Digital Infrastructures in Afghanistan

By Sofie Flensburg, Signe Lai & Emilie Lehmann-Jacobsen

December 2024

IMS

Publisher
IMS (International Media Support)
March 2025

Editor:
Asha Mahadevan & Helle Wahlberg, IMS

Co-editor:
David Lush

Authors:
Sofie Flensburg
Signe Lai
Emilie Lehmann-Jacobsen

Report title:
Digital Infrastructures in Afghanistan

Published in Denmark by IMS in 2025

Cover image:
IMS

Layout:
Vitali Dzehtsiarou

ISBN
978-87-92209-34-4

IMS
Nørregade 18
1165 Copenhagen K
Denmark
+45 8832 7000
info@mediasupport.org

Join the global work for press freedom and stay up to date on media issues worldwide.

IMSforfreemedia
IMSforfreemedia
IMSInternationalMediaSupport
ims-international-media-support

IMS (International Media Support) is a non-profit organisation supporting local media in countries affected by armed conflict, human insecurity and political transition. We push for quality journalism, challenge repressive laws, and keep media workers of all genders safe so they can do their jobs. Peaceful, stable societies based on democratic values rely on ethical and critical journalism that aims to include, not divide.
www.mediasupport.org

IMS

Contents

Photo credit: Kaveh Kazemi / Getty Images

Introduction

When the Taliban (hereafter referred to as the de facto authorities, DFA) took over control of Afghanistan in 2021, they also gained control of a blossoming digital landscape. In contrast to their past position on the Internet and its connected services, the DFA chose to allow the Internet and even began to expand possibilities for connectivity in the country. New cables are currently being established and cell towers are being raised all over the country ("Afghanistan expands," 2024; Khawrin, 2023). This study maps the digital infrastructure in Afghanistan to understand how access to the internet has developed in the country, how it looks today and how it might look in the future. Furthermore, it probes ownership structures and control measures of the digital infrastructure to understand the extent of the DFA's powers over people's access to information and its abilities to track and surveil the population.

Using the methodology developed by assistant professors Signe Lai and Sofie Flensburg (2019) from the University of Copenhagen, this study traces the underlying infrastructures that allow – or constrain – individual Afghans' digital communications. We follow the bits of data as they travel from the end-user's device, through the local network services and central fibre highways to the servers of apps and websites as well as a multitude of potential third-party services. These services collect and distribute metadata on the user's behaviour, preferences, locations and much more. Through this approach, we identify the key components of the Afghan internet infrastructure, the actors who control them, and how they can enable and constrain basic human capabilities.

Afghanistan is an interesting case when it comes to digital infrastructure. As the following sections will explore, internet connectivity has been heavily marked by the years of war and conflict and shifting strategies of the DFA. Backed by foreign investments, the internet infrastructure has been built and expanded, thus allowing for an ongoing digitalisation with potential for both emancipation as well as repression. In other words, Afghanistan constitutes a core context for understanding how different parts of the digital infrastructure can be used as means of control and how this should be addressed in international development strategies. This study is, therefore, meant to inform international development agencies, non-governmental organisations (NGOs) and government institutions seeking to support Afghan citizens' digital access inside Afghanistan.

The mappings and analyses presented in this study are based on a comprehensive collection of data on internet use and other key indicators of digitalisation, on news articles and reports, and on journalistic research on current conditions for civilians in Afghanistan. As we discuss throughout the paper, statistical data is not always up to date. Sometimes, it is entirely absent. This not only exacerbates the general challenge of measuring the distribution of internet technologies and their use but also speaks to the important need for advancing methods and data sources for monitoring digitalisation, especially in development contexts.

1. The history of connectivity in Afghanistan

The history[1] of the internet in Afghanistan can roughly be divided into three phases:

- An early phase ranging from the 1990s up until the fall of the Taliban in 2001, characterised by very limited connectivity in the form of slow fixed dial-up connections, first-generation mobile networks, occasional satellite links established by NGOs and United Nations agencies, and a general ban on the internet.

- A post-Taliban era from the early 2000s to the regime reclaiming power in 2021, characterised by attempts to rebuild and expand network access for military as well as humanitarian purposes through international funding and development projects.

- The last stage of internet connectivity taking off in 2021 when an increasing number of Afghans seemed to have gained some sort of internet access, partly due to a growing interest from the Taliban in building and improving digital infrastructure in the country.

The timeline below shows cornerstone moments in this overall development.

Following the fall of the Taliban in 2001, the first official internet connection was announced in Afghanistan in 2002 with the launch of the first internet café in the Kabul Intercontinental Hotel later the same year (Wentz et al., 2008). In its wake, various institutional arrangements were put in place to formally administer the .af domain and license the first Internet Service Provider (ISP) in 2003 (ibid.).

In the following years, various international investments were made to rebuild and expand the Afghan telecommunications infrastructure, including the Nato-funded Silk Highway project to ensure high speed internet and global connectivity to Afghan universities, first through a satellite connection and later fibre-optic cable

1 The first two phases are outlined in Wentz et al., 2008.

2001 US-led invasion of Afghanistan removes the Taliban from power

2002
First Internet connection in Afghanistan. Afghan Wireless (AWCC) opens first Internet Cafe in Kabul Intercontinental Hotel in July.

2003
.af domain is introduced and the Afghanistan Network Information Center (AFGNIC) is established to administer domain names; licensing of the first Internet Service Provider (ISP)

2004
The Virtual Silk Highway project, a Nato project, includes Kabul University (Nato, 2015)

2006
In November 2006, the MCIT contracted the Chinese firm ZTE to establish a fibre-optic cable network in Afghanistan, the "Optical Fibre Cable Backbone Ring" (MCIT, 2005)

(North Atlantic Treaty Organisation [Nato], 2015). Afghanistan's access to the internet was further strengthened in 2006 with a fibre cable ring which increased network capacity (Ministry of Communication and IT [MCIT]), 2005). Since then, several initiatives were taken which expanded and improved mobile networks. This helped mobile communication to increase significantly in the 2010s (Lakshmanan, 2010).

The 2021 withdrawal of US forces and the takeover by the Taliban severely damaged the communications infrastructure and shut down local networks (Kumar, 2021). In the past three years, the regime has shown a growing interest in rebuilding and improving connectivity throughout the country and is encouraging foreign infrastructure investments ("Afghanistan expands," 2024). Despite its growing push for digitalisation, a number of digital services continue to be banned or blocked, including the social media platform TikTok due to fears that it will "mislead" young users ("Afghanistan: Taliban orders," 2022).

The most striking change during the current period is the DFA's strategy towards the internet: from restricting and prohibiting public internet usage in its first period in power to actively encouraging and facilitating citizen digitalisation through recent years' buildout of internet infrastructure and launch of digital services and media. This should be seen in the light of a recent and broader rise in digital authoritarianism (Shahbaz, 2018) where repressive regimes use the internet to surveil and sanction citizens and social movements, control data traffic, spread propaganda and dis-/misinformation, and so forth. The DFA's renewed interest in the internet triggers a dilemma for international development projects which previously focused on the emancipatory potential of increasing connectivity: should projects be supported which enhance people's access to the internet and its connected services such as social media platforms if the technologies to access them are used for surveillance and to sow distrust and spread disinformation?

2021 US-forces leave Afghanistan; The Taliban take over, infrastructures are damaged as part of conflict, but rebuilt to secure Taliban connections

2010 SILK-Afghanistan is launched to provide connectivity initially to 11 universities and several governmental institutions (Nato project)

2013 Arrival of 3G

2017 Arrival of 4G

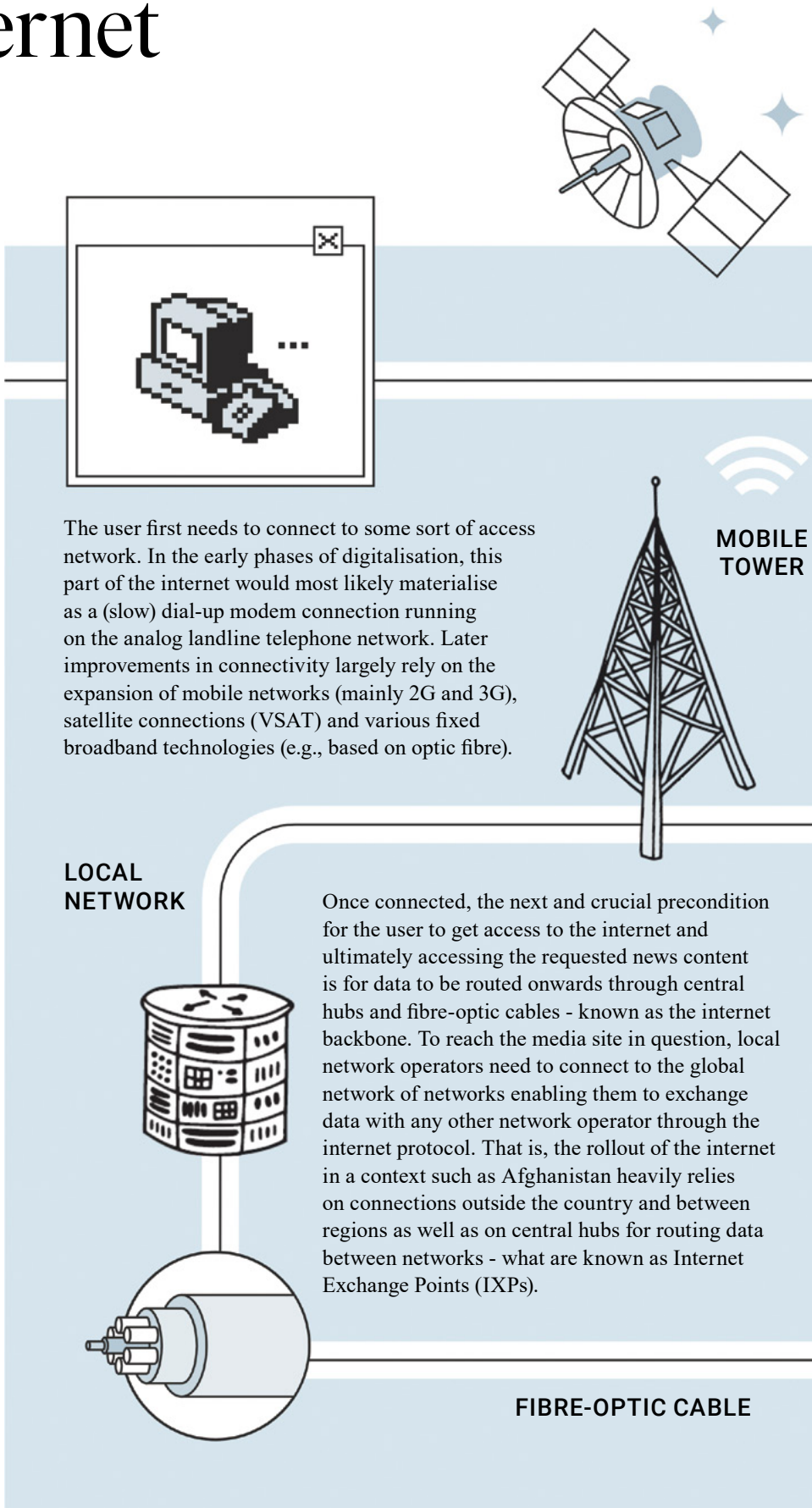
2022 Taliban bans TikTok

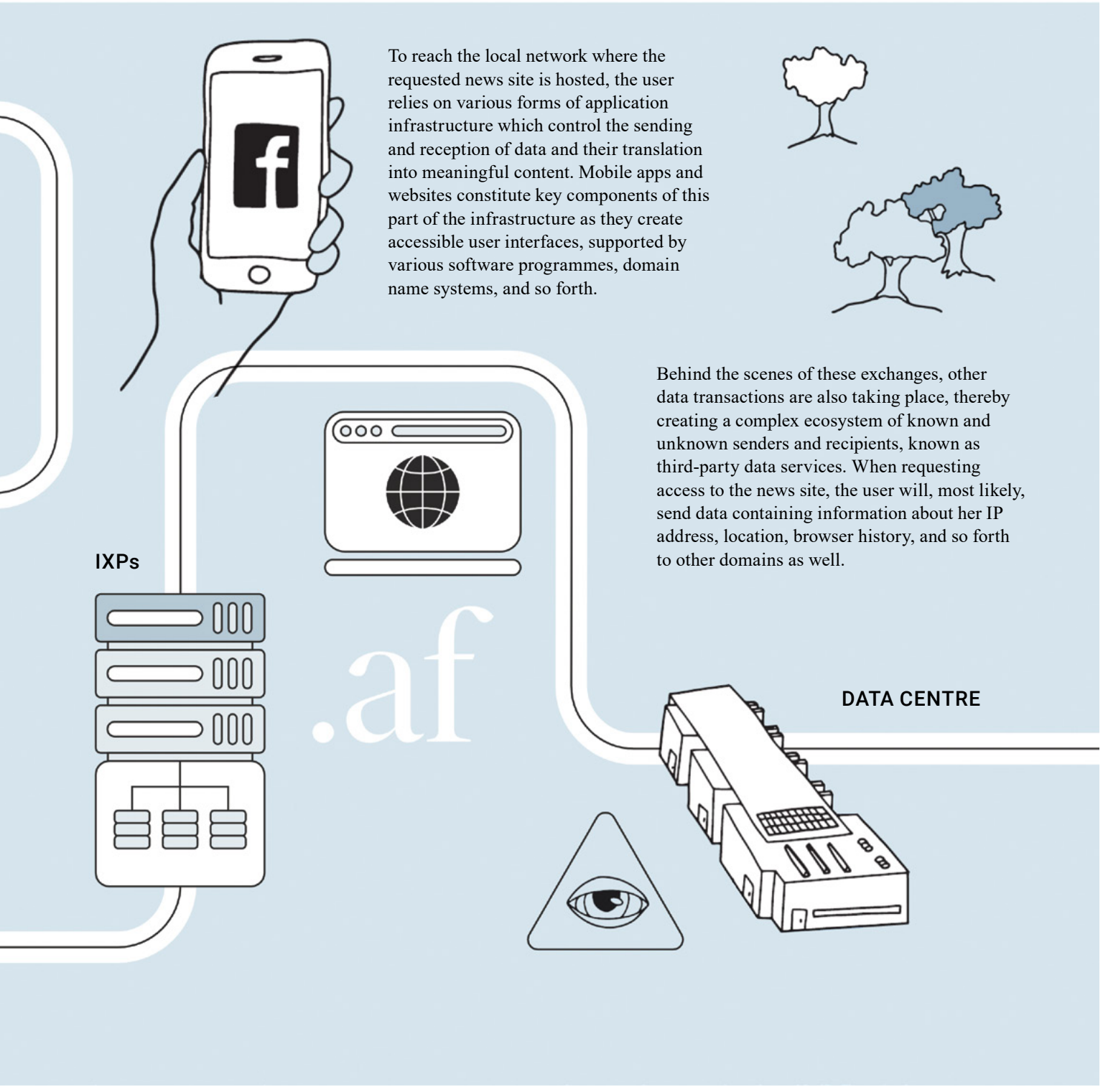
2. Architectural organisation of the internet

To further understand this dilemma, we need to delve deeper into the architectural organisation of the internet and its different levers of control. A better grasp of the various components will help us create a knowledge foundation that can be used to develop solid strategies for improving the living conditions and security of Afghan citizens.

To outline the basic and critical components of the digital infrastructure, we trace the chain of technologies required for any type of internet-based activity to take place. That is, for instance, when a user wants to check the news on a digital media site, the following steps have to take place.

The following chapters 3 - 6 provide a closer look into these four key layers of the internet infrastructure to discuss how the Taliban can (and do) control them.




To reach the local network where the requested news site is hosted, the user relies on various forms of application infrastructure which control the sending and reception of data and their translation into meaningful content. Mobile apps and websites constitute key components of this part of the infrastructure as they create accessible user interfaces, supported by various software programmes, domain name systems, and so forth.
Behind the scenes of these exchanges, other data transactions are also taking place, thereby creating a complex ecosystem of known and unknown senders and recipients, known as third-party data services. When requesting access to the news site, the user will, most likely, send data containing information about her IP address, location, browser history, and so forth to other domains as well.
IXPs
.af
DATA CENTRE

3. Accessing the Afghan internet

While there are clear indications of a significant rise in connectivity in Afghanistan, the exact extent of internet penetration is very difficult to determine since data is scarce and sometimes contradictory. The official global monitoring authority, the International Telecommunication Union[2] (ITU), has limited up-to-date information on internet usage. Its latest statistics are from 2019 (i.e. before the takeover by the DFA) and state that 17.6% of the population reports to have been online within the last three months. Statistics published by DataReportal[3] suggests that internet penetration has increased slightly to 18.4% in 2024. Mobile telephony is much more widespread compared to internet connections with 27.67 million active cellular mobile connections, according to DataReportal (Kemp, 2024), which is equivalent to 64.6% of the total population.[4]

Although internet usage is unevenly distributed across urban and rural areas, social groups (with around one third of the population being illiterate), and between genders (with women generally having less access than men), most reports suggest that the growth in internet usage may be higher than statistics show. A recent audience study by the BBC Media Action (Zaki et al., 2023) shows that 36% of participants report having access to the internet at home or elsewhere with significantly higher numbers among the 15–24-year-olds (59%), urban (50%), and educated (74%) parts of the population. The DFA reported an internet penetration rate of around 25% to Bloomberg in 2022 (Tarabay & Najafizada, 2022).

Looking at the network infrastructure supporting internet usage, data from the World Bank (2024) shows a very limited number of fixed broadband subscriptions (0.08 per 100 inhabitants in 2023). This suggests that few Afghans access the internet through a wired connection (e.g., based on optical fibre, cable, or copper). Although public wifi might be an option in urban areas and universities, mobile data (on subscription or prepaid) is commonly used to access the internet. In 2022, the DFA announced that it was going to upgrade the 4G network (Rabie, 2022). Yet, most Afghan connections continue to rely on 2G and to a smaller degree on 3G and 4G with prices well above the world average, according to the International Telecommunication Union (2024).

According to the Taliban-led Afghan Ministry of Communications and IT (MCIT), this critical 'last mile' of the internet infrastructure is operated by 63 different internet service providers (ISPs). Of these, Afghan Wireless (AWCC) - a joint venture of Telephone Systems International and the Afghan Ministry of Communications - is the largest, supplying more than 5 million customers, from individuals and government entities to businesses and organisations in all 34 provinces (Afghan Wireless, 2024). The United Arab Emirates-owned ISP, Etisalat, Afghan Roshan, and South African MTN are amongst other key ISPs (the latter announced its withdrawal from the country after the 2021 takeover but, to the best of our knowledge, has refrained from leaving).

2 ITU is the United Nations specialised agency for information and communication technologies (ICTs). The organisation is made up of 194 Member States and more than 1000 companies, universities and international and regional organisations. The ITU allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies connect seamlessly, and works to improve access to digital technologies in underserved communities worldwide.

3 Published by private analytics company Kepios.

4 It is, however, important to note that some users might have more than one mobile subscription.

5 Statements taken from ATRA's own webpage, https://atra.gov.af/who-we-are.

Equipment in server room. Photo: Erik Isakson / Getty Images

The degree of state involvement in the ISP market and individual network operator activities is difficult to assess. Yet, recurrent network shutdowns during and following the Taliban takeover suggest that the regime - despite the large number of market actors - exerts some form of control on this part of the infrastructure. While we have not been able to find concrete evidence of how this influence is enforced in practice, the Afghanistan Telecom Regulatory Authority (ATRA), functioning under the MCIT, describes that its key function "is to oversee and control the activities of its licensees to make sure all services provided are in line with laws and regulations of the country" and to identify "illegal and ineligible activities conducted by individuals or other entities".[5]

Access networks, thus, constitute a central lever of internet control in Afghanistan as well as everywhere else, as they directly enable or constrain users' ability to go online. The shutdown of local networks is a method used frequently by authoritarian regimes to restrict users' ability to communicate and obtain information in times of conflict (Björksten, 2022). Prior to 2021, the DFA had "a history of targeting telecommunications infrastructure and later mobile-phone towers which forced mobile companies to shut or limit their coverage" (Stokel-Walker, 2021). During the takeover, shutdowns of mobile networks were a clear instrument to stop the spread of information, to stop protests, and ultimately, to prevent Afghans from leaving the country. According to activists and human rights organisations, the regime continues to use local network shutdowns to limit protests and reporting on violence.

While shutdowns are an effective way of directly blocking all online activities, access network infrastructure can also be used for other means of power exertion including the blocking of particular domain names and IP addr esses. Another common use is the extraction of individuals' network traffic, location data, and so forth – which is often used for prosecution purposes. As such, measurements of connectivity in the form of internet subscriptions and active users should be seen not only as indicators of improved communication rights, access to information and freedom of expression, but also as potential instruments of new forms of power exertion.

4. The backbone of digital communication

Apart from the last mile of the internet outlined above, another precondition for online communication is the routing of data traffic between different access networks. This has been a key priority for the Afghan State both before and after 2021. The reconstruction and expansion of terrestrial fibre highways within and outside the country has received significant investments and at the time of writing this report, a multitude of connections are being built. While this backbone of the internet and its control mechanisms are highly black-boxed and opaque – not only in Afghanistan but globally as well – we can sketch out its contours in Afghanistan using public databases and registers.

According to the International Telecommunication Union (2024), Afghanistan has a total of 5,078 kilometres of optical fibre spanning 91 cables that are in operation as of 2024, while 4,116 kilometres are either planned (17 cables) or under construction (three cables). The existing cables were established in a grand digital infrastructure project called Optical Fibre Cable Backbone Ring, which ran from 2006 to approximately 2016. The project forms a ring-shaped network running from Kabul over Kandahar to Herat and Mazar and back to Kabul, connecting more than 20 provincial capitals in the process. The ring has been a catalyst for the growth of the Afghan internet and connectivity rates over the past 10 years (Madoury, 2021). The new and planned cables are meant to connect other and more remote regions to the Optical Fibre Ring. These regions include centrally-located and mountainous provinces as well as regions in the North-East. None of these regions have ever been connected through fibre networks.

The initiatives taken by the DFA since the 2021 takeover to expand the country's fibre optic networks are a testament to the regime's new stance on digital infrastructure buildouts. The 20 new cables that are either in the planning stage or under construction will ensure digital communication paths to provinces that have thus far been difficult to reach, even with radio communication, due to the mountainous landscape. The length of the cables is almost equivalent to that of the existing fibre networks, thereby signifying an infrastructure project of considerable scale. In December 2023, the Taliban-led Afghan Ministry of Economy issued a directorate to local and foreign non-governmental organisations stating that they should "refrain from allocating projects and budgets specifically for [...] public awareness projects, peace consolidation, advocacy and conflict resolution" and instead allocate funding for "infrastructure projects" (Ministry of Economy, 2023). While this includes all types of infrastructures including roads and electrical grids, the cost of expanding the fibre-optic backbone ring has previously been estimated at $40 million (MCIT, 2015). It has, however, not been possible to determine precisely who is funding these expansions or who will own the cables after they are installed.

Figure 1: The two maps show respectively the current optic fibre cables that amount to a total of 5,078 km (map 1), and then the ones that are either under construction (marked with yellow) or planned (marked with stippled lines) that amount to 4,116 km (map 2), predominantly in central provinces. Source: https://bbmaps.itu.int/bbmaps/.

The Afghan internet is connected to the global internet through its neighbouring countries Iran, Pakistan, Turkmenistan, Tajikistan and Uzbekistan. Two cables are run by foreign telecommunications operators (the Pakistani PTCL and the Turkmenian GKE Turkmentelecom), while the remaining 89 are operated by the MCIT. This means that the state handles all data traffic between network operators within the country as well as the majority of international traffic(!). Moreover, Afghanistan has one single Internet Exchange Point (IXP) facility, where traffic is exchanged between disparate networks. It is called NIXA and is located in Kabul. This too is controlled by the MCIT (PeeringDB, 2024).

With the Afghan State operating the vast majority of backbone infrastructure in the country as well as connections to the global internet, the DFA have significant clout when it comes to internet control. There is and have been regular targeted shutdowns of the internet both nationwide and in particular regions as a means for the DFA to strike down on protests and prohibit media reporting. While access network companies can shut down local communities and block specific web domains (websites and apps), backbone operators can potentially cut Afghanistan off from the outside world – i.e., the global internet. As all services - from platforms to media - rely on fibre highways and internet exchange points for transporting data, backbone providers - in this case the DFA through their control of the MCIT - have the power to incapacitate the services. They do this by cutting key distribution routes via so-called internet kill switches that are located in this part of the infrastructure.

5. Information interfaces and communication services

The next level to analyse comprises the applications and platforms used to access the internet. Technically speaking, websites and mobile apps function by translating data packages transmitted through access and backbone networks into comprehensible content for the user while also breaking user requests down to data. The infrastructural elements involved in these transactions include hosting services (called cloud solutions), domain name systems, operating systems, browsers and app stores. All of them allow data to be stored and processed at the edges of the network. This part of the internet infrastructure is thereby critical for the production and distribution of information. Analysing this layer not only provides us with information on how people actually use the internet, but also allows us to further understand how the DFA might use the internet and underlying digital technologies to their advantage.

As with the backbone layer, monitoring of application infrastructure is highly limited. There are no official lists which show, for instance, the national usage of website domains and mobile apps or the underlying infrastructures they depend on. This section, therefore, relies on various data sources (such as commercial databases that are often unclear in their methodological descriptions and developed for purposes other than research) to provide insights into the application layer in Afghanistan. According to GlobalStats (2024), Alphabet (Google's parent company) dominates the operating system market with Android holding a 78% market share. Apple comes in second with 9.6% and Windows is third with 8%. As for the browser and app store markets, Alphabet dominates with 84% of global internet users using the Chrome browser and Google Play being the dominating app store.

When investigating the most used apps and websites in Afghanistan and comparing the various available data sources (such as online web traffic companies Semrush[6] and Ahrefs;[7] top lists from app stores and self-reported platform usage from audience studies[8]), it is clear that social media and messaging services such as Facebook, YouTube, TikTok, Instagram, Telegram and WhatsApp are popular platforms. However, the lists also contain online versions of the Qur'an, VPN apps, proxy browsers and video editors. Furthermore, we find local apps from telecom companies (in particular, AWCC) for topping up prepaid phones and wiring funds to friends and family members. Finally, we have observed an increase in online stores - particularly Chinese stores such as Temu and Shein.[9] It is interesting to note that circumvention tools (such as VPN apps and proxy browsers) and TikTok, which is banned in Afghanistan, are among the most popular apps. This shows that at least some Afghans attempt to circumvent the controls of the DFA and access content that is deemed improper by the regime. The fact that platforms such as Facebook and WhatsApp continue to remain on lists of most downloaded apps in app stores also indicates that there continues to be an increase in the number of people getting devices to access the internet. These apps would not be on the lists of most downloaded apps if people already had them on their devices. This corresponds well with the DFA's ambitions of ensuring better access to the internet for people living across the country.

As is visible from the breakdown described above, international companies own and control the majority of the most used application infrastructure in Afghanistan. Facebook remains the most used social media platform; YouTube is the most used platform for streaming of videos and Google is the most used search engine. People's access to information online in Afghanistan is, thereby, to a large degree, predetermined by these companies and their products' algorithms that dictate what is accessible to the individual. However, there is an additional layer on top of and interwoven with the application layer. The DFA have, from the beginning of their takeover, attempted to control people's access to information by also meddling with the application layer. First, they took over control of the .af domain that had previously been handled by a US and a Czech registrar (Stokel-Walker, 2021). New policies for registrations of domains were made which resulted in some webpages losing their domains and more colourful domains such "broke.af" and "queer.af" going offline (Satter, 2024). In connection to this

6 https://www.semrush.com/
7 https://ahrefs.com/
8 Such as Zaki et al., 2023.
9 On a side note, the increase in online Chinese shopping platforms could be related to the inflow of Chinese workers in Afghanistan following new China-Afghanistan business agreements.

takeover of Afghan domains, the DFA similarly began to block and restrict access to websites with content deemed "immoral" in the eyes of the regime. In 2022, they reported to have blocked about 23 million websites (Tarabay & Najafizada, 2022) including international media, civil society organisations and local independent media. This blocking is most likely taking place through the ISPs using so-called blacklists that deny access to domains on the lists; again, testifying to the control that can be exerted through the access network layer.

While it is very difficult for governments to exercise power over the major tech companies behind platforms such as Facebook and Google, the DFA have, like most other authoritarian regimes, attempted to limit the reach of these. In 2022, they announced the first ban of apps by banning both the popular TikTok and an online multiplayer game PUBG ("Afghanistan: Taliban orders", 2022). Later, the regime attempted to ban Facebook pages of foreign media such as BBC and CNN; however, without much success. In 2024, they also announced plans to block Facebook entirely (Rai, 2024). Taliban spokesman Zabihullah Mujahid later changed this stance in an interview with Committee to Protect Journalists by saying, "Facebook will not be banned, but restrictions will be imposed on it." (Committee to Protect Journalists, 2024, para 6). In general, the DFA seem to have somewhat of a love-hate relationship with the major social media platforms: from completely denouncing the use of social media and the internet to gradually embracing them as useful tools for spreading propaganda. Most of the platforms have responded to the DFA's use of social media by limiting their reach and deplatforming their official accounts (Shead, 2021). However, following the Taliban takeover, Facebook made certain exemptions: such as permitting a handful of Afghan ministries to maintain their profiles even under Taliban leadership and share content via the social media platform (Biddle, 2021).

One could question why the DFA have not just banned all international platforms from Afghan servers, since doing so would allow them to fully control people's access to information. The answer is probably that an overarching ban would not be in their best interests. The DFA rely on the platforms to distribute their content. And they - as all other information providers - need to go where audiences are if they want to catch their attention. Like other authoritarian regimes, the DFA also use the platforms to influence public opinion in more covert ways. While people in Afghanistan might be accustomed to propaganda coming from official sources, they are less experienced when it comes to recognising propaganda or mis/disinformation stemming from sources that do not appear to be the DFA. As an Internews study analysing mis- and disinformation in Afghanistan concluded, the Taliban's use of disinformation "is a strategic tool designed to control the narrative, consolidate power, and seek legitimacy" (Internews, 2024, p. 12). And for this purpose, they are heavily dependent on the existing social media platforms, where the tech companies struggle to remove deceptive or false content.

6. The data ecology

Lastly comes the data layer. For the purposes of this analysis, this layer refers to the presence of third-party services that support first party applications in understanding their users, storing and distributing content, selling targeted ads and, increasingly, keeping track of users. Though often hidden and opaque, third-party technologies constitute a critical part of the digital infrastructure and market since most applications are both functionally and commercially dependent on externally-provided tools and services. The technologies and market actors involved in these activities can be identified by reverse engineering and unpacking specific websites and apps. However, the tools for doing this are developed in and for a Western context and they are not yet designed to capture important third-party services operating in and perhaps from Afghanistan. The tools are most likely to miss these third-party services. For this reason, this section does not provide an exact account of the current realities in third-party infrastructures and trackers in Afghanistan; instead, it will give an indication of the kinds of technologies that are present as well as how they can be mobilised by the DFA.

While the previous section describes the challenges related to composing lists of most used applications - from websites to apps and web apps - there are other, related bumps on the road towards researching the kinds of third-party actors involved in the Afghan application ecosystem. First, third-party services are not the same across applications - the technologies differ and can do different things. An example: websites rely on cookies to track their user base. Cookies can relay information on where the user came from and goes to online (i.e. their browser history), IP address, device IDs and so forth. The equivalent technology in apps - called software development kits (SDKs) - can access a suite of other kinds of information that are also related to the mobile device which runs the app - including contacts, images, GPS location, and the phone's camera and microphone. In other words, the level of information to be gathered by third-party actors inside digital applications varies considerably depending on the kind of application. The possibilities for analysing and engaging with them vary as well: tools developed for reverse engineering applications so that we can investigate, for instance, the cookies they embed, or the SDKs they use, depend on libraries of known third-party trackers to which they then compare the data. This means that the analysis is only as good as the library of known trackers, and as of now, these are quite Western-centric and do not account for local Afghan actors (if they exist).

When we look under the hood of the most used applications in Afghanistan and the kinds of third-party actors they depend on for their services, we find a large bulk of the "usual suspects" in tracking from Silicon Valley (see Figure 2). These are actors like Facebook and Google who have excelled at building a business around user data, targeted advertising, and personalisation. Some of their most used third-party trackers - like Google Analytics for analysing users to one's website or app and Facebook Ads for delivering targeted ads - are present across the vast majority of the most popular outlets. However, we also see prominent Chinese and Russian trackers including Huawei Core Services, Yandex Ads and VKontakte among the third-party trackers installed in the most used applications in Afghanistan. This is most likely the result of Russian and Chinese presence in the country and the latter's involvement in infrastructural projects and investment in the country.

While we cannot detect all third-party trackers specifically developed for and distributed by the DFA with the methods currently available, we can see that the third-party trackers that we can detect access a wide suite of user information that can, in turn, be accessed by the DFA. One frequently used app, the Pakistani Qur'an app called Quran Majeed, for instance, accesses several sensitive data

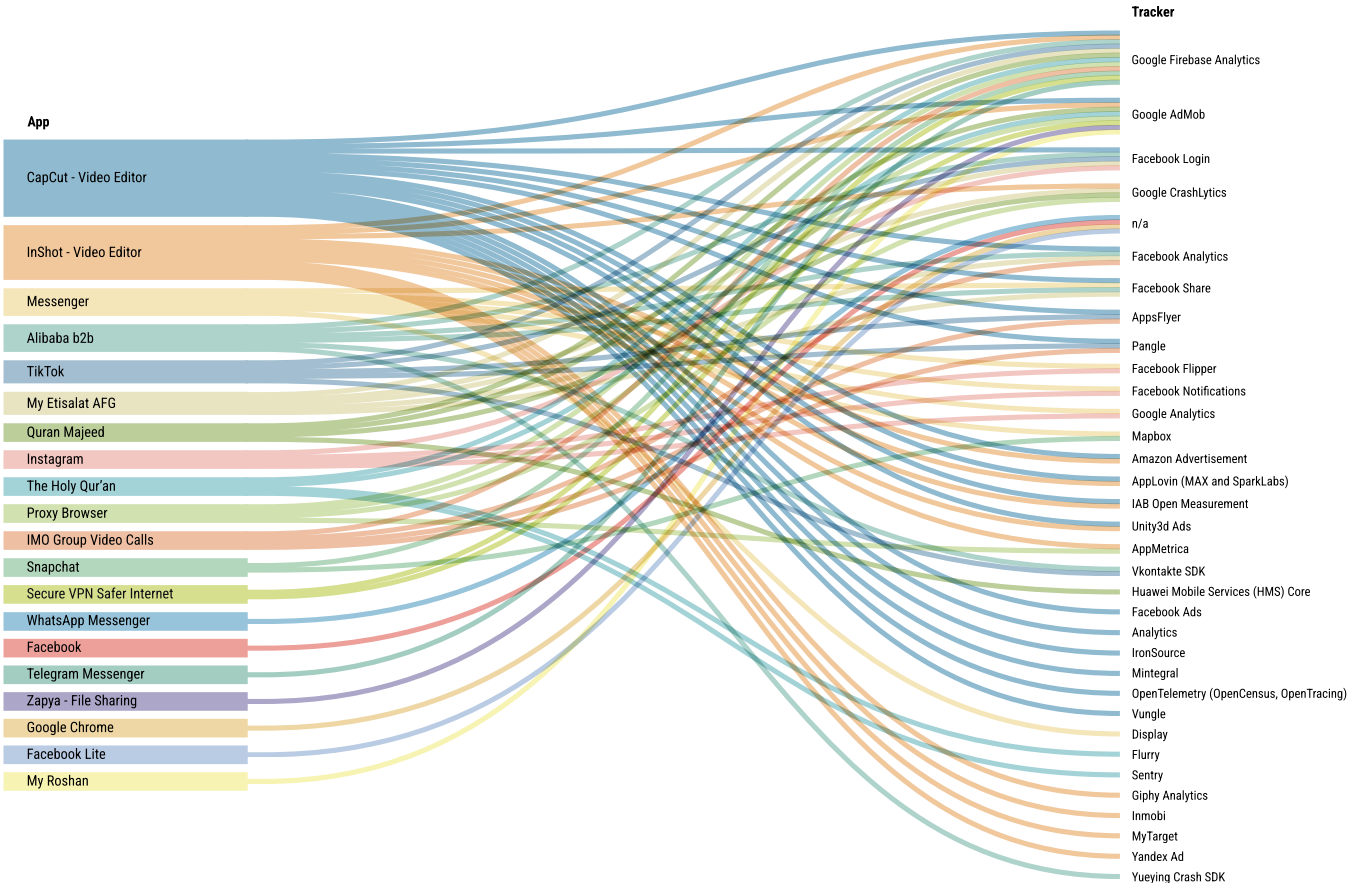


Figure 2: 20 popular Android apps figuring in the Exodus Privacy database. The chart shows which third-party technologies (right) receive information when a user in Afghanistan uses the popular apps (left). The CapCut – Video Editor, that has the most trackers, is owned by ByteDance, TikTok's parent company.

including location, phone storage (e.g., images), and sound recording through the microphone. The third-party services accessing this user information are, as far as our analyses show, strictly US tech companies; yet, as mentioned above, we cannot know if there are actors from Pakistan embedded too.

The reason why we should pay attention to this layer is of course due to safety concerns. If the DFA can access tracking data on people through their use of apps, then they would have stronger means to target people opposing their regime. We are, however, at this point not certain about the extent of the DFA's capabilities in this regard. While there is no doubt that they have a completely different approach to the internet, social media and digital infrastructure in 2024 compared to the last time they were in power, we do not know their skill levels in accessing and utilising the data that they might have access to. Nonetheless, there are many reports of the much more analog techniques for gathering information. The DFA are known to routinely confiscate people's phones and check them for any kind of sensitive information or illegal content. Moreover, the mere fear of the Taliban being able to monitor browser history or network traffic compels many Afghans to refrain from carrying their phones with them when leaving their homes and being extra careful when accessing banned web pages and apps - something that was also visible in our analysis of the application layer where VPNs rank highly.

7. The promises and pitfalls of Afghan connectivity – conclusions and perspectives

The internet used to be seen as a threat to authoritarian or military regimes as it held emancipatory and democratic potential in presenting opportunities for reaching out to the outside world or mobilising within a specific context. From an authoritarian perspective, it was something to be dismantled or shut down entirely. But these days, the internet is increasingly seen as a tool for oppression and spreading propaganda (much like other communication technologies before it – e.g. press, radio and television), with China and Russia leading as examples for other countries. This is true also in conflict zones, where the destruction of internet technologies was a priority but is now increasingly being replaced by strategies wherein internet technology takeover is used proactively,[10] enabling further control and surveillance of territories.

As such, internet connectivity constitutes an increasingly ambiguous privilege in unstable and authoritarian regimes. While holding a lot of potential for emancipation – e.g., increasing access to information, providing platforms for public debate, facilitating social mobilisation, etc. – internet usage also entails several risks as regimes become increasingly aware of how it can be used to spread and monitor online content, track user behaviour and locations, shut down networks or redirect data flows.

Building on the findings outlined in this paper, development initiatives should pay critical attention to the Taliban's recent investments in and potential requests for aid aimed at developing the country's digital infrastructure. As seen in other contexts (e.g., Myanmar), network buildout and the subsequent uptake of internet services entails significant data collection that can be used to persecute and sanction civilians. Furthermore, the more digitised a society is, the more severe are the consequences of recurrent shutdowns of local networks and web domains. That is, the more people depend on the internet for everyday activities, the more critical are the shutdowns and limitations of the infrastructure supporting these activities.

There is also a need to critically reflect on how to ensure that efforts to reach Afghan audiences using online platforms and digital technologies do not cause harm to them but are supported by relevant measures to safeguard users and enhance their digital literacy levels. While we still have limited information on the DFA's capabilities in surveilling the Afghan population online and accessing sensitive data, there is no doubt that the DFA have the means within their reach should they choose to use them. In order to ensure that audiences can circumvent blocking and tracking tools, access independent information and navigate hostile online information environments, development efforts should prioritise online safety and security, critical thinking and the promotion of platforms and channels for easy and safe access to relevant and reliable information.

With the DFA having embraced online spaces and digital technologies as efficient tools for maintaining control of the population, development efforts with ambitions to secure basic human rights and fundamental freedoms should similarly pay attention to these realms. The story is still being written and the infrastructure is currently under development but soon, even the online spaces will be too difficult and dangerous for the public at large to manoeuvre unless they do it on the DFA's terms.

10 One such example is Russia taking over control of the Internet in occupied areas of Ukraine. Both by channelling internet traffic through Russian providers but also by forcing people to replace SIM cards in their phones to Russian cards – and thereby subjecting Ukrainians to Russia's censorship and surveillance machine (Burgess, 2022).

References

Afghanistan expands fiber optic services to 26 provinces. (2024, June 18). *TOLOnews*. https://tolonews.com/afghanistan-189323

Afghanistan: Taliban orders TikTok, PUBG ban for 'misleading youths.' (2022, April 22). Retrieved from https://www.bbc.com/news/world-asia-61185931

Afghan Wireless. (nd). About us. Retrieved August 7, 2024, from https://afghan-wireless.com/about-us/

AWCC opens 4G internet services for first time in Afghanistan. (2017, May 4). Retrieved from https://www.ariananews.af/awcc-opens-4g-internet-services-for-first-time-in-afghanistan/

Biddle, S. (2021, November 23). Facebook grants government of Afghanistan limited posting rights. *The Intercept*. https://theintercept.com/2021/11/23/facebook-afghanistan-taliban-exception/

Björksten, G. (2022, June). *A taxonomy of internet shutdowns: The technology behind network interference.* Access Now. https://www.accessnow.org/wpcontent/uploads/2022/06/A-taxonomy-of-internet-shutdowns-the-technologies-behind-network-interference.pdf

Burgess, M. (2022, June 15). Russia is taking over Ukraine's internet. *Wired*. https://www.wired.com/story/ukraine-russia-internet-takeover/

Committee to Protect Journalists. (2024, April 8). *CPJ calls on Taliban to drop plans to restrict Facebook access in Afghanistan*. https://cpj.org/2024/04/cpj-calls-on-taliban-to-drop-plans-to-restrict-facebook-access-in-afghanistan/

Flensburg, S., & Lai, S. S. (2019). Mapping digital communication systems: Infrastructures, markets, and policies as regulatory forces. *Media, Culture & Society*, 016344371987653. https://doi.org/10.1177/0163443719876533

GlobalStats. (2024). *Social media stats Afghanistan*. Retrieved August 7 2024, from, https://gs.statcounter.com/social-media-stats/all/afghanistan

International Telecommunication Union. (n.d.) *Broadband Maps: Afghanistan Fiber Backbone Overview.* [Map] Retrieved May 10, 2024 from https://bbmaps.itu.int/bbmaps/

International Telecommunication Union. (2024). *DataHub - Afghanistan*. Retrieved 7, 2024 from, https://datahub.itu.int/data/?e=AFG

Internews. (March 2024). *Understanding and addressing mis-/disinformation in the Afghan ecosystem*. https://internews.org/wp-content/uploads/2024/06/AF-Disinfo-Report-Layout-Mar2024_Edit.pdf

Kemp, S. (2024). *Digital 2024: Afghanistan*. DataReportal. https://datareportal.com/reports/digital-2024-afghanistan

Khawrin, I. (2023, May 26). 44 new cell towers to be erected in the Northern Zone: ATRA. *Pajhwok Afghan News*. https://pajhwok.com/2023/05/26/44-new-cell-towers-to-be-erected-in-northern-zone-atra/

Kumar, R. (2021, July 15). Taliban targeting Afghanistan's crucial power, IT infrastructure. *Al Jazeera*. https://www.aljazeera.com/news/2021/7/15/taliban-afghanistan-it-electricity-power

Lakshmanan, I. A. R. (2010, March 23). Fighting the Taliban with cellphones. *New York Times*. https://www.nytimes.com/2010/03/24/world/asia/24iht-letter.html

Madoury, D. (2021, August 31). What's next for the internet in Afghanistan? *Kentik.com*. https://www.kentik.com/blog/whats-next-for-the-internet-in-afghanistan/

Ministry of Economy, Islamic Emirate of Afghanistan. (2023, December 30). *Directorate of non-governmental organisations (NGO).* Unpublished document.

Ministry of Communications and IT, Afghanistan. (2005). National optical fiber backbone. https://web.archive.org/web/20170509094540/http:/mcit.gov.af/Content/Media/Documents/englishletter13620111012123375533325325.pdf

Ministry of Communication and IT Afghanistan. (2015, June 16-17). Presentation by MCIT on Afghan Fiber Optic Ring [Conference presentation]. Practical steps towards a knowledge-based economy, Dushanbe, Tajikistan. https://www.unescap.org/sites/default/files/Presentation%20by%20MCIT%20On%20fiber%20connectivity%20in%20Afghanistan.pdf

North Atlantic Treaty Organisation. (2015, May 20). *SILK-Afghanistan: 10 years of promoting internet connectivity in Afghanistan*. https://www.nato.int/cps/en/natohq/news_120114.htm?selectedLocale=en

PeeringDB. (2024). NIXA. Retrieved August 7, 2024, from https://www.peeringdb.com/ix/2245

Rabie, P. (2022, August 31). Taliban claims it's upgrading Afghanistan to 4G despite ongoing online censorship. *Gizmodo*. https://gizmodo.com/taliban-internet-4g-afghanistan-1849478980

Rai, A. (2024, April 9). Taliban announce plans to block access to Facebook in Afghanistan. *The Independent*. https://www.independent.co.uk/asia/south-asia/taliban-facebook-ban-afghanistan-cpj-b2525668.html

Satter, R. (2024, February 16). "broke.af" goes offline as Afghan web domains suspended amid payment dispute. *Reuters*. https://www.reuters.com/technology/brokeaf-goes-offline-afghan-web-domains-suspended-amid-payment-dispute-2024-02-16/

Shahbaz, A. (2018). *Freedom on the net report 2018: The rise of digital authoritarianism*. Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Shead, S. (2021, August 17). Facebook, TikTok won't lift ban on posts that promote Taliban after the fall of Afghanistan. *CNBC*. https://www.cnbc.com/2021/08/17/taliban-content-banned-on-facebook-instagram-whatsapp.html

Stokel-Walker, C. (2021, September 7). The battle for control of Afghanistan's internet. *Wired*. https://www.wired.co.uk/article/afghanistan-taliban-internet

Tarabay, J., & Najafizada, E. (2022, August 31). Taliban continues censorship, web blocks as it promises 4G. *Bloomberg News*. https://www.bloomberg.com/news/newsletters/2022-08-31/taliban-continues-censorship-web-blocks-as-it-promises-4g

Wentz, L., Kramer, F., & Starr, S. (2008). *Information and communication technologies for reconstruction and development: Afghanistan challenges and opportunities.* Center for Technology and National Security Policy, National Defense University. https://www.files.ethz.ch/isn/134903/DTP%2045%20Afghan%20ICT.pdf

World Bank. (2024). *Fixed broadband subscriptions (per 100 people) – Afghanistan*. https://data.worldbank.org/indicator/IT.NET.BBND.P2?locations=AF

Zaki, M., Modaqeq, Z., Torab, S., Howie, F., Gautham, M., & Jabarkhail, I. (2023). *A survey of media consumption in Afghanistan*. BBC Media Action. https://www.bbc.co.uk/mediaaction/documents/media-consumption-in-afghanistan-survey-report-final.pdf

IMS

Good Journalism. Better Societies

IMS is a non-profit organisation working to support local media in countries affected by armed conflict, human insecurity and political transition. *www.mediasupport.org*

CONTACT
info@mediasupport.org

VISIT
www.mediasupport.org

CONNECT
IMSforfreemedia
IMSforfreemedia
IMSInternationalMediaSupport
ims-international-media-support