (№ 21-IVKQ) “On normative legal acts”
37 The Telecoms Law, article 39, Paragraph 1 of the article states: “operators, providers are obliged to create conditions for conducting search operations, intelligence and counter-intelligence activities in accordance with the law; to provide telecommunications networks with additional technical means in accordance with the conditions established by the relevant executive authority; to resolve organizational issues; and to keep secret the methods used in conducting these events.” Paragraph 2 of the article states: «The operator, the provider shall be liable for the violation of these requirements in accordance with the law.»
According to national law, and international conventions ratified by Azerbaijan, online surveillance should be sanctioned by court in each case. However, the general requirement for telecom operators and providers to install surveillance equipment grants law enforcement authorities wide discretion to access information through telecommunications networks without a court order.

New legislation adopted since 2017 has created additional obligations for ISPs. These include mandatory registration of ISPs and new requirements to comply with government requests concerning information inquires, surveillance, blocking of online resources and the suspension or termination of the provision of services.

On 28 October 2016, parliament passed amendments to the Telecoms Law for the stated purpose of bringing it in line with the Law on Combating Religious Extremism adopted on 4 December 2015. According to the new article 40.4-1 of the Telecoms Law, the provision of communications services to both individuals and legal entities may be suspended in regions where special operations against religious extremism are implemented at the instruction of the body conducting such operations. Amendments to the article 40.5 of the Telecoms Law relieves operators and providers of the obligation to inform their clients in the event that telecommunications services are restricted or suspended due to emergency situations, special operations against religious extremism, or natural disasters.

Human rights experts consider that article 39 of the Telecoms Law, which gives the executive branch wide discretion to implement regulatory measures without judicial control, creates conditions for serious human rights violations.

While tightening data-sharing obligations for providers and operators, the government also abolished pre-existing obligations for registered operators and providers with respect to the protection of personal data of clients.

Further, on 14 June 2016, the MTCHT issued new rules concerning the special technical means that operators and providers are required to install on their networks to facilitate search operations and intelligence and counter-intelligence measures by law enforcement authorities. These rules use the term Telecommunications Control System (hereinafter «TCS») to refer to special hardware and software that provide confidential control over the exchange of information among those targeted by relevant law enforcement measures, and over statistical information related to network use. TCS consists of data extraction facilities, transport network, and control centres. The June 2016 rules (article 1.5) state that details on the installation of TCS by telecommunications operators and providers will be provided separately by the State Security Service (SSS), the Ministry of Internal Affairs (MIA) and the Special State Protection Service (SSPS). The rules further state that the costs related to the installation, maintenance and implementation of TCS equipment will be borne by telecommunications operators and providers themselves.

According to part 3 of these rules, telecommunications operators and providers must install TCSs in a timely manner and hand over the equipment to SSS and SSPS, respectively, for operational use, even if retaining it on their balance sheets. The relevant authorities are not required to inform telecommunication operators and providers about operational search, intelligence and counter-intelligence activities carried out through their networks nor about the data obtained through such measures.

Pursuant to article 445 of the Criminal Procedure Code, surveillance operations such as the interception of telephone conversations; monitoring of mail, telegraph, and other correspondence; and extraction of information from technical communication channels and other technical devices are carried out only by court decision. However, in contradiction of this provision,

38 Article 445 of the Criminal Procedure Code of the Republic of Azerbaijan and Article 10 of the Law on Operation-Search Activity
39 Law No. 27-VQ
41 By the Decision of the Cabinet of Ministers of the Republic of Azerbaijan No. 191 dated 30 April, 2018, Part 6 of the “Rules for registration operators and providers of Internet telecommunications services” the provision imposing obligations on operators and providers regarding the protection of personal data has been repealed.
42 «Rules of providing of communication networks with additional technical means by telecommunication operators and providers for carrying out search operations, intelligence and counter-intelligence actions”, available (in Azerbaijani) at: http://e-qanun.az/framework/33275
43 Wiretapping of telephone conversations ad extraction of information from technical communication channels and other technical means are carried out by the Ministry of Internal Affairs and the State Security Service in accordance with Presidential Decree No. 507 dated 19 June 2001 “On the division of powers among entities of operative-searching activity in the implementation of investigation and search operations” available (in Azerbaijani) http://e-qanun.az/framework/3569
article 10, paragraph 4 of the Law on Operation-search Activity states that these types of operations may be carried out without a court decision, on the basis of a reasoned decision by an authorized official of the body carrying out the search operation when necessary to prevent serious crimes.\(^4\) In practice, most investigative activities carried out on the basis of a reasoned decision of an authorized official have been left without judicial oversight.\(^5\) Government surveillance through the interception of communication is jeopardizing privacy and security and violates international human rights law.\(^6\)

\(^4\) In this case, the authorized official of the body conducting the search operation shall, within 48 hours of carrying out the search, provide a reasoned decision on the conduct of the search operation to the court exercising judicial supervision and to the prosecutor.


\(^6\) The UN General Assembly has condemned unlawful or arbitrary surveillance and interception of communications as "highly intrusive acts" that interfere with fundamental human rights (see General Assembly resolutions 68/167 and 71/199).
INTERNET SHUTDOWN
DURING THE 2020 WAR IN NAGORNO-KARABAKH: CONTEXT AND IMPACT

On 27 September 2020, the unresolved conflict over the contested region on Nagorno-Karabakh escalated into new clashes between the armed forces of Azerbaijan and Armenia. The fighting continued for 44 days until a ceasefire agreement entered into force.

On the same day as the clashes began, the MTCHT published an announcement on its website, saying that internet access would be limited across Azerbaijan to prevent ‘Armenian provocation’. The ministry did not provide any further information on the nature or duration of these restrictions, leaving it unclear what resources would be affected and for how long. In practice, millions of internet users in the country were plunged into digital darkness as they found themselves unable to access major online resources, in particular social media and communication platforms such as Facebook, WhatsApp, Telegram, Zoom and others. In addition, as discussed in more detail below (see the section on ‘The lack of alternative solutions for internet access and anti-VPN campaign’), internet users across the country also had problems downloading VPNs -- tools used to get around blocking measures -- and, thus, could not use these to access inaccessible platforms or sites previously blocked in the country.

Finally, in a statement issued on 11 November 2020, the day after the ceasefire agreement entered into force in Nagorno-Karabakh, the MTCHT announced

that it was lifting the internet restrictions as of 12 November. However, even after this, residents continued to report difficulties with internet access and slow connectivity especially outside the capital Baku. In addition, several months later, the Open Observatory of Network Interference (OONI) found that several circumvention tool websites continued to “present signs of blocking” in Azerbaijan.

What is an internet shutdown?

According to the global #KeepItOn coalition, an internet shutdown is “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable for a specific population or within a location, often to exert control over the flow of information. An Internet shutdown happens when someone – usually a government – intentionally disrupts the internet or mobile apps to control what people say or do.”

According to the #KeepItOn campaign's 2020 report on internet shutdowns, at least 155 internet shutdown incidents were documented globally in 2020. “For a world that was and continues to be under lockdown or at least some forms of movement restrictions, 155 intentional communication disruptions came at a high cost to the fundamental human rights of people around the world.” For the first time, Azerbaijan was included on the list of countries where significant internet disruptions were registered.

Legal basis for the 2020 internet shutdown

Under national law, the requirements for restricting the use of communications during emergencies and situations when martial law has been declared are set out in the Telecoms Law, the Law on Emergency Situations, and the Law on Martial Law, as well as the Special Rules for the Use of Communications in State Emergency Situations and the Special Rules for the Use of Communications during Martial Law, which have been adopted by the Cabinet of Ministers.

According to article 1.4 of the Special Rules for the Use of Communications during Martial Law, measures aimed at restricting the rights and legitimate interests of telecommunications and postal operators, internet providers, TV and radio broadcasters, as well as of the subscribers and users of such services will be implemented in accordance with the constitution and laws of the Republic of Azerbaijan. The rules oblige telecommunications operators to give priority to ensuring that telecommunications channels can be used for the needs of military bodies during martial law. During martial law, military authorities, have the right to use telecommunications networks, facilities and entities, as well as postal, television and radio broadcasting entities, regardless of the ownership and organizational-legal form of such entities.

Acting in coordination with military authorities, the MTCHT may restrict the access of individuals and legal entities to telecommunications networks in territories where martial law is applied. In coordination with military authorities, the MTCHT may also temporarily suspend telephone and internet services for the purpose of meeting the needs of military authorities. The period of restrictions may not exceed the period of martial law.

52 http://www.e-qanun.az/framework/10663
53 http://www.e-qanun.az/framework/6193
54 http://e-qanun.az/framework/35170
55 15 February 2012. № 37) http://e-qanun.az/framework/23121
56 30 November 2018. № 517) http://e-qanun.az/framework/40871
57 Article 2.1.9 of the Special Rules for the Use of Communication during the State of Martial Law
58 Article 3.5 of the Special Rules for the Use of Communication during the State of Martial Law
59 3.10 of the Special Rules for the Use of Communication during the State of Martial Law
On 27 September 2020, Azerbaijan’s president signed a decree declaring martial law in the entire territory of Azerbaijan, starting at midnight (00:00) on 28 September 2020. The decree was sent to parliament (milli meclis) the same day, and this body immediately approved it. The following day, on 28 September 2020, the UN General Secretary was informed about the introduction of martial law in Azerbaijan. Martial law remained in force in the country until being lifted on 11 December 2020.

According to paragraph 2 of the presidential decree, the state of martial law was to be implemented through measures provided for in the Law on Martial Law. The decree did not mention any specific restrictive measures, except for curfew measures.

It should be noted that the Law on Martial Law does not specifically empower the government to shut down or restrict the use of the internet, although it allows for restrictions or suspensions of the activities of mass media, which are considered to include online information resources under the Law on Mass Media (article 3).

The MTCHT announced the internet restrictions on the same day as the decree on the imposition of martial law was adopted, but before this decree entered into force. Neither when first announcing the internet restrictions nor during the remainder of the 46-day internet shutdown did the MTCHT specify the services and resources to which the restrictions applied. Thus, internet users only learned the extent of the internet throttling as they navigated it in practice.

In accordance with international human rights law, the right to freedom of expression might be restricted in exceptional circumstances for the purpose of protecting national security. However, any restrictions must be compatible with the requirements for permissible limitations on this right set out by international treaties, in particular the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR).

According to the United Nations Human Rights Committee, any restrictions on the right to freedom of expression must be provided for by a law that is formulated with sufficient precision to enable people to know what conduct is prohibited, and the restrictions must be strictly necessary and proportionate to their objective, with the least intrusive instrument being chosen in all circumstances. The Committee has stressed that any restrictions on internet resources must meet these same basic requirements. The Committee has stated that permissible restrictions on online resources, as a rule, should be content-specific, while generic bans on the operation of certain websites and systems are not compatible with article 19 of the ICCPR, which safeguards the right to freedom of expression. The Committee has also made it clear that it is inconsistent with this article to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.

In a similar vein, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression considers fully cutting off users from internet access, regardless of the justification provided, a violation of Article 19 of the ICCPR. He has called on states to ensure that internet access is maintained at all times, including during times of political unrest. He has also called on states to provide full details regarding the necessity and justification for any measure to block individual websites, stressing that decisions to block content must be undertaken by a competent judicial authority or other independent body.

The European Court of Human Rights (ECtHR) has emphasized that the internet has become a principal means of exercising the right to freedom of expression and that any restrictions on internet access must be assessed in the light of this fact. According to the Court, restrictions on access to online sources of information are only compatible with the ECHR if a strict legal framework is in place regulating the scope of the ban and affording the guarantee of judicial review to prevent possible abuses. The Court has found impermissible the imposition of restrictions that render large amounts of

---

60 Presidential order on martial law (available in Azerbaijani) at: https://president.az/articles/40979

61 Parliament's law on martial law (available in Azerbaijani) at: https://meclis.gov.az/documents/165-VIQR.pdf


63 UN Human Rights Committee, General comment No. 34 (Article 19: Freedoms of opinion and expression), https://www2.ohchr.org/english/bodies/hrcdocs/gc34.pdf

information inaccessible for internet users, without ascertaining whether a less far-reaching measure could have been taken.  

The 46-day internet restrictions in Azerbaijan were imposed for the apparent purpose of protecting national security, which is a permissible ground for limiting the right to freedom of expression under international human rights law. However, the restrictions did not meet the requirements of legality, necessity and proportionality established by the ICCPR and the ECHR. There was an unclear legal basis for the restrictions, which were introduced before martial law had taken effect in the country, and the MTChT announcement about the restrictions failed to specify the extent and duration of them. Moreover, while internet users experienced far-reaching restrictions on access to online resources in practice, the government did not even attempt to explain why these measures were needed to achieve the stated objective of preventing ‘Armenian provocation’ and why more limited content-specific measures were not sufficient. There was no court review of the restrictions, which had a significant impact on the enjoyment of freedom of expression online during an extended period of time and which, at least partly, continued even after the state of martial law was lifted.

National legal experts have criticised the extensive internet restrictions imposed in the context of the 44-day war in Nagorno-Karabakh. For example, at the time of the active military operations, media law expert Alasgar Mammadli said in an interview that the authorities should have focused on restricting certain online content rather than shutting down the entire internet. He argued that the Law on Martial Law primarily is about content control of information detrimental to national security and territorial integrity.

65 Ahmet Yıldırım v. Turkey, 18 December 2012. See more in European Court of Human Rights Factsheet on access to Internet and freedom to receive and impart information and ideas, March 2021, at https://www.echr.coe.int/Documents/FS_Access_Internet_ENG.pdf


The lack of alternative solutions for internet access and anti-VPN campaign during the 2020 shutdown

During the country-wide internet shutdown seen during the 44-day war in Nagorno-Karabakh in autumn 2020, no internet service providers or mobile operators offered alternative internet access to their users. At the same time, many government institutions, including the office of President Ilham Aliyev shared up-to-date news on their social media accounts. The president’s wife, First Vice President Mehriban Aliyeva used her Instagram account to encourage Azerbaijani to actively engage in an “information war” on social media.

International experts on internet shutdowns have pointed out that it is possible for government networks to continue to have access to the internet while implementing broader internet restrictions through a variety of mechanisms in place. Such mechanisms range from leaving wireline broadband connections in operation in order to serve government offices and banks, or having an entirely separate network for government offices and affiliates. Most likely, at the time of country-wide internet disruptions in Azerbaijan in autumn 2020, the government implemented what is known as network segmentation filtering. When this occurs, the network is divided into smaller networks (subnets), which allows for “controlling the flow of traffic between subnets […] or even blocking the entire flow of traffic if necessary.” Given the control mechanisms in place in Azerbaijan, the government-run infrastructure (proxy, filterware or Deep Packet Inspection devices, of which Azerbaijan has plenty, see the next chapter) can easily filter and throttle internet traffic based on the source and destination addresses at any granularity from Autonomous System Numbers (ASN), subnet or IP address. The same filtering mechanism can be applied to voice calls by source or destination phone number, with granularity by area code, provider number pool, or even by individual phone numbers.

Many private internet users resorted to VPNs in an attempt to access Facebook, WhatsApp, Telegram and other social media and communication application platforms that were blocked during the 44-day war. However, at the same time, internet users from across the country reported difficulties with downloading VPN services on their devices and, thus, with using such tools to access unavailable

social media and communication platforms, as well as websites that already previously had been blocked in the country. As discussed further in the following chapter, since 2017, the Azerbaijani government has blocked access to a number of popular independent and opposition news sites, including Meydan TV; the Azerbaijani service of Radio Free Europe/Radio Liberty (RFE/RL), Azadiq Radio; the Azadiq newspaper and others. Readers typically use VPNs to bypass censorship and access these sites. However, because of the problems with VPN services during the 44-day war, this became largely impossible.

The problems with VPN use reported during the 44-day war suggests that the government was attempting to restrict the use of such services. Both authorities and pro-government media platforms publicly discouraged people from using VPN services, arguing that VPNs were unsafe and dangerous. For example, media argued that VPNs steal personal data and spread viruses, and one article published by a pro-government media outlet claimed that VPNs shared user data with Armenian intelligence agencies.\(^68\) It was also argued that VPN use is illegal and subject to fines, although national legislation does not prohibit the use of VPNs nor provide for liability on this ground.

On 20 October 2020, the Special State Security Service encouraged citizens to refrain from using VPN services to access social media platforms because of privacy concerns.\(^69\) However, the authorities did not officially announce that VPNs were blocked in the country during the 44-day war.

Despite the rumours and speculations about the alleged security risks associated with the use of VPNs, which were promoted by pro-government media and reinforced by government statements, Azerbaijan still ranked among the top countries where VPN services were in high demand between 27 September and 10 November 2020, i.e., during the period if the nation-wide internet shutdown.\(^70\)

The responsibility of providers during the 2020 shutdown

As part of our investigation of the impact of the 46-day internet shutdown in September-November 2020, we carried out a survey among ISPs in the country. We contacted 28 ISPs, out of which 14 responded to our inquiries.

We asked the surveyed ISPs whether they offered any compensation to their customers for the restrictions on internet services during the shutdown (which meant that customers paid for services they were not able to use). Most of the ISPs who responded said that they did not offer any discounted rates or other compensation to their clients. Their argument was that the shutdown was government imposed and therefore outside of their control, and some said that they did not implement any compensation schemes since the government did not offer any compensation to providers.

The surveyed ISPs offered similar responses with respect to problems their customers encountered with respect to VPN use. While many of them reported that their customers had informally complained about problems connecting to VPNs during the shutdown, they said that they had not offered any compensation to these customers. Providers also justified this decision by arguing that the restrictions were government-imposed. In addition, they argued that ISPs are not responsible for technical difficulties associated with the use of VPNs. For example, the Sazz provider said that the “talk of compensation is irrelevant” for these reasons. Some providers told their clients that VPN services were unavailable because such services are

---

illegal, although national law does not prohibit the use of VPNs, as discussed above. For example, the Enginet provider said that it had told its clients who complained about restrictions on VPN use that the company does not support VPNs because "it is not permitted".

Other companies informed their clients that their internet services (including both website and mobile applications) would not be accessible on devices where VPNs were in active use. Azerfon, which is believed to have ties to the ruling family, encouraged its customers to refrain from using VPNs with reference to the alleged risk of interception of passwords and other personal information of VPN users. Other operators and providers followed suit.

Legal experts whom the authors of this report consulted expressed different views with respect to the responsibility of ISPs to offer compensation to customers who experienced difficulties with accessing VPNs and other online resources during the 44-day war. Lawyer Fariz Namazli argued that it was up to the providers themselves to decide whether or not to offer any discounts to their clients since the country's Law on Martial Law sets out the precedence of state interests over the interests of internet users during a state of war and allows for censoring mass media and online news resources during such a period.

Other legal experts argued that ISPs should have had to offer at least some form of compensation to customers affected by the internet restrictions, stressing that the failure to do so resulted in violations of the rights of thousands of internet users. The chair of the organization Free Consumers Rights, Eyyub Huseynov said that providers currently operate on an "all for one, all for all" model in Azerbaijan where consumers are not part of the model. He said that most internet service agreements signed between companies and consumers are "one-sided" and highlighted the need for change in this area. One solution according to Huseynov would be for providers to offer free of charge services to customers in the months that follow situations such as the one seen during the 44-day war. However, at the time of writing of this report, no ISPs had made such offers to their customers.

Out of three national mobile operators, only one, namely Azercell responded to our inquiries. Like many of the other providers interviewed for the report, this operator said that it did not make any general announcement to its clients about the internet disruptions since these were not caused by the company but were government-imposed. The company only informed clients about the limitations in place in response to inquiries made by clients. The only compensation that Azercell offered to clients was the reactivation of internet bundles that clients had purchased but were unable to use during the 44-day war. A company representative explained that this was done when clients got in touch with the company.

The lack of compensation schemes by ISPs and mobile operators during the 44-day followed a similar pattern as that seen in the context of the COVID-19 pandemic. Even though many families suffered from financial difficulties due to the lockdown measures imposed in response to the pandemic, the companies retained their previous tariffs.

The wider impact and costs of the 2020 shutdown
Given the length of the internet shutdown seen during the war in Nagorno-Karabakh in autumn 2020 its impact was unprecedented. During the 46 days that the shutdown lasted, residents were unable to use social media and communication platforms for accessing and exchanging information, communicating with family members (including those living along the frontline or in cities under attack), friends and colleagues, and for other purposes related to their work, studies and spare time activities. The disruptions in internet access also affected businesses, especially small-to-medium enterprises (SMEs), resulting in lost contracts, and the loss of business, employment and income.

72 There are three separate articles that address access to media under martial law. According to these articles the following measures may be taken under martial law: military censorship of media information and materials; application of a special regime of mass media in the territory (territories) where martial law is applied, submission of proposals to the relevant bodies on restriction or suspension of their activity if there are legal grounds; regulation of the activity of mass media in the frontline zone. https://rm.coe.int/16809fbd3d
Against this background, measuring the economic costs of the shutdown will help us to assess and illustrate its wider broader impact on the population.

The economic costs of internet disruptions vary between countries, depending on the internet penetration rate and other factors. According to a Deloitte report on the economic impact of internet disruptions, “it is estimated that for a highly connected country, the per day impact of a temporary shutdown of the internet and all of its services would be on the average 23.6 million USD per 10 million population. With lower levels of Internet access, the average estimated GDP impacts amount to 6.6 million USD and to 0.6 million USD per 10 million population for medium and low internet connectivity economics respectively.”

Based on Deloitte’s internet ecosystem metrics, Azerbaijan would qualify as a highly connected country, with an internet penetration rate of over 80% within a population of around 10 million. However, the official internet performance indicators in Azerbaijan are misleading for the reasons discussed earlier in this report. Therefore, we used adjusted figures for the calculation of the costs of the 46-day shutdown and found that the overall costs corresponded to those of countries with a lower level of internet access in Deloitte’s scheme.

**Tracing the costs**

To calculate the costs of the 46-day internet disruptions that Azerbaijan experienced during the war in Nagorno-Karabakh in September-November 2020, we used the Cost of Shutdown Tool (CST). CST relies on several indicators and methodologies for the calculations. It should be noted that the final calculated amount is also an estimate.

According to the CST estimate, Azerbaijan’s economy suffered a 2 billion USD loss during the 46-day shutdown. The daily estimated loss totalled 44.5 million USD.

The CST also provides an option for calculating the costs of a partial internet shutdown, resulting from blocked, filtered or throttled services. We used this option to calculate the impact of the social media shutdown that was part of the broader 46-day shutdown.

---


75 According to the State Statistics Committee users accessing the internet via a tablet or smartphone from home, make up 70.7 percent of the total population. Only 18.7 percent and 26.2 percent access the internet via desktop or laptop respectively. In the meantime, only 0.9 percent of enterprises offer their services via websites and mobile apps. 51.5 percent of enterprises have access to the Internet. Companies with websites make up 9.8 percent.

76 [https://netblocks.org/cost/](https://netblocks.org/cost/)


The services that are built into the CST are Facebook, Twitter, YouTube, Instagram, and WhatsApp, all of which were blocked throughout the 46-day shutdown. Based on this calculation, the economic loss was 150 million USD in total, or 3.2 million USD daily.

However, neither of these calculations gives a fully accurate estimate of the total costs of the 46-day internet shutdown. Azerbaijan did not experience a total internet blackout (as assumed in the first calculation), but at the same time, the restrictions imposed were not limited to social media platforms (as assumed in the second calculation) but also affected other online services, e.g., Microsoft Teams, Zoom and Skype. Finally, the CST calculates the digital economy value at a set 16 percent. However, in the case of Azerbaijan, the added value of ICT is only 1.6 percent. For a more accurate calculation, we decided to account for the level of economic development and associated growth in Azerbaijan especially in the digital economy (see below). Our final calculations based on these factors and a readjustment of the formula in indicator for digital economy value (using 1.6 percent, instead of 16 percent) indicate that Azerbaijan suffered a total economic loss of 243 million USD (413 million AZN) during the 46-day shutdown.

### The CST

The CST relies on a combination of formulas and methodologies developed by the Brookings Institute and The Collaboration on International ICT Policy in East and Southern Africa (CIPESA). We narrowed down our calculations to the following two formulas developed by the Brookings Institute:

- **National Internet Shutdown Costs** = National GDP * Duration (measured as percent of the year based on number of days the Internet was shut down) * Extent of Digital Economy (measured by the percentage of that nation’s economy derived from the digital economy) + the multiplier effect of the disrupted digital economy

- **National Free App Shutdown Costs** = National GDP * Duration (measured as percent of the year based on number of days the Internet was shut down) * Free Digital App GDP Impact (measured by Erik Brynjolfsson and JooHee Oh at 0.23 of one percent of national GDP) + the multiplier effect of the disrupted digital economy

### The formula

**Cost** = National GDP (81,681 million AZN) * Duration (0.00273%) * Extent of digital economy (1.6%) + the multiplier effect (2.54) = 9.1 million AZN (5.3 million USD)

Or 418.6 million AZN (247 million USD) in total for 46 days. The difference in total amounts based on this specific formula and the final calculated cost mentioned above (413 million AZN/243 million USD) are directly linked to the growth indicators of each affected industry and indirect losses that we factored during the research. We also had to produce estimates for some indicators such as the impact of shutting down some of the social media platforms.

---

79 The multiplier effect of the disruption of the digital economy was calculated at 2.54 (ratio) in contrast to the original indicator proposed by the Brookings Institute formula which is 1.54. The 2.54 ratio was taken from the Strategic Road Map for Telecommunication and Information Technologies decree signed by the President Ilham Aliyev in 2016.
like Twitter, which is not very popular in Azerbaijan. The platform’s popularity grew during the war but the user base is still more limited than that of Instagram or Facebook.

For the purpose of this research, and in order to assess the impact of internet disruptions in 2020, we will analyze indicators for 2019 keeping in mind the restrictions on access to the internet that existed before these disruptions.80

In 2019, the turnover of the ICT industry in Azerbaijan amounted to 2.2 billion AZN (1.2 billion USD). Compared to 2018, the nominal increase was 17 percent, and in real terms it was around 15 percent. In contrast to other economic areas, this was a significant growth.

Mobile communications make up the bulk of this turnover. The direct profits of these companies account for 41 percent of the ICT industry. Among the industry’s most profitable areas were: data services; the provision of maintenance and other information services in computer networks; activity related to data processing, development and management of web pages; and software development.

As there is no local production, all telecommunication equipment is imported. If in the past the ICT import totalled an average of 370 million AZN (216.9 million USD) per year, in 2019 it exceeded 900 million AZN (527.7 million USD) and accounted for 3.9 percent of total imports.

Impact of internet disruptions by area

When assessing the economic impact of the 46-day internet shutdown in different areas, we focused on the following areas: the ICT market (including mobile and internet communication), e-commerce, the advertisement market, social media and communication apps (which were inaccessible during the shutdown) and finally the indirect costs.81 Aside from the economic costs, we also analysed the impact that the internet restrictions had on education.

Our analysis exposed significant economic losses among the industries that rely on the internet for their operations.

ICT market

The ICT market suffered a significant decline in September - November 2020, compared to in 2019. Taking into account that there was a nominal increase of 19.12 percent of this sector in the first few months of 2020, before the COVID-19 pandemic-related restrictions were introduced, a similar growth was expected for the months of September, October and November 2020. Instead, growth declined during these months. As a result, it can be concluded that the ICT market lost a total of about 56.7 million AZN (33.4 million USD) during these 3 months.

To better understand the scale of the economic losses, we can also refer to the statistics provided by whois.az. This site registers sites opened within the «az» domain. According to the site, as of October 1, 2020, there were 36,302 such sites in Azerbaijan. However, by 1 January 2021, the number had decreased to 35,967 sites. In other words, at least 335 sites were closed down during this period.

Taking this a step further, it is possible to estimate the costs of the restrictions of internet services for private customers in terms of both the time and money lost. During the 46-day internet shutdown, private households continued to pay for internet services, despite the difficulties they experienced with respect to accessing most online resources, including social media platforms, which are the main source of information for most people in Azerbaijan.
The average internet user globally spends 6 hours and 43 minutes online per day according to data from early 2020. Thus, we can estimate the time lost during the internet shutdown as 6 hours for each of 46 days for the average user. The two most popular social media platforms in Azerbaijan are YouTube and Facebook. According to data from Alexa.com, Azerbaijani users spend an average of 51.06 minutes on these two platforms daily, which makes up 16 percent of their time. In 2019, the population paid a total of 120,896.3 AZN (71,000USD) for internet access. This equals approximately 10,074.7 AZN (5,900 USD) per month. Using this figure, we can estimate that the Azerbaijani people spent a total of 15,194.6 AZN (8,900 USD) on internet access during the 46 days of the shutdown, although they were unable to use most internet resources.

Advertising market

The online advertising market in Azerbaijan has experienced significant growth in recent years especially due to the surge in social media use. Assuming that the rate per capita on online advertising ranged between 3 and 3.6 USD, the total annual turnover of this market was around 60.3 million AZN (35 million USD) in 2019. As a result of the internet restrictions imposed during the war in Nagorno-Karabakh, the online advertising market was virtually suspended. Using the turnover figure from 2019 as the basis, we can calculate that the costs of this suspension amounted to 7.6 million AZN (4.5 million USD).

E-commerce

Contractions in e-commerce were deeply felt during the 46-day internet shutdown. Many small businesses in Azerbaijan sell and advertise their products through social networks. Due to the internet disruptions and the blocking of social networks, many businesses were forced to shut down. According to the Central Bank, no actual growth of this market was observed in October 2020, and only limited growth in November 2020, compared to previous months in 2020, when it experienced an average increase of 31.18 percent. Even during the strictest lockdown measures in April and July 2020, respectively, the e-commerce registered growth was 18 percent and 11 percent, respectively. Based on this, we estimate that the minimum loss of growth during the 46-day internet shutdown was 15 percent per month, and thus we conclude that the e-commerce market suffered a total loss of 58 million AZN (34 million USD).

Indirect costs/impact

The internet restrictions also impacted companies and businesses working in other fields than those mentioned above as they were unable to use the internet for online meetings, business transactions, and other relevant work, which reduced their operations.

To calculate the overall direct and indirect costs of internet shutdowns, the CST is using a ratio of 2.54 of the indirect costs. By applying this ratio to the estimated costs of the 46-day internet shutdown in Azerbaijan (162.6 million AZN, or 95.4 million USD), we can conclude that the total direct and indirect costs of this shutdown was 413.0 million AZN (or 243 million USD).

Education

Education was also seriously affected by the 46-day internet shutdown as the restrictions came at a time when online teaching tools were widely used at all levels of education due to the COVID-19 pandemic. Long-standing problems such as inequality in internet access and lack of adequate internet infrastructure compounded this impact.

According to official figures provided by the Ministry of Education, the total number of registered secondary and high school students in the 2020-2021 academic year was 1,569 million, while the total number of teachers was
In connection with the transition to online education in connection with the COVID-19 pandemic, the Ministry of Education introduced Microsoft Teams as the official e-learning platform for educational institutions at all levels. In total, 1,442,203 students and 128,132 teachers in Azerbaijan registered with the platform as of the beginning of the 2020-2021 academic year.

Available ministry data indicates that the total number of active users of the Teams platform in Azerbaijan was 1,170,528 in January 2021. However, it is not clear how many of them were students and teachers. The ministry defines active users as users who access the platform at least once a week. It is estimated that some 32% of students and teachers are not active users (taking into account the total number of registered students and teachers).

The rural-urban divide in internet access, which was discussed earlier in this report, exacerbates the issue of access to online education. According to the Ministry of Education, the rate of participation in online classes among middle and high school students has been around 75 percent of all students in Baku and other cities across the country since the start of the academic year. Taking into account that the internet penetration rate is highest in the wider Baku area, where about 40 percent of the total number of students live, the participation rate is likely to have been higher than the average there and lower in other areas. Thus, the figure quoted by the ministry means that a significant number of students, especially students living outside the Baku area have had no or limited access to online education. During the war in Nagorno-Karabakh, the number of students participating in online classes further decreased as a result of the internet disruptions imposed across the country.

The Ministry of Education has stated that free video lessons are posted on its online portal, but it has not explained how students whose families cannot afford internet access or the devices needed to connect to the internet can access these videos. The ministry has suggested that parents take their children to computer centres that are available in 28 schools in 17 regions. However, it is a highly unrealistic scenario that the parents of all students who are unable to access online classes at home would attend such classes in the computer centres, especially during a global pandemic that requires social distancing.

In the absence of alternative solutions, Azerbaijan’s internet economy suffered a 243 million USD loss during the 46-day internet shutdown, and the long-term impact is yet to be seen. The prospects for recovery of the digital economy are poor, taking into account the government’s approach and its track record on fundamental freedoms.

---

82  Azerbaijan has the second lowest pupil-teacher ratio at the primary level and fourth lowest at the tertiary level according to Asian Development Bank report 2020. “The low ratio in Azerbaijan, as noted in World Bank (2015), is because of a decline in the number of students. This has been attributed to concerns over the quality of teaching, itself a result of low standards for hiring teachers. Low salaries at all levels of education discourage the qualified and competent from becoming teachers.” https://www.adb.org/sites/default/files/publication/624476/aze-diversified-resilient-inclusive-development.pdf


The internet shutdown during the war in Nagorno-Karabakh in autumn 2020 fits into a pattern of internet restrictions in Azerbaijan, including restrictions on internet access, pervasive surveillance, invasive cyberattacks, and systematic trolling. These tactics have been used as part of the government’s relentless campaign against dissent and has resulted in serious violations of the freedoms of expression, association and assembly, the right to privacy and protection of personal data and other fundamental rights of journalists, human rights defenders, political activists and other members of civil society. The different sections of this chapter discuss these issues in detail.

Restrictions on internet access

While the internet shutdown in autumn 2020 was the longest one to date, Azerbaijan has also previously experienced several internet disruptions. While some of these were deliberate, others were the result of accidents and could have been avoided had the ICT infrastructure not been so highly monopolized.

The first internet disruption documented in Azerbaijan dates back to November 2015, when a fire damaged Delta Telecom - the internet backbone of the country. Five years later, in April 2020, several cities and districts across the country experienced internet disruptions when Delta Telecom's fibre-optic cables were damaged.

Users across the country reported difficulties accessing the internet in February 2020, when Azerbaijan held a snap parliamentary election. These disruptions caused problems with accessing videos from polling stations,

which documented election violations on Facebook and YouTube. In October 2020, internet was inaccessible in downtown Baku during a peaceful, unsanctioned rally organized by the National Council, an umbrella opposition group. These disruptions are believed to have been intentional, but no government institution, ISP or mobile operator took responsibility for them.

Later in this chapter, we describe several additional examples of deliberate internet disruptions, which were reported during international events hosted by Azerbaijan.

Digital surveillance

**Key terminology**

**Black boxes** - Black boxes installed in TeliaSonera’s operation centres in Azerbaijan enabled police and security services to monitor all forms of communication, internet traffic, phone calls, and location data. Example: anyone with access to these “black boxes” can trigger a password reset and intercept the recovery code before the user.

**RCS** - A Remote Control System (RCS) “renders the use of secure communication channels moot by collecting data on an infected device itself, not only data sent over the internet. Emails are recorded by keystroke loggers before encryption and RCS can turn on a device’s camera or microphone without alerting the user.”

**DPI** - Deep Packet Inspection (DPI) means digital eavesdropping that allows information extraction. DPI “is a method of monitoring and filtering internet traffic through inspecting the contents of each packet that is transmitted through an inspection point, allowing for filtering out malware and unwanted traffic, but also real-time monitoring of communications, as well as the implementation of targeted blockings and shutdowns.” DPI can be deployed to blacklist websites and messaging apps.

**Sandvine** - A U.S.-based company owned by the private equity firm Francisco Partners. Sandvine’s technology has been used to censor the internet in more than a dozen countries, including Azerbaijan in recent years.

**Allot** - an Israeli security firm that sold DPI technology to Azerbaijan.

**Verint** - an American/Israeli surveillance company.

**NICE** - an Israeli surveillance company.

**Hacking Team** - an Italian company manufacturing surveillance technology.

**DDoS** - a Distributed Denial of Service Attack (DDoS) occurs when someone attacks the normal traffic of a targeted server, service or network for the purpose of disrupting the service by overwhelming it with internet traffic. As a result, the service is unable to handle the traffic and thus rendered inaccessible.

The extent of online surveillance in Azerbaijan has been documented over the years by journalists, rights defenders and activists. In 2014, an OCCRP investigation revealed how mobile operators were directly passing on information about its users to the respective government authorities. In a country where the government enjoys unprecedented control over the ICT industry and where some of the key players in the market such as mobile operators and ISPs are affiliated with the government or its officials, the findings of the investigation was not at all surprising. The 2014 investigation quoted the director of the Media Rights Institute, Rashid Hajili as saying that both mobile companies and ISPs were obliged to provide special facilities to the Ministry of National Security (MNS) for surveillance purposes in accordance with

---


89 “American technology is used to censor the web from Algeria to Uzbekistan,” Bloomberg, 8 October 2020, https://www.bloomberg.com/news/articles/2020-10-08/sandvine-s-tools-used-for-web-censoring-in-more-than-a-dozen-nations?ref=AhigZgK


91 The Ministry of National Security was dissolved in 2015 based on a presidential decree. It was replaced by the National Security Service, which exercises domestic duties, and a foreign intelligence service.
existing legal provisions as explained earlier. In the case of mobile companies, no court approval was sought to eavesdrop on the conversations and SMS exchanges of their customers - a common practice to this day.

One of the first accounts of collaboration between mobile companies and the government is that of journalist Agil Khalil. In 2008, Khalil was working on a story about alleged involvement of MNS employees in corrupt land deals. After taking photographs for the story, he was approached by MNS agents and beaten. The journalist escaped from his attackers and managed to take photos of them. Khalil filed a complaint with the police, and an investigation was opened but eventually dropped, without the perpetrators having been identified and prosecuted. Soon after turning to the police, the journalist realized that he was being followed. When he filed another complaint with the police about the surveillance, police again failed to follow through. A few days later, Khalil was subjected to a new attack: this time, an unknown assailant stabbed and injured him. Khalil again turned to the police, accusing both the MNS and the mobile operator Azercell (whose services he was using) of being responsible for the attack. He argued that the operator had helped the MNS to track down his whereabouts, thereby facilitating the attack. The involvement of Azercell in the case became more evident when the operator provided a local court, which examined the journalist’s complaint, with alleged SMS exchanges between Khalil and a man named Sergey Strekalin, who the MNS claimed was Khalil’s lover and had stabbed the journalist out of jealousy. When Khalil’s lawyer requested access to these SMS exchanges, Azercell refused, which called into question the authenticity of these messages. Khalil left Azerbaijan the same year after another attempted attack against him and the continued failure of the authorities to hold accountable his assailants. He took his case to the ECtHR, resulting in that the Azerbaijani government made a so-called unilateral declaration (an official admission) before this court in 2015 that it had violated Khalil’s right to life, freedom from ill-treatment and freedom of expression and agreed to pay 28,000 EUR in compensation to him. As the government made this admission, there was no ECtHR ruling on the case.

Interception of SMS exchanges remains an acute problem in Azerbaijan. In recent years, scores of political activists, journalists, rights defenders and independent media platforms have had their social media accounts compromised. In many of these cases, those affected have had SMS notification enabled as a two-step verification (2FA) procedure for accessing their Facebook accounts. As a result, when their accounts were compromised, they were unable to restore access to the accounts relying on traditional troubleshooting steps offered by social media platforms such as Facebook. Thus, they were unable to retrieve password reset codes sent by Facebook by SMS as their messages were intercepted by the operators, only to be passed on to the relevant government bodies. This experience shows that mobile companies have been involved in many of these attacks. However, none of the operators have taken the blame, so far.

The earliest example of SMS surveillance goes back to 2009, when 43 Azerbaijans voted for Armenia’s entry in the Eurovision Song Contest through votes cast by SMS. A number of these people were summoned and questioned by the security services. In an interview with Azadliq Radio (the Azerbaijani service of Radio Free Europe/Radio Liberty), one of these voters, Rooshan Nasirli said that the authorities demanded an “explanation” for his vote and told him it was a “matter of national security”. He told the service: “They were trying to put psychological pressure on me, saying things like, ‘You have no sense of ethnic pride. How come you voted for Armenia?’ They made me write out an explanation, and then they let me go.” The authorities did not deny that they had identified and summoned people who voted for Armenia, and argued that they were merely trying to understand the motives of these people.

Three years after the Eurovision scandal, an investigative documentary aired on Swedish TV called “Mission: Investigate” revealed how the Swedish telecommunications giant TeliaSonera, which at the time owned a majority stake of Azercell, allowed “black boxes” to be installed within their telecommunications networks in Azerbaijan from as early as 2008. These boxes enabled...
security services and police to monitor all network communication, including internet traffic and phone calls in real-time without any judicial oversight.\footnote{96}

The exposure of these black boxes explains the type of technology the government was deploying already at the time of Eurovision in 2009. The investigation aired by Swedish TV also confirmed that wiretaps were used as evidence in politically motivated cases.

In March 2018, both TeliaSonera and the other Azercell shareholder, Turkcell sold their shares to Azintelecom LLC, a government owned subsidiary and left the country.\footnote{97} The company representatives said nothing about the black boxes left behind. Azercell is known to have ties to the ruling family, namely the daughters of President Ilham Aliyev, Arzu and Leyla Aliyeva.\footnote{98}

An investigation by Citizen Lab in 2014 revealed that Azerbaijan was also among the countries using Remote Control System (RCS) surveillance technology called Davinci, which allows for data collection on infected devices both online and offline. Specifically, the technology allows for file extraction from a targeted device, interception of emails and instant messages, as well as remote activation of the device’s webcam and microphone.\footnote{99}

In order to use the RCS spyware to access the targeted devices, these devices must first be infected with the spyware. Infection often occurs through phishing attacks that “convince a user to open a cleverly disguised executable file, or authorize installation of an application.”\footnote{100}

A leaked email exchange from the Italian surveillance malware vendor Hacking Team indicates that a representative of this company travelled to Baku in July 2012 to present RCS software to the MNS. According to a leaked email dated 26 July 2012, during the demonstration of the RCS, the MNS expressed particular interest in a so-called Network Injector (NI) to be used for infecting devices knowing only limited information, such as a Skype username or an email address. The Hacking Team representative also explained that he had provided the MNS with instructions for how to infect devices via Gmail, specifically by sending a.doc file. Finally, the MNS was interested in offline infection tools. According to the Hacking Team representative, the only concern the MNS had was that it took “too many clicks” to active an infection on a targeted device.\footnote{101}

This email exchange is just one of hundreds where the Hacking Team communicates with their client in Azerbaijan starting as early as 2012. The name of one person mentioned in the email quoted above, i.e., Reuven appears in many of the exchanges. Reuven’s full name is Reuven Elazar, Director of Sales and Business Development CEE at the Israel-based surveillance company NICE. At the time, NICE was engaged by the Hacking Team to distribute the latter’s technology in several countries, including Azerbaijan. The client’s Technical Manager mentioned in the email is likely a man named Riad, who frequently exchanged emails with the Hacking Team, specifically about the RCS software’s technical applicability. In one leaked email Riad specifically asked the Hacking Team to show how to apply the software to Facebook, Twitter and mobile phones.\footnote{102}

The Israeli-American Verint based in New York is another company from which Azerbaijan bought surveillance software. According to an independent investigation published in 2015, Verint was the primary provider of the state-of-the-art PSTN (public switched telephone network)- and IP-based surveillance monitoring centres in the country since 2000s onwards. One of its monitoring centres was located inside the MNS. These monitoring centres were divided in two separate categories - active and passive.\footnote{103}

\begin{thebibliography}{99}
\bibitem{98} “Azerbaijani President's daughters tied to fast-rising telecoms firm,” RFERL, 27 June 2011, https://www.rferl.org/a/azerbaijan_president_aliev_daughters_tied_to_telecoms_firm/24248340.html
\bibitem{100} “Mapping Hacking Team's Untraceable spyware,” Citizen Lab, 17 February 2014, https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/
\bibitem{101} See leaked Hacking Team email (in Italian) dated 26 July 2012, released by Wikileaks at https://www.wikileaks.org/hackingteam/emails/emailid/4433236
\bibitem{102} https://www.wikileaks.org/hackingteam/emails/emailid/4433857
\end{thebibliography}
“Active monitoring targets a specific user/entity using identifiers such as IP addresses or unique signatures. Automated requests initiated by the state will return full data package on said user/entity. Having made available their cables to the state, telecoms providers know monitoring is taking place, but know not what is being monitored.

Passive monitoring is a process by which the center collects all of the telecom provider’s data: this process includes filtering on the basis of the specific parameters set in place by the national security services. Passive monitoring is intended to be invisible; telecoms providers may not know it is in operation.”

In addition to a circuit switch monitoring system, Verint also sold Azerbaijan a very basic Deep Packet Inspection (DPI) system in 2009.

In practice, Azerbaijan’s (now former) MNS relied on active, target-based monitoring which was made possible as a result of the compliance of local telecoms.

Verint also supplied Azerbaijan with a system that allowed the MNS to collect information from social media. One of Verint’s former employees, who travelled to Azerbaijan to train the client, was asked how to use the system “to check sexual inclinations via Facebook.” This technology was used in 2017, when the Azerbaijani government carried out a crackdown against gay and transgender people.

Based on the evidence collected up to now, it can be concluded that the Azerbaijani authorities are likely to have used RCS technology since 2013, in combination with a homegrown malware called AutoItSpy.

Azerbaijani civil society representatives have repeatedly been targeted by phishing.

Civil society representatives targeted by phishing:

In 2016, an unknown person pretending to be human rights defender Rasul Jafar sent emails using a custom malware agent. The emails contained an infected Microsoft Word file titled “list of political prisoners”. Once the file was opened the malware “installed a keylogger that recorded the user’s keystrokes and relayed screenshots of their computers back to the attacker, potentially compromising all of their passwords, contacts and private communications.”

In January 2020, an IP linked to the Ministry of Internal Affairs was used to target members of civil society in several documented attacks. First, veteran human rights lawyer Intigam Aliyev received an email from Rasul Jafar with a WeTransfer link to a downloadable file entitled “invoice for EU”. Aliyev, spotting that something was wrong, forwarded the email to Jafar who confirmed that the email had not been sent by him. The email was investigated by Virtual Road, a secure hosting project run by the Qurium media foundation, which hosts a number of Azerbaijan news websites blocked inside the country. This investigation showed that the WeTransfer link provided in the email contained malware capable of collecting keystrokes, screenshots, and WiFi credentials from the targeted computer.


107 Citizen Lab identified RCS endpoint in Azerbaijan active between June-November 2013 used by Azertelecom - the second largest internet provider outside Baku. In October 2013, Azerbaijan held highly contested presidential elections.


The Azerbaijani authorities beefed up their surveillance capabilities further ahead of the European Games, which took place in the capital Baku in June 2015. According to Virtual Road, a, Azerbaijan acquired sophisticated DPI equipment right in time for the European Games. The seller was the Israeli security company Allot Communications. The new equipment, which cost 3 million USD, allowed the MNS to monitor social media and communication apps such as Facebook, Viber, and WhatsApp. It is unclear for what specific purposes the MNS monitored these platforms at this time. Two years later, when Azerbaijan hosted the Islamic Solidarity Games, the authorities did not only monitor the communication on social media and communications platforms but also blocked access to WhatsApp, Viber and Skype, which were unavailable throughout the games. First the authorities denied any responsibility, but after the end of the games, the MTCHT admitted that access to these platforms had been blocked for security reasons.\footnote{111} The ministry did not explain how this had been done.

To recap, by 2015, the government had black boxes, and RCS and DPI surveillance technology at its disposal. It had successfully tested this equipment to snoop on Azerbaijani voters during the Eurovision song contest in 2009.\footnote{112} In addition to Allot, the Canada-based company Sandvine also sold DPI equipment to Azerbaijan in 2015. The customer in Azerbaijan was Bakcell\footnote{113}, one of the three national mobile phone operators. This partnership was published on Sandvine’s website where the company hailed Bakcell as “the leading provider of intelligent broadband network solutions for fixed and mobile operators” in Azerbaijan. Bakcell worked with the Azerbaijan-based IT company Bestcomp Group to roll out the Policy Traffic Switch (PTS) it purchased from Sandvine. According to investigations by Qurium Media, Bestcomp frequently accompanies the State Agency for Public Service and Social Innovation during their visits abroad.\footnote{114} It is unclear whether Sandvine technology was deployed before 2017 but forensic work carried out by the Virtual Road in 2018 revealed that Sandvine’s DPI was used to block at least one website in 2018.\footnote{115} During the 44-day war in 2020, Sandvine partnered with Delta Telecom to block access to a number of social media platforms that provide video streaming, namely YouTube, Facebook, and Instagram.\footnote{116}

\begin{itemize}
\item A few days later, a group of civil society activists, journalists and human rights defenders received another suspicious email. The alleged sender was Robert Facino, the head of the Secretariat of the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe. The email included a WeTransfer link to a downloadable document called “Report-2019.docx.hta”. A Virtual Road investigation found that this link contained a malware that granted the attacker direct access to the victim’s device.\footnote{110}
\item A similar malware was distributed via Facebook messenger.\footnote{110}
\end{itemize}
In 2017, the Virtual Road's forensics team exposed how DPI technology was deployed to block access to independent and opposition websites in Azerbaijan. The team found that the Electronic Security Centre at the Ministry of Communications instructed upstream providers to block access to azadliq.info, azadliq.org, meydantv and abzas.net through the use of DPI equipment in March 2017. The same month, Azerbaijan's Law on Information, Informatization and Protection of Information was amended to grant the authorities wide powers to block access to websites allegedly featuring prohibited information threatening the state or society. In accordance with the new provisions, the authorities can immediately block access to such websites if the website owners fail to remove the allegedly unlawful content within eight hours of receiving notification about this, without having to obtain court approval of the measure prior to its implementation. Court approval can be sought only after the blocking measure has taken effect. Moreover, given the lack of independence of the judiciary in Azerbaijan, a fair judicial assessment cannot be expected in these cases. At the time of the discussion of the new amendments, the Chair of the Board of the State Press Council, Aflatun Amashov argued that that the new provisions were necessary to combat the propaganda of violence, religious extremism, incitement to national, religious, and racial hatred, disclosure of state secrets, abuse and slander, breach of privacy and family life. However, in practice, the new provisions have provided the authorities with new tools to silence dissent.

Also after the adoption of the new provisions on blocking internet content, DPI continued to be used against independent or opposition online news sites, such as in the case of gununsesi.org in December 2019 and in the case of the already previously blocked azadliq.info in January 2019.

In 2017, a court order obtained by MTCHT effectively blocked access to a total of five independent and opposition media websites on the grounds that these websites allegedly posed a threat to Azerbaijan's national security and featured content promoting violence, hatred, and extremism. A handful of other websites featuring content critical of the authorities were blocked without a court order on similar grounds or for alleged slander and spreading of misinformation.

In some cases, the MTCHT requested news sites to remove specific articles unfavourable to those in power. For example, news platforms az24saat.org and monitortv.info were ordered to remove articles that concerned then presidential aide Ali Hasanov on the grounds that these articles allegedly contained slander and lies.

The independent and opposition news website argument.az was blocked after publishing a story about a regional protest.


The case of Meydan TV, Azadliq newspaper, Azerbaycan Saadi and Turan TV, which were all blocked in 2017, illustrates the failure of the authorities to provide any evidence to back up their claims that independent and opposition news sources have published allegedly unlawful content. Although the government argued that these websites had published articles aimed at the forcible change of the constitutional order, the organization of mass riots and other illegal activities, it did not specify to which articles these accusations applied. The European Human Rights Advocacy Center (EHRAC), which represents all the four websites mentioned at the European Court of Human Rights, concluded: “No effective and independent review took place in the first instance decision to block access to these websites in 2017 and in subsequent years. The courts simply accepted the authorities’ allegations at face value and made no attempt to adequately consider or explain why the content was unlawful.”

**DDoS and hacker attacks**

In addition to blocking access to independent and opposition websites, the Azerbaijani authorities have systematically carried out DDoS attacks against such sites since 2017. As a result of DDoS attacks, independent and opposition websites have in some cases been inaccessible for several days.

According to the Virtual Road, in March 2017, the abzas.net opposition news platform was targeted by a series of DDoS attacks. The attacks lasted for eight days and rendered the website inaccessible for five days until it successfully migrated to secure hosting infrastructure. The IP network behind the attacks was linked to the Azerbaijani government, specifically to the Ministry of Foreign Affairs, the Cabinet of Ministers and the mailserver of the Ministry of Transport.

In August 2018, the Virtual Road reported DDoS attacks against two other online Azerbaijan-covering media platforms, gununsesi.info and azadliq.info. The forensics traced the source of the attack to an IP that hosts several government institutions including the Special State Security Service, which is under direct command of the president.128

In 2019, the websites of the abzas.net, gununsesi.info, azadliq.info and 24saat.org media resources were repeatedly subjected to DDoS attacks.129

In April 2020, the Virtual Road reported that Timetv.live was targeted by DDoS attacks after publishing a story critical of the State Oil Company (SOCAR). The source of the attack was the same IP linked to the Ministry of Interior, which was used to carry out phishing attacks against journalists and rights defenders in January 2020, as discussed above.130

In May 2020, the website of the independent Turan News Agency was subjected to multiple DDoS attacks, which rendered it inaccessible for at least one day.131

Since 2018, there has also been a spike in hacker attacks targeting Azerbaijani civil society activists, rights defenders, and journalists. As a result, dozens of emails and social media accounts have been compromised. A number of these attacks are described below.

In November 2018, journalist Aziz Karimov received a password reset request from Facebook. Karimov sensed something was wrong because he had not requested any reset. In little over an hour, he lost access to his Facebook profile, as well as to the four Facebook pages he was administrating. One of these pages belonged to the Turan News Agency. The same month hackers also targeted the Facebook account of Azadliq Radio, the Azerbaijani service of

---


Radio Free Europe/ Radio Liberty, Azadliq Radio's website has been blocked in Azerbaijan since 2017. Since then, its social media page on Facebook has gained popularity. The hackers, who compromised the page of the service, deleted over 2000 videos, posts, and photos and several thousands of its followers. In the case of Karimov, the source of the attack was traced back to Enginet, a national ISP. When we investigated ISPs for this report, we traced the ownership of this provider to the former chief of the Information Systems Department of the Ministry of Education, Samir Mammadov.132

In March 2020, a group of Azerbaijani women rights and LGBTQI activists were targeted by hacker attacks. As a result of these attacks, Gulnara Mehdiyeva, founder of a feminist movement lost access to her Telegram, Facebook, Gmail and Protonmail. A year later, Mehdiyeva was targeted again ahead of International Women’s Day, celebrated on 8 March when several of her personal audio messages on Facebook were compromised and leaked.133 The audio files were stolen from private messages she had exchanged on Facebook in relation to the previous hacker attack. During the coordinated hacker attacks carried out in March 2020, two Facebook pages that focus on LGBTQI issues, the Minority Magazine and Nefes LGBT Alliance were also compromised. Years’ worth of content was deleted as a result of the attack. Several members of LGBTQI community also reported attempts to compromise their Facebook accounts.134

Other hacker attacks carried out in March 2020 targeted several Facebook pages affiliated with the online news platform anews.az.135

In April 2020, the abzas.net news platform was hacked. The hackers removed a month’s worth of content and changed the headlines of some of the stories published on the site.136 As described above, earlier in 2017, abzas.net was subjected to a series of DDoS attacks and access to it was arbitrarily blocked in Azerbaijan. Following this, a new version of the site was launched, and it was this version of it that was hacked in 2020.

In June 2020, Meydan TV, an independent news platform blocked in the country, had its social media accounts compromised. The news website lost two years of its content on its Azerbaijani language Facebook page, and two months of content on its Instagram page. The previous month, in May 2020, Meydan TV was subjected to DDoS attacks.137 The June 2020 attack was not the first time the social media accounts of Meydan TV were compromised. In February 2018, hackers took control of the platform’s Facebook page, deleted years of posts, and removed 100,000 of the news platform’s subscribers.138

In addition to Meydan TV, the Facebook page of the online news platform argument.az was also compromised in June 2020. The page lost 12,000 followers and all posts published on the page until March 2020 were deleted. Access to Argument.az was blocked several times in 2018-2019. First, the website was blocked by court in August 2018 because of two articles it had published that were deemed to threaten national security. The decision was annulled two days later. However, the website was blocked again in April 2019 after it published a story about protests in one of Azerbaijan’s regions. This time the MTCHT blocked the site without any court approval. The website appealed the MTCHT’s decision to court, arguing that the decision was illegal. Although the blocking measure was lifted and the website became accessible the same month, the court proceedings in this case were still ongoing at the time of writing of this report.139

In June 2020, human rights lawyer Intigam Aliyev had his Facebook account compromised. A few days later, the opposition group D18 also reported

132 At present, the director of Enginet is Anar Nagiyev, and the company’s founder is Elnur Malikov. Previously it was reported that Elnur Malikov is related to Samir Mammadov. The information provided by the Ministry of Taxes indicates that Teymur Mammadov was the legal representative of the company in 2018. But according to the company’s website, Enginet’s legal representative at present is Samir Mammadov.


that the group’s Facebook page had been hacked. The following month, freelance journalists Aysel Umusova and Fatima Movlamli, as well as activist Rustam Ismayilbeyli had their Facebook accounts compromised despite having 2Factor Authentication (2FA) enabled on their accounts.140

Another activist targeted in June 2020 was Mehman Huseynov, a popular citizen journalist and editor of Sancaq, a socio-political magazine which documents corruption and human rights violations in Azerbaijan. When undergoing treatment for cancer at this time, Huseynov took time off from his work and social media. In his absence, Sancaq TV’s Instagram account was hacked. In March 2021, someone tried hacking into Sancaq TV’s Facebook page but did not succeed.141

In September 2020, hackers attacked the Facebook page of bastainfo.com, a website affiliated with the opposition party Musavat that is blocked in Azerbaijan. The hackers removed page followers and content shared on it since 2017.142 Prior to this, in January 2020, several members of the Musavat party had reported having their social media accounts compromised.143

In March 2021, a group of journalists and feminist activists were targeted via Facebook and Telegram. Activists Vafa Nagi and Narmin Shahmarzade had their Facebook accounts compromised. Following the attack, the hackers began an online harassment campaign against the women by sharing non-consensual intimate images (sometimes referred to as revenge porn) via their hacked Facebook accounts and Telegram channels. Journalist Fati-ma Movlamli was also among the women targeted via Telegram channels.144

It has not been possible to verify the source of most of the hacker attacks described above, although the pattern of attacks suggests the involvement of the authorities. However, in at least one case, it was demonstrated that the perpetrators were linked to the State Security Service. In September 2020, student activist Rustam Ismayilbeyli received a warning via Facebook messenger from a person named Elvina Mammadova, who presented herself as an employee of the State Security Service. She threatened to disclose intimate images of Ismayilbeyli’s partner unless he stopped his activism.144 A year later, the images in question were published on one of the Telegram channels set up to target the women mentioned above, which, thus, demonstrated the involvement of the State Security Service in those attacks.145

The authorities have vowed to investigate the recent attacks146. However, in response to a complaint she filed with the police regarding the attack to which she was subjected when her personal messages were leaked online, activist Gulnara Mehdiyeva was informed that no criminal case was planned to be opened.147 There have been no effective investigations into hacker attacks against civil society representatives reported in earlier years.

In the case of news platforms whose Facebook pages were compromised, the attacks came shortly after they had published stories critical of the authorities. The platform editors were threatened and forced to remove critical content often exposing a government official or a corruption scandal. This was the case in relation to argument.az, Sancaq.tv, anews.az and others.

In March 2021, a group of journalists and feminist activists were targeted via Facebook and Telegram. Activists Vafa Nagi and Narmin Shahmarzade had their Facebook accounts compromised. Following the attack, the hackers began an online harassment campaign against the women by sharing non-consensual intimate images (sometimes referred to as revenge porn) via their hacked Facebook accounts and Telegram channels. Journalist Fatima Movlamli was also among the women targeted via Telegram channels.144

The authorities have vowed to investigate the recent attacks146. However, in response to a complaint she filed with the police regarding the attack to which she was subjected when her personal messages were leaked online, activist Gulnara Mehdiyeva was informed that no criminal case was planned to be opened.147 There have been no effective investigations into hacker attacks against civil society representatives reported in earlier years.

In the case of news platforms whose Facebook pages were compromised, the attacks came shortly after they had published stories critical of the authorities. The platform editors were threatened and forced to remove critical content often exposing a government official or a corruption scandal. This was the case in relation to argument.az, Sancaq.tv, anews.az and others.

In 2018-2021, the Facebook pages and Instagram profiles of several high-profile opposition leaders were also compromised.

---


144 Screenshot obtained from the activist.


In 2018, in the run up to the presidential election, which the opposition boycotted, the Facebook accounts of opposition leader Ali Karimli and former presidential candidate Camil Hasanli were hacked.\textsuperscript{148}

In November 2019, the Facebook page of opposition leader Gultekin Hajibeyli was hacked. Later, in January 2020, Hajibeyli discovered that at least two fake accounts were impersonating her on social media platforms. A fake Instagram profile claimed that Hajibeyli was an “escort woman”, while a fake Facebook profile insinuated that she was the mistress of other, male politicians. It was not possible to identify the source of the attacks against Hajibeyli in these cases. However, in October 2019, a conversation she had with a US diplomat via her mobile device and audio recording of an in-person meeting she had with an EU diplomat were leaked by the pro-government RealTV channel. These leaks indicated that Hajibeyli’s mobile phone was wiretapped and that she was under surveillance.\textsuperscript{149} The opposition activist’s Instagram account was hacked again in May 2020.\textsuperscript{150}

Trolling

The ruling part and other government institutions have employed trolling networks to attack outspoken critics, independent and opposition media on social media platforms. Pro-government trolls typically leave hundreds of comments under posts for the purpose of derailing the discussion and intimidating dissent. Trolls and pro-government accounts on social media platforms have also abused mechanisms for reporting violations of community rules and copyright infringements to block access to content critical of the authorities.


and local media, public figures including opposition and the ruling party of Azerbaijan, to create a perception of widespread criticism of some views and widespread support of others.”

This was the first time that Facebook confirmed that the Azerbaijani government is operating a troll army. However, while this step was welcome, Facebook has failed to follow up and take action against other fake accounts used to target critics of the regime, thus allowing the government-initiated trolling to continue.

As early as in 2011, there were signs that specific online groups had been tasked with protecting Azerbaijan’s interests. Chief among them was Azerbaijan’s pro-government youth organization, IRELI (its status was changed to that of a public union in 2018). IRELI’s then Secretary General Rauf Mardiyev said that the objective of the organization was to prepare young people to “take active part in the information war”. He also said that: “Email attacks, promotion campaigns on social networks and the effective use of Wiki technologies are among our priorities.”

A lot has changed since Mardiyev’s interview in 2011. First, Facebook no longer limits the number of pages a single user can create, making it easier for herders to manipulate online content managing botnets and trolls. A recent case in which 500 fake pages attacked the independent online news platform Meydan TV illustrates this trend. The attack took place in February 2021, when Meydan TV shared a call for applications for a capacity building program held in partnership with IPHR on its Facebook page. A closer look at the more than 500 negative comments that this post generated revealed that they had all been made from accounts created in the last few months.

This was not the first time Meydan TV’s social media accounts were targeted. In October 2016, ahead of a constitutional referendum held in Azerbaijan, leaked screenshots showed herder Elmar Mammadov instructing a group of Azerbaijani Facebook users to target Meydan TV and Azadliq Radio as soon as these started live streams of planned protests. Mammadov also warned the group to refrain from using the name of the ruling party to avoid suspicion. Abroad trolls are deployed to attack international events where Azerbaijan’s dismal human rights record and press freedom are criticized by distorting the discussion and hijacking conference hashtags.

A more powerful actor than Mardiyev who was also attempting to control online discussions was Ali Hasanov, former presidential advisor. Hasanov was known as the “King of Trolls” and was notorious for his attacks against government critics both at home and abroad. While Hasanov is widely believed to have led a government troll army used to discredit opponents, he himself denied these allegations. When leaving office in 2019, he told the BBC’s Azerbaijan service that these allegations were “false and slanderous” and insisted that there was no troll army in Azerbaijan but “simply the public supporting the president.”

In 2018, the Azerbaijani opposition news site abzas.net was informed by Facebook that its page had been removed from this platform due to alleged violations of community standards. This happened after the abzas.net page was subjected to troll army attacks of hundreds of users, who falsely reported the page as being in violation of Facebook’s community standards. When making the decision to remove the page, Facebook failed to take this into account. The page was later restored thanks to an intervention by the digital security helpline operated by Access Now.

There have been similar cases on YouTube, where fake accounts or other pro-government accounts have falsely accused channels associated with the political opposition of copyright violations, resulting in that content on these channels has been taken down or that the channels have been temporarily disabled. For example, in March 2020, the YouTube channel of the Azadliq newspaper was informed that several of its videos had been blocked by the platform due to alleged copyright violations. In another case, several videos that France-based journalist Natig Adilov had posted on YouTube were

---

152 “It took Facebook more than a year - and a whistleblower - to remove a troll farm connected to Azerbaijan’s Ruling Party,” BuzFeedNews, 8 October 2020, https://www.buzzfeednews.com/article/craigsilverman/facebook-azerbaijan-troll-farm


blocked by the platform due to false reports about copyright violations. Shakir Zade, an Azerbaijani activist living abroad, had his YouTube channel disabled twice - in December 2019 and January 2020 when government-backed media outlets accused him of multiple copyright infringements. The YouTube channels of AzadSoz and HamamTimes were also targeted on similar grounds in 2018. Several YouTube videos posted by Meydan TV were taken down in 2018 based on copyright complaints filed by a company called Muse Network, which Meydan TV believes acted in coordination with the Azerbaijani government. The same company also reported videos of Azadliq Radio.

After giving an interview to the Azerbaijan service of Voice of America about police violence she faced during an assembly held in Baku on 8 March 2021, activist Rabiyya Mammadova was targeted by Facebook trolls calling her a liar.

The cases that concern videos published on YouTube, illustrate abuse of the mechanism for reporting copyright infringements on this platform. Under this mechanism, anyone can submit a request to YouTube to take down content featuring copyright protected work published without authorization. All it takes is for the claimant to provide his or her name, contact information and a description of the alleged copyright infringement. YouTube’s copyright policy and Content ID – a computer algorithm filtering and blocking infringing content - lacks discretion and is often unable to distinguish between authorized and unauthorized copyright, and often requires a third-party intervention such as digital security helpline teams to provide assistance in cases of activists, journalists, and rights defenders targeted on the platform.

The type of attacks described are typically aimed at tarnishing the reputation of those targeted, humiliating them publicly and disrupting their work. When journalists and media platforms are subjected to DDoS or hacker attacks, they have to spend time dealing with this emergency instead of carrying out their work. Similarly, activists who attacked online are forced to stop their work and focus on the attack, securing their social media accounts, emails, and devices. This is all time consuming, emotionally draining and exhausting. Targeted civil society members are often left to their own devices and do not have access to adequate assistance to help them to promptly and effectively resolve the emergency. In the longer term, these kinds of attacks may deter activists, journalists and other members of civil society from continuing their work out of fear of being targeted again, because of the reputational damage that the attacks have inflicted or out of a sense of helplessness. It would therefore be important to develop and improve the support mechanisms available to targeted journalists, activists and human rights defenders, in addition to continuing and expanding efforts to prevent them from being targeted in the first place.

Conclusions

This report shows that the 46-day internet shutdown, which took place in Azerbaijan during the war in Nagorno-Karabakh in autumn 2020, was part of a long-term government strategy of internet control, censorship and repression.

During the 46-day shutdown, the internet did not go completely black in the country, but residents were unable to access major online resources, in particular social media and communication platforms. In addition, internet users across the country had problems downloading VPNs -- tools used to
Further, the report provides ample evidence of how foreign companies such as Allot, Sandvine, NICE and others have provided the Azerbaijani government with surveillance technology that has been used to monitor and suppress dissent. This shows the importance of measures to hold such companies to account for the human rights violations their products cause.

The report also discusses the lack of adequate responses by global social media and communications platforms to government-initiated attacks targeting Azerbaijani civil society activists, journalists and human rights defenders, as well as their organizations on these platforms. It is important that YouTube, Facebook, Telegram and other social media and communications platforms develop policies that are better informed by the political realities in countries such as Azerbaijan to avoid that they -- indirectly -- support the governments’ repressive agendas with respect to dissent.

Finally, the report shows that it is crucial that Azerbaijani civil society members are conscious of the online risks they face and take relevant measures to improve their online security and protect themselves from the technology and strategies that the government is using to target, intimidate and attack government critics.

This report highlights how the 46-day shutdown was symptomatic of the government’s heavy-handed approach to controlling the internet. For years, the government has restricted internet access and monitored and suppressed online dissent through monopoly over the ICT industry, extensive surveillance mechanisms, as well as arbitrary blocking measures, online attacks and intimidation targeting internet sites and users critical of the government. This approach has resulted in serious violations of the right to freedom of expression, the right to privacy and other fundamental rights and freedoms of the citizens of Azerbaijan. In addition, it has resulted in that Azerbaijan is lagging behind other countries with respect to internet development and access.

In addition to shining light on how the Azerbaijani government is flouting its international human rights obligations because of its repressive internet policies, the report also draws attention to how other actors -- directly or indirectly -- have facilitated or contributed to the implementation of these policies. First, the 46-day internet shutdown raised questions about the responsibility of internet providers, who participated in implementing the internet restrictions among their customers and offered their customers little, if any compensation for the lack of access to services they had paid for.

access otherwise unavailable online resources. Thus, the shutdown seriously affected the lives of residents, limiting their opportunities to use internet resources to carry out their work and studies, obtain and exchange information, communicate with colleagues, relatives and friends, and take care of basic tasks. Given its unclear legal basis, and its scope and duration, the shutdown clearly did not meet the strict requirements for permissible restrictions on the right to freedom of expression set out by international human rights law, although it was implemented during a state of martial law.

The broader impact of the 46-day internet shutdown is illustrated by its economic costs, which we estimate amounted to a total of 243 million USD, including both direct and indirect costs. The economic impact was compounded by the fact that the authorities failed to offer alternative solutions or support to companies and sectors directly affected by the shutdown. The shutdown also aggravated pre-existing problems with lack to access to education seen in the context of the COVID-19 pandemic, when online education has been widely used.
Based on the issues discussed in this report, we would like to make the following recommendations:

**To the government of Azerbaijan**

Safeguard fundamental rights and freedoms on the internet, including the right to freedom of expression, the right to freedom of association and assembly, the right to privacy and protection of personal data, the right to education, and the right to effective remedies for violations of human rights in accordance with its obligations under international human rights law.

Ensure that any restrictions imposed on access to internet resources are consistent with the strict requirements for permissible limitations on the right to freedom of expression set out by international treaties ratified by Azerbaijan, in particular the European Convention on Human Rights and the International Covenant for Civil and Political Rights.

Provide full information on any restrictions on access to internet resources resulting from government decisions and policies, including the reasons for the restrictions, their scope and duration and; when relevant, offer alternative solutions for internet access to users relying on the internet for the purposes of their work, studies and other needs.

Stop using digital surveillance, cyberattacks, trolling and other tactics to monitor, control and repress dissent online; and ensure that individuals and organizations who post/share/discuss information critical of the government on online platforms are not subjected to retaliatory measures.

Establish an independent, oversight body of the country’s ICT sector as set out in the 2016-2020 National Strategic Roadmap for the development of this sector.

Ensure transparency of new legislation and policies affecting the exercise of fundamental human rights online, including by facilitating public debate on such measures and involving experts and civil society in the elaboration of them.
To Azerbaijan’s Ministry of Education
Ensure equal access to online education tools for students from across the country, including by using different platforms and by providing students with internet access points and working in tandem with other relevant government institutions to improve internet access nationwide.

To internet providers in Azerbaijan
Take adequate measures to protect the right to internet access, privacy and other rights of customers by refraining from participating in the enforcement of internet restrictions and surveillance schemes that do not have a clear legal basis and that have not been sanctioned by competent authorities in accordance with the requirements of national and international law.

Promptly inform customers about any temporary restrictions on internet access and offer appropriate assistance and compensation to customers in such cases.

To Azerbaijan’s civil society
Take care to be aware and stay up-to-date on existing online threats facing members of Azerbaijan’s civil society and take appropriate measures to mitigate and minimize risks.

Improve digital hygiene and use up-to-date software on any devices used to connect to the internet.

To international companies selling surveillance technology
Refrain from selling surveillance technology to states such as Azerbaijan, where this technology is known to be used as part of government-led campaigns against dissent.

Provide public information about the types of surveillance technology sold to individual states.

To global social media platforms
Ensure that company policies are informed by adequate information about the country contexts in which the companies operate.

Ensure that mechanisms are in place to effectively and promptly respond to trolling and other coordinated attacks targeting platform users, and consider working with regional focal points and/or trusted partners to identify sources of threats, intimidation and attacks.

Develop procedures for reporting violations of community rules, copyright infringements and other violations, as well as for addressing such reports to prevent abuse of these procedures, in particular, by agents acting in the framework of government-coordinated attacks against dissidents.

To international institutions and foreign governments
Prominently and consistently raise concerns about violations of human rights online with the Azerbaijani government, including in specific individual cases of concern.

Help ensure accountability for foreign companies that export surveillance technology to Azerbaijan that is used to target opposition members, civil society activists and journalists for politically motivated reasons.

Help ensure that global social media platforms develop more effective policies for dealing with fake accounts, trolling and abuse of complaints mechanisms in countries such as Azerbaijan, where such problems are widespread.

Step up support to help protect Azerbaijan’s civil society from digital attacks.

To international civil society
Implement tailored programs to help protect Azerbaijani civil society representatives from online attacks and to assist those targeted by such attacks.

Continue monitoring the situation with respect to the protection of human rights online in Azerbaijan, and help local civil society actors to raise concerns about violations in this area and to engage in advocacy when and where relevant.