JUSTICE FOR MYANMAR

REPORT

Silk Road of Surveillance:

The role of China's Geedge Networks and Myanmar telecommunications operators in the junta's digital terror campaign

Justice For Myanmar is a covert group of activists using research, data visualisation and reporting to expose the companies and criminals profiting from brutality, war crimes and mass-scale suffering.

justiceformyanmar.org

2025 | Myanmar

Executive Summary.....1

The Myanmar junta's terror campaign online 3

What is Geedge Networks?.....7

The Myanmar junta's implementation of China's "Great Firewall”.....9

Telecommunications companies in Myanmar implementing mass surveillance for the illegal junta.....15

Legal Findings.....30

Recommendations.....34

Appendix: Geedge deployment in Myanmar.....37

Endnotes.....39

Executive Summary

A new leaked dataset reveals the Chinese company Geedge Networks' business in Myanmar and exposes a significant number of telecommunications companies that are implementing sophisticated surveillance and censorship technology on behalf of the illegal Myanmar military junta. The leaked dataset offers detailed insights into the inner workings of Chinese internet surveillance and censorship technology that is exported to Myanmar by a company that frames its work as associated with China's Belt and Road Initiative.

The dataset has been reviewed by a coalition of media and non-governmental/civil society organisations through the Great Firewall Export project made up of Amnesty International, InterSecLab, the Globe and Mail, Paper Trail Media, Tor Project, DER STANDARD, and Follow The Money.

The Internet in Myanmar since the military's February 2021 illegal coup attempt is among the most restricted in the world. The rolling out of a commercialised version of China's Great Firewall gives the junta unprecedented access to and control over the online activities of 33.4 million internet users in Myanmar.

Notably, the hardware, software and support provided by Geedge Networks to the Myanmar military junta enables the tracking of network traffic at the individual level and can identify the geographic location of mobile subscribers in real time by linking their activity to specific cell identifiers (cell IDs). As such, the junta has an enhanced capability to effectively track down, arrest, torture and kill human rights defenders, journalists and revolutionary forces across the country. The military junta can do so with the direct assistance of telecommunications companies in Myanmar exposed in the dataset – including ATOM (formerly Telenor Myanmar), Mytel, Myanma Posts and Telecommunications (MPT), Ooredoo Myanmar, Frontiir, StreamNet , Golden TMH Telecom, Internet Maekhong Network (IM-Net), Myanmar Broadband Telecom (MBT), Myanmar Telecommunication Network (MTN), Campana, Global Technology Group and China Unicom – that are integral to the set-up of a national firewall for the Myanmar junta.

This investigation into the business dealings of Geedge Networks with the Myanmar junta builds on a June 2024 report by Justice For Myanmar into how Geedge was initiating country-wide internet surveillance and censorship through the junta-controlled Information Technology and Cyber Security Department (ITCSD) of the Ministry of Transport and Communications (MOTC).

By providing hardware and software to the illegal Myanmar military junta, Geedge may be aiding and abetting in the commission of crimes against humanity, including the acts of torture and killing, carried out by members of the junta within a widespread or systematic attack on a civilian population. Further investigation is required on this. In the meantime, Geedge Networks is limiting the rights to freedom of expression, association, and digital movement of the people of Myanmar. For that reason, Geedge Networks should be targeted with international sanctions, and individuals in directive and leadership positions within the company should be investigated for aiding and abetting violations of international human rights laws and potentially also international crimes.

Telecommunications companies identified in the Geedge dataset as supporting the junta's online surveillance machinery should be held to account for the serious risks of online and offline violence, and de facto harms such as arrests, torture and killings, of Myanmar civilians.

Geedge Networks is closely affiliated with the Chinese state and export of its systems to Myanmar align with the Belt and Road Initiative. China's involvement in the mass surveillance and repression of the civilian population in Myanmar is part of a broader pattern in which the Chinese government remains a principal supplier of arms to the Myanmar junta, aiding and abetting the commission of war crimes and crimes against humanity.

The Myanmar junta's terror campaign online

Internet in Myanmar since the military's illegal coup attempt on February 1, 2021 is defined by widening and pervasive surveillance, censorship and internet shutdowns, a digital front in the junta's nationwide terror campaign. The effect is a broad chilling of freedom of expression, association and information, with the junta turning online expression into a potential death sentence. Telecommunication users practice self-censorship and even limit digital resistance to mitigate grave risks to their safety amid the junta's mass arbitrary arrests, widespread torture, enforced disappearances and executions.

Myanmar's information environment is ranked as one of the worst in the world, tied with China in 2024.[1] According to Freedom House's Freedom on the Net ranking, the Myanmar junta routinely orders significant internet restrictions that often coincide with violent offline crackdowns.[2] This is coupled with data price hikes, online trolling, and crackdowns on virtual private networks (VPNs).

These practices also impede access to lifesaving emergency information. In the context of the devastating 2025 Sagaing Earthquake, connectivity blackouts hindered family tracing and coordination with aid providers.[3]

Arbitrary arrests by the junta based on the online expression of dissent, including through social media posts, remain commonplace in Myanmar. Between 2022 and 2024, Data for Myanmar reported nearly 1,500 arrests for anti-junta content on Facebook, TikTok, and Telegram, with additional arrests triggered following the junta's scanning of users' private messages.[4] Citizens face intrusive biometric tracking in the form of mandatory e-IDs, facial recognition at checkpoints, and AI-enabled monitoring that links online behaviour to users' physical identities.[5]

Information revealed by the Norwegian broadcaster NRK in August 2025 shows how collaboration between the military junta and telecommunications companies can be deadly. According to leaked documents on the conduct of Norwegian telecoms company Telenor following the military's coup attempt, 1,300 mobile customers had their traffic data handed to the junta or their phones blocked, with 500 customers at immediate risk of arrest. Documents also contained statements by the junta that it would use information from Telenor to arrest and sentence people to prison terms of between three and seven years. Telenor data transfer relating to phone usage and location has been linked to the arrest and subsequent execution of pro-democracy activists Jimmy and Phyo Zeyar Thaw, which amounted to crimes against humanity.[6]

As the junta prepares for a sham election, it is intensifying its repression. In January 2025, the junta enacted a cybersecurity law that provides it with extensive control over access to information.[7] The law introduces unchecked measures for the military junta to control internet content and applications, and surveil user activities.[8] The law mandates that internet service providers store user data for up to three years and includes penalties for disseminating disinformation and rumours which could lead to fines or imprisonment for individuals and digital service providers, a serious breach of human rights.[9]

On July 29, 2025, the junta then enacted a law to protect military secrets, which also attempts to control information amid defections from the junta and whistleblowers in its ranks. The law prescribes life imprisonment or the death penalty for the transfer of military secrets.[10]

As part of its illegal coup attempt and ahead of its planned sham election, the military junta dissolved the so-called State Administration Council and replaced it with State Security and Peace Commission (SSPC) on July 31, 2025. Since its

change of name to SSPC on July 31, the junta has further intensified its campaign of terror against the people, with indiscriminate airstrikes and shelling, arbitrary arrests, torture and the destruction of whole communities.

Digital surveillance and censorship is now increasing as part of the junta's attempts to hold a sham election in December. An “election” protection law it passed in July carries the death penalty and has already resulted in the arrest of Nay Thway, a resident of Taunggyi, for criticising the junta's "election" in a Facebook post.[11]

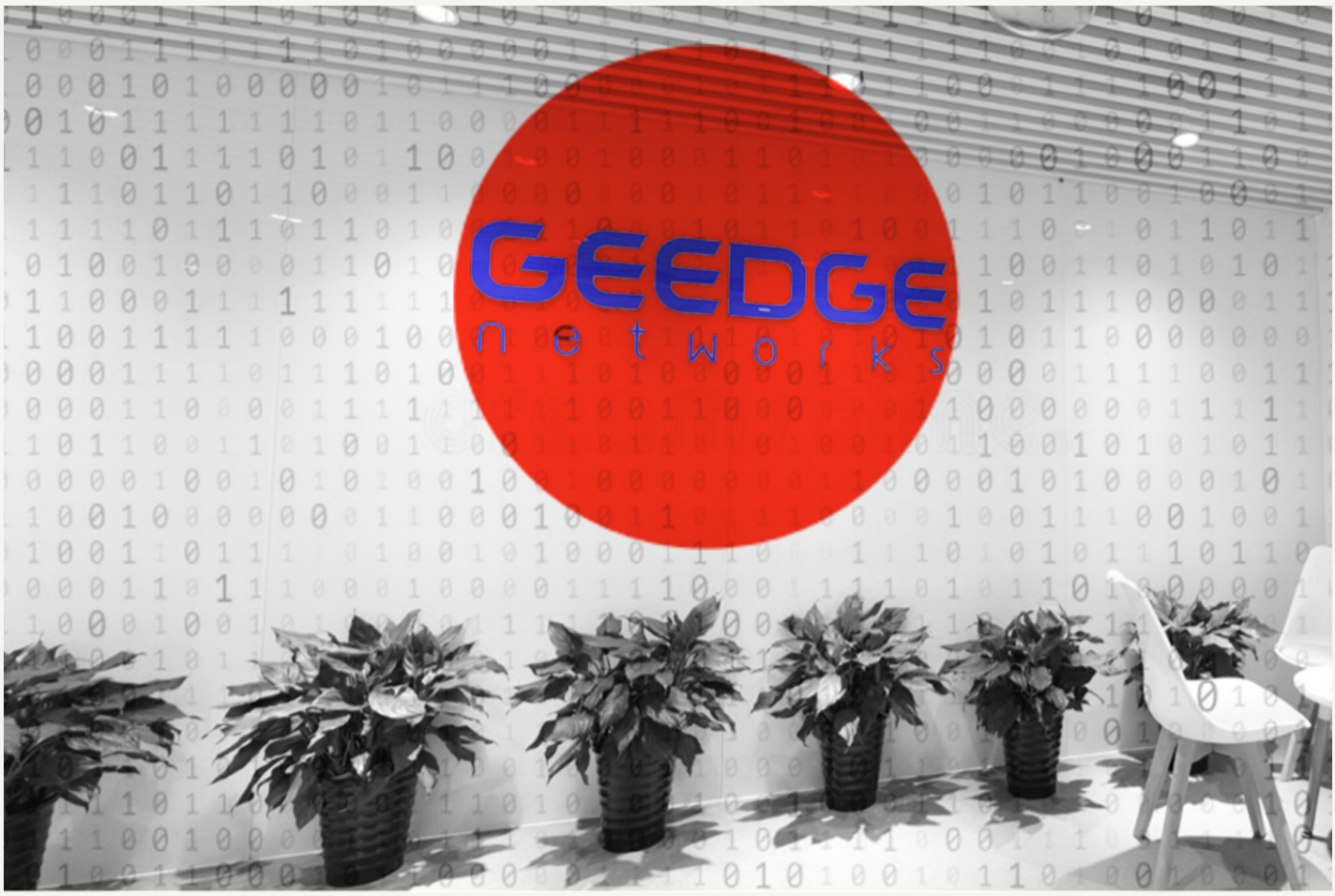
The junta's online and offline terror campaign has been enabled by the Chinese government and companies, and their complicity is only deepening. Chinese companies are the junta's main arms suppliers. This includes state-owned enterprises that continue to supply the Myanmar military with weapons, maintenance, and the repair and overhaul of weapon platforms. This support has continued unabated since the attempted coup in February 2021 and has included deliveries to all branches of the Myanmar armed forces: land, air and navy. Myanmar military personnel are also being trained, including through scholarships provided by Chinese state-owned arms companies, at numerous defence-oriented universities and engineering schools affiliated with the Peoples' Liberation Army. On 22 October 2024, the Myanmar junta formed a working committee to prepare a memorandum of understanding with the Chinese government for the creation of a new joint venture security firm to "handle the import of weapons and special equipment, including communications devices and restricted tools," showing that the supply of weapons, equipment and technology is only continuing.[12]

In the telecommunications front, no company has been more important for the junta's attempts to control and surveil the internet than China's Geedge Networks, which has sold the junta a commercialised version of China's "Great Firewall". Using a new leak of documents from Geedge Networks, Justice For Myanmar has investigated the extent of Geedge Networks’ collaboration with the military junta, and the telecommunications companies operating in Myanmar that have joined the junta's country-wide online surveillance and censorship regime.

The Geedge dataset has been reviewed by a coalition of media and non-governmental/civil society organisations through the Great Firewall Export project. The coalitions is made up of InterSecLab,[13] which provided support on the technical aspects of the collaboration, hosted the research platform and made the Geedge dataset searchable, Amnesty International,[14] the Globe and Mail, Paper Trail Media, Tor Project, DER STANDARD and Follow The Money. This collaboration has resulted in the publication of reports and articles outlining Geedge

Networks’ export of a "Great Firewall” globally, enabling far-reaching and significant surveillance of internet and telephone users.

The larger dataset encompasses Geedge Networks’ internal Jira (ticketing system) and Confluence (a software for writing and sharing notes with coworkers) instances, as well as source code and binary files used for deployment of surveillance infrastructure in Myanmar and other highly repressive countries. In relation to Myanmar – codenamed M22 by Geedge Networks – the leak includes detailed technical documents on the deployment in the country, network diagrams showing implementation, tests, logs and communication with companies in Myanmar on whose premises hardware and software has been installed. Documents from a second source include a draft 2023 contract between the junta-controlled ministry of transport and communications and an unnamed Chinese company for the supply of a “secure web gateway” to be sold through Myanmar Foreign Trade Bank, which is also illegally under junta control.



What is Geedge Networks?

Geedge Networks, also known as Jizhi (Hainan) Information Technology Co. Ltd. (积至（海南）信息技术有限公司, is a Chinese private network security company based in the Hainan Free Trade Port. The company was set up in 2018. It is owned by Dongguan Hulian Network Security Investment Partnership (Limited Partnership) and Nali (Chengmai) Information Consulting Center (Limited Partnership). Chinese corporate data lists Wang Yuandi (王媛娣) as Geedge Networks' legal representative and CEO.

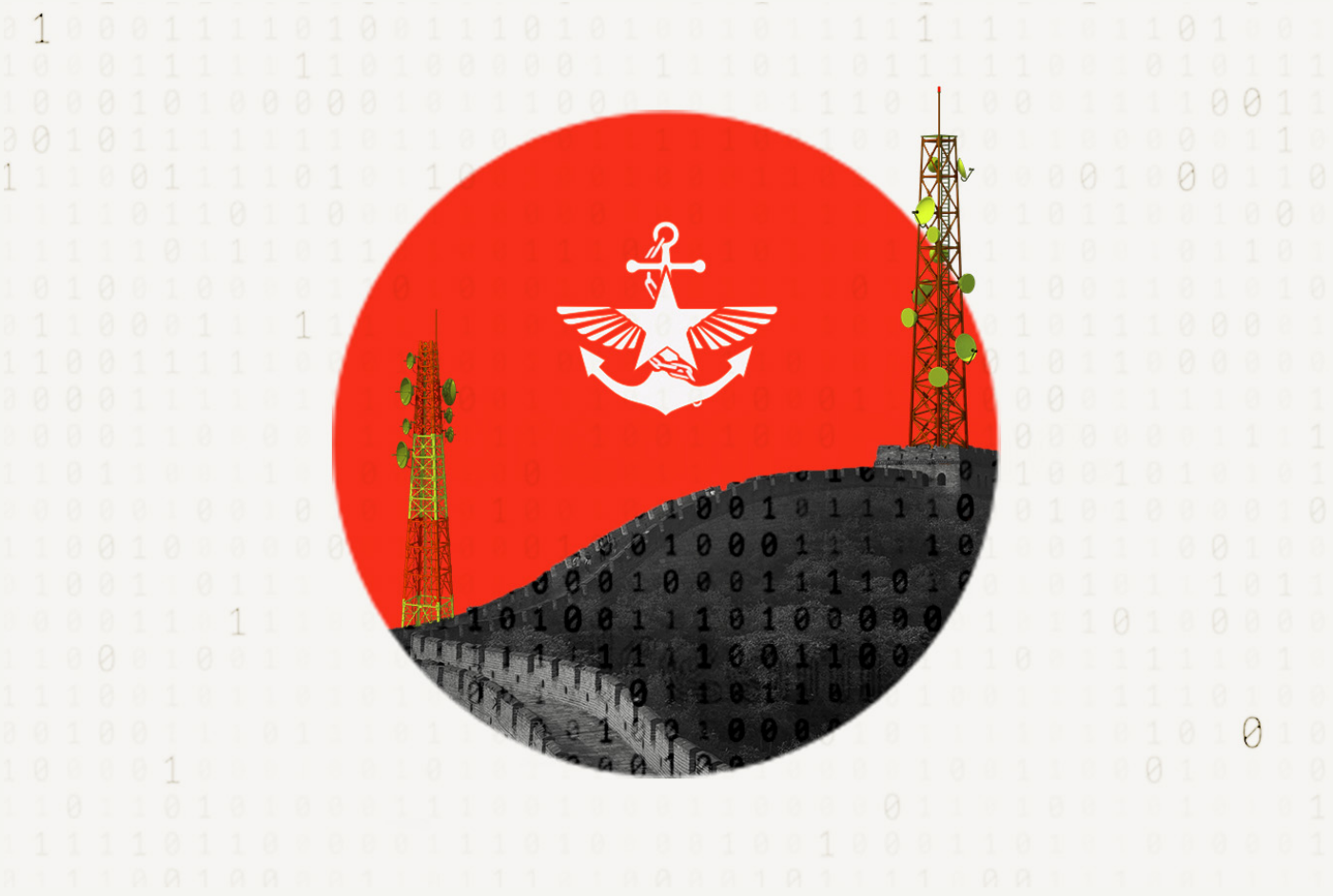
Among Geedge Networks' key staff is Fang Binxing (方滨兴), the company's co-founder and chief scientist who, according to the Geedge dataset, is leading the implementation of Geedge's surveillance and censorship system in Myanmar.[15] An academic at the Chinese Academy of Engineering, Binxing is known as the "father" of China's Great Firewall for his work on the blocking and filtering system that denies China's netizens access to a large number of foreign websites.[16]
Geedge Networks works closely with the 'Massive and Effective Stream Analysis' (Mesalab) research group at the Institute of Information Engineering at the Chinese

Academy of Sciences, which, by its own account, focuses on "the research and application of information and network security."[17]

Through Fang Binxing, Geedge Networks is also closely linked with another Chinese State-owned company, China Electronics Information Industry Group (中国电子信息产业集团有限公, CEC), where he has been the chief scientist.[18] As previously exposed by Justice For Myanmar in 2024, CEC's wholly owned subsidiary China National Electronics Import and Export Corporation (中国电子进出口有限公, CEIEC) has supplied a location tracking system to the junta controlled Information Technology and Cyber Security Department (ITCSD) of the Ministry of Transport and Communications through Myanmar broker Mascots Group.[19] Justice For Myanmar reiterates its call for sanctions against the Mascots Group network for its role in supplying surveillance technology to the military junta.

Geedge Networks has associated itself with China's Belt and Road Initiative, a core component of China's foreign policy that seeks to further enhance connectivity between China and countries across Asia, Europe, Africa, Oceania, and Latin America.[20] Myanmar officially joined the China Belt and Road Initiative in 2017, when State Counsellor Aung San Suu Kyi signed a memorandum of understanding (MoU) on a state visit to Beijing.[21] Numerous other agreements and MoUs were signed subsequently related to key projects within this cooperation framework.[22] This included a 2018 MoU between the two countries for the construction of a China-Myanmar Economic Corridor.[23] Considered a vital artery of the Belt and Road Initiative, the economic corridor foresees the establishment of two transport lines from the port of Kyaukphyu in the Bay of Bengal and from Yangon that converge at Mandalay and continue to the Chinese border at Muse with special economic zones (SEZs) and industrial zones set up adjacent to major cities and along the border.[24]

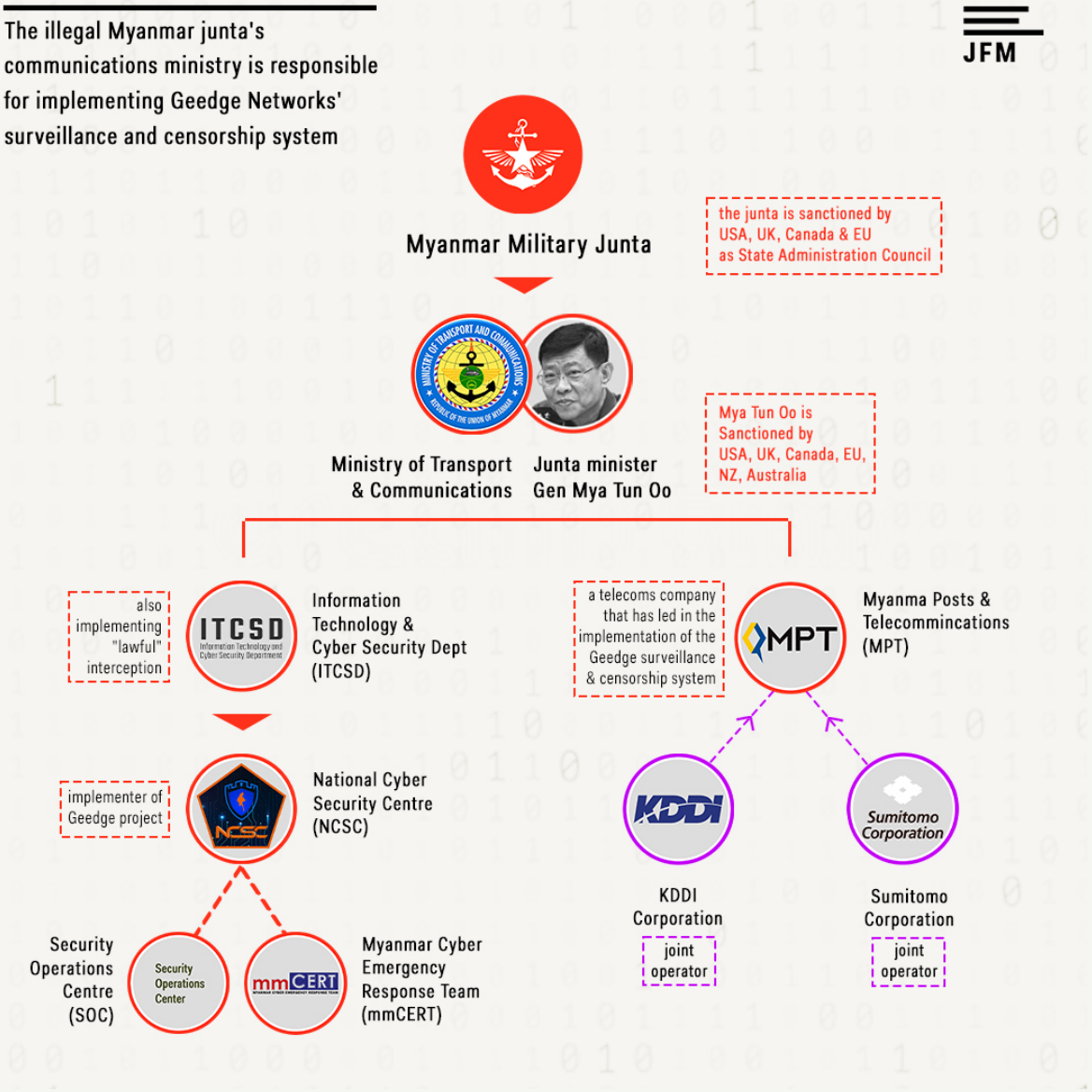
Another component of the Belt and Road Initiative is the 'Digital Silk Road' that specifically focuses on digital infrastructure and technology projects, and seeks to promote Chinese technology, goods, and services in Belt and Road partner countries.[25] By Fang Binxing's own account, Geedge Networks was founded in response to the Chinese Government's official "go global" policy (走出去战略) that encouraged Chinese enterprises to invest overseas, including through opportunities provided by joining the Belt and Road Initiative, in the process linking the initiative to surveillance, censorship and the serious human rights and international law violations that stem from Geedge's sophisticated systems.[26]



The Myanmar junta's implementation of China's "Great Firewall”

The Geedge dataset contains significant detail on how Geedge products have been deployed. In Myanmar, Geedge Networks' principal partner has been the Ministry of Transport and Communications (MOTC) through its National Cyber Security Center (NCSC) which reports to the MOTC’s Information Technology and Cyber Security Department (ITCSD). The ministry and its constituent parts were illegally seized by the Myanmar military through its February 1, 2021 coup attempt.

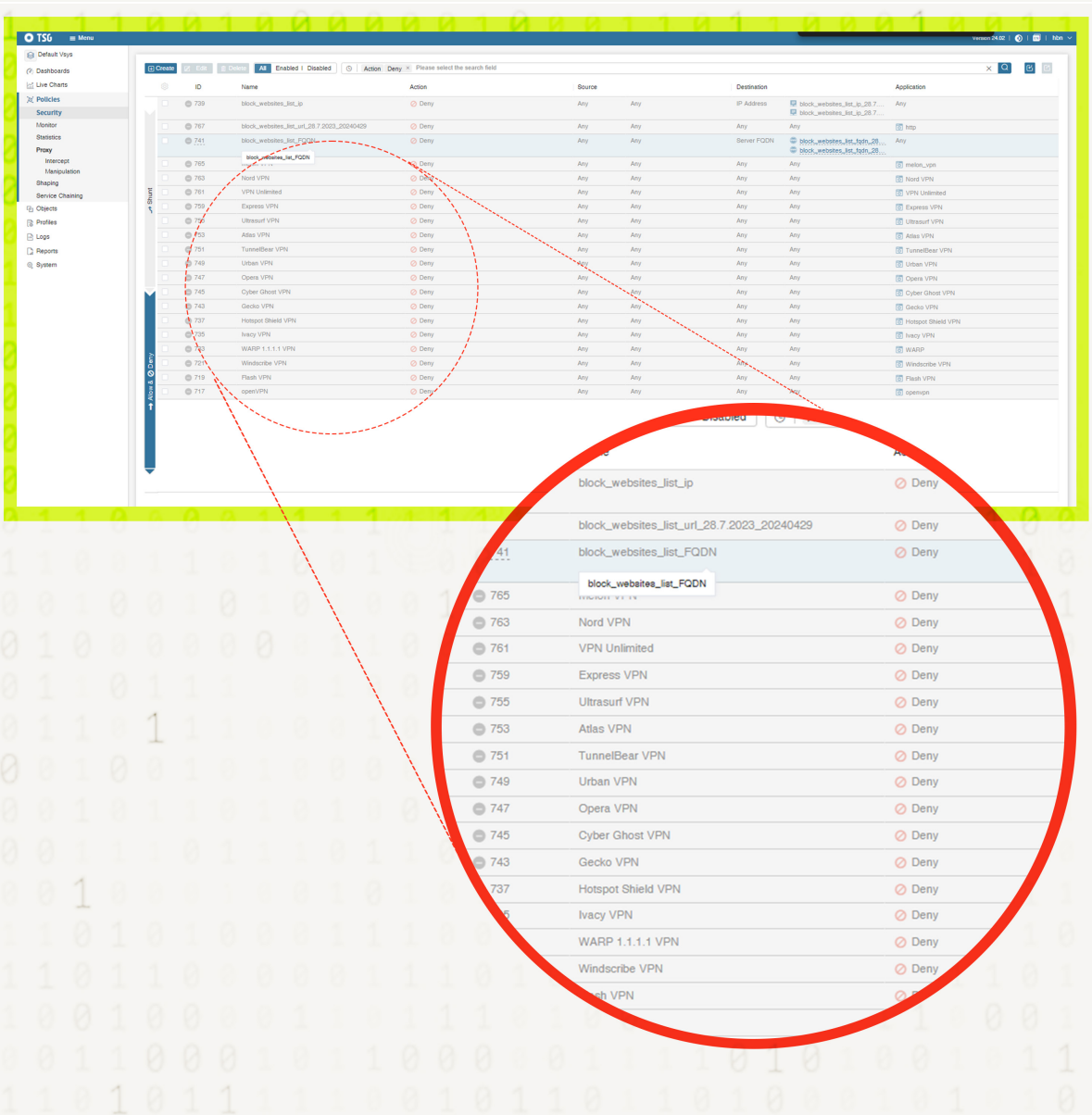
According to Myanmar sources, the NCSC is divided into a Myanmar Cyber Emergency Response Team (mmCERT) and a Security Operations Center (SOC). The mmCERT notably handles "digital forensics", "international and regional cooperation" and "technical assistance and advice”.[27]



The ITCSD, for its part, is also responsible for the implementation of so-called "lawful interception" to provide the military with real-time monitoring of communications, including the tapping of phone calls. The department is additionally involved in making deals with international satellite operators to lease satellite channel bandwidths for ministries, media, and telecommunications companies, including for military use.

Geedge Networks' systems provided to the junta were first installed and piloted on-site in Myanmar between June and November 2022 according to documents in the Geedge dataset.

Geedge Networks technicians travelled to Myanmar for an "environment survey" and a visit to the Myanma Posts and Telecommunications (MPT) and the NCSC in 2022. This "proof-of-concept" visit entailed checks on "internet topology, network interfaces and server rooms" in Myanmar, training of NCSC staff, and "a presentation of test cases" to illustrate how to practically block VPNs, including "subscriber paid VPN nodes like Nord VPN and Proton VPN", "limit YouTube" and control Viber voice calls based on the "requirements of the NCSC".



The Geedge system provides the junta with centralised control to set rules for the blocking of VPNs across internet service providers nationwide. Image extracted from the Geedge dataset.

Documents seen by Justice For Myanmar also elaborate on the nature, functioning, and physical locations of the surveillance architecture – both hardware and software – supplied by Geedge Networks for the Myanmar junta.

A "TSG [Tiangou Secure Gateway] solution review description" document confirms that Geedge Networks was to provide MOTC with both the hardware and software required to successfully implement extensive surveillance and censorship. Contractual arrangements between Geedge Networks and the Myanmar military junta include TSG Centralized Management, Network Zodiac for system operation and maintenance, and Cyber Narrator for supporting what internal datasets refer to as "hunting" the IP addresses of evasive proxies. According to Geedge Networks' review document to the MOTC, all software programs have "long-term authorization" and come with a three-year free of cost warranty which is specified to include monthly system updates and the deployment of Geedge technicians in Myanmar. Hardware warranties and express delivery of spare parts are also accounted for. After the initial warranty has expired, the MOTC is expected to purchase an additional warranty and technical support package, which includes the deployment of two Geedge Networks engineers to Myanmar for on-site technical support.

The dataset provides new detail about Geedge Networks products deployed in Myanmar and elsewhere.

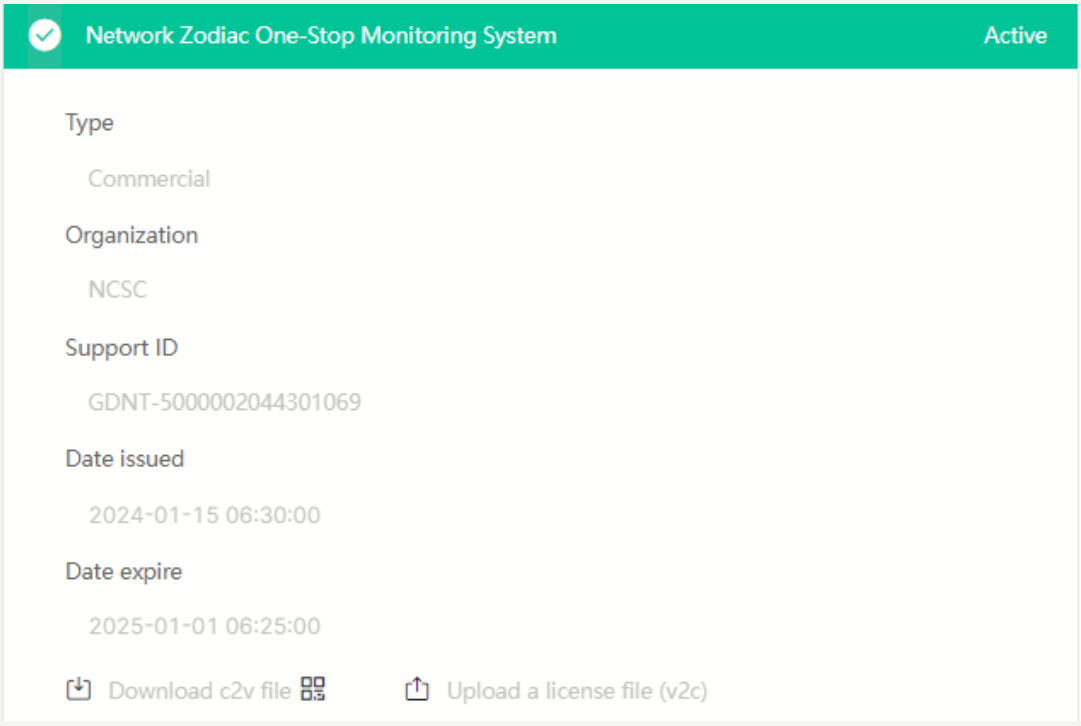
Tiangou Secure Gateway (TSG)

TSG is the central tool in the Geedge Networks' surveillance and censorship arsenal, consisting of hardware and software to manage, surveil and block internet traffic, comparable to China's "Great Firewall", one of the largest and most sophisticated online censorship operations in the world.[28]

TSG provides monitoring and filtering capabilities of internet traffic, including internet-based telephone traffic. This provides the junta with extensive visibility of internet traffic in Myanmar, while also facilitating the identification and blocking of web content and applications. Within the data set is a list of 55 priority apps for blocking that Geedge provided to the Myanmar junta, including popular VPNs and the messaging app Signal.

According to the Geedge Networks website, "TSG performs deep packet inspection on network traffic, classifies their content using a stream-based analysis engine, and provides a simple, integrated security service".[29] TSG's claimed features include the ability to decrypt and inspect traffic between the server and client that is encrypted with secure sockets layer (SSL) and transport layer security (TLS) encryption protocols.[30] One way it does this is by monitoring and skipping security

certificates on websites. Where decryption is not possible, the system is also able to capture metadata and analyse online behaviour.



A screenshot of the junta's National Cyber Security Centre's Network Zodiac license, extracted from the Geedge dataset.

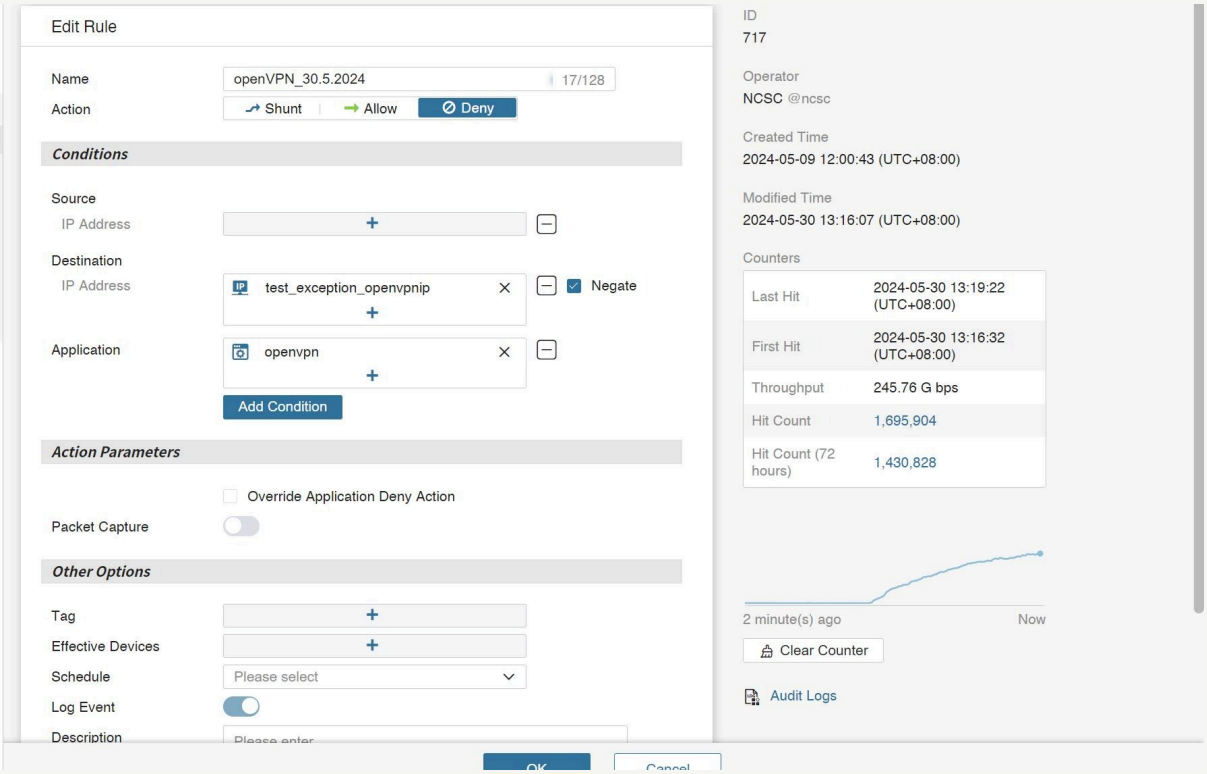
Decrypted plain text traffic can then be mirrored to a third party for archiving and analysis.

TSG also features an application firewall to "deny or allow more than 1000 applications based on their behaviours and attributes".

According to a Geedge TSG Solution Review document, the TSG package consists of licenses for three key packages of software: TSG with Central Management "for the central management such as GUI, Policy, Events and Records, Network Visibility and Report"; Cyber Narrator "for supporting hunting the IP addresses of evasive proxy" and Network Zodiac "for system operation and maintenance".

This is coupled with hardware assembled in China that is also provided by Geedge. Hardware described in the company's proof of concept for the Myanmar junta consisted of an Optical Bypass Protector, Ether Fabric, TSG XM14220, TSG Central Management, TSG OLAP (Server 1), TSG OLAP (Server 2) and ISP Traffic Aggregation Switch.

Further technical descriptions are outlined in the report, *The Internet Coup: A*



A screenshot of the TSG interface used by the junta's National Cyber Security Centre to block VPNs, extracted from the Geedge dataset.

Technical Analysis on How a Chinese Company is Exporting The Great Firewall to Autocratic Regimes, by InterSecLab.[31]

Documents suggest that the system in Myanmar works through installation in 26 data centres of 13 internet service providers (ISPs) and internet gateways (IGWs) across Myanmar, the majority being in Yangon and Mandalay. There may likely be additional installations and companies that are not captured here. Data collected at the regional centres is then accessed remotely and aggregated at two central command centres in Yangon and Naypiydaw, the junta's interface with the Geedge system that is operated by NCSC. Based on documents in the Geedge dataset, Justice For Myanmar believes the command and control centre in Naypyidaw could be part of the monitoring centre operated by ITCSD, which is located in the State Security and Peace Council (formerly State Administration Council) Office.

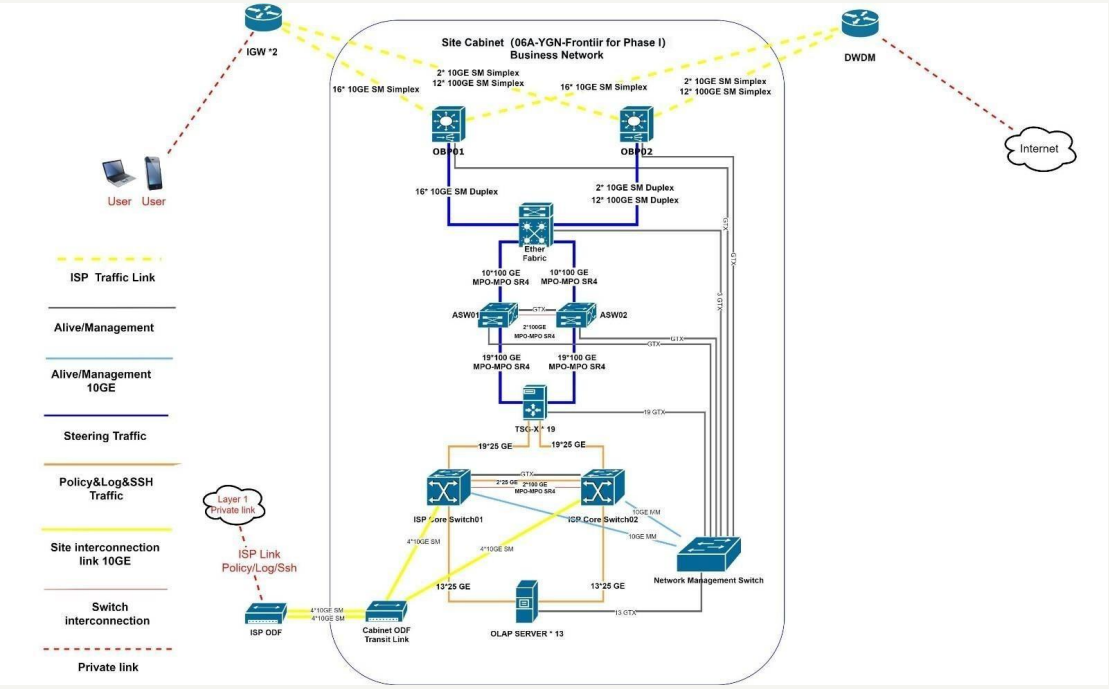
Telecommunications companies in Myanmar implementing mass surveillance for the illegal junta

Diagrams and spreadsheets seen by Justice For Myanmar confirm how TSG has been deployed in data centres of 13 telecommunications companies across 7 towns and cities in Myanmar: Naypyidaw, Yangon, Mandalay, Tachilek, Kyaingtong, Muse and Myawaddy. Notably, a document dated 15 July 2024 contains detailed information about the installation of TSG in numerous data centres, including their quantity and physical location, and their corresponding ISPs.

Information from the Geedge files includes updates dating back to January 2022 and up to August 2024, indicating that these network configurations were active during this period.

Network diagrams from Geedge show site cabinets located in data centres of telecommunications operators. Information technology experts consulted by

JusticeFor Myanmar confirm that these diagrams show physical cabinets inside data centres and illustrate, in practical terms, the functioning of Geedge Network-supplied hardware and software that is used to monitor and censor Myanmar web traffic.



An image showing the integration of Geedge hardware in Frontiir's Yangon data centre, extracted from the Geedge dataset.

The diagrams, such as that above for a Frontiir (Myanmar Net) data centre, shows the origin of Myanmar internet traffic which enters the system through dense wavelength division multiplexing (DWDM) optical fibre, is then transmitted to the cabinet via single-mode optical fibre and exits to the access network through the internet gateway (IGW). The web traffic is mirrored through an optical bypass protector (OPB) which is designed to tap the optical fibres while protecting connected equipment from failures, which is a network architecture that creates a mirror copy of all the internet traffic passing through for inspection by the Geedge system. All the traffic is then processed by the Geedge Networks TSG-X boxes, which are at the heart of the system. After passing through TSG-X, internet traffic data is analysed, filtered and logged, and is then routed through two core switches which direct the traffic records to online analytical processing (OLAP) servers, which facilitate the analysis of data. The ISP Link Policy/Log/SSH link refers to a separate management network that allows the system to be remotely operated. It is connected to an optical distribution frame (OPF) cabinet, with its own dedicated private "layer 1" physical link, meaning that the management network

interconnecting the regional centres and the central command and control centres is likely completely isolated from the internet.

Telecommunications companies collaborating with the military junta for the implementation of the Geedge system have expanded incrementally, from 6 in 2022, starting with Myanma Posts and Telecommunications (MPT), and growing to at least 13 by 2024. Companies exposed in the Geedge files that have implemented TSG include:

- Myanmar Posts and Telecommunications (MPT)
- Telecom International Myanmar Company Limited (Mytel)
- ATOM Myanmar Limited
- Ooredoo Myanmar Limited
- Frontiir Company Limited (Myanmar Net)
- Campana Mythic Company Limited
- Stream Net Company Limited
- China Unicom (Myanmar) Operations Company Limited
- Golden TMH Telecom Company Limited
- Myanmar Broadband Telecom Company Limited (MBT)
- Global Technology Company Limited (GlobalNet)
- Myanmar Telecommunication Network Public Company Limited (MTN)
- Internet Maekhong Network Company Limited (IM-Net)

Myanma Posts and Telecommunications (MPT)

Myanma Posts and Telecommunications (MPT) is a national mobile network operator that has implemented Geedge systems at its data centres in Yangon, Naypyidaw and Mandalay. Leaked documents suggest that MPT was the first company in Myanmar to implement Geedge systems and when Geedge technicians visited Myanmar in 2022 for an environmental survey and training, they engaged with MPT. MPT is a joint operation between the junta-controlled Ministry of Transport and Communications and Japanese multinational companies Sumitomo Corporation and KDDI Corporation through their joint venture KDDI Summit Global Myanmar Co., Ltd. (KSGM). This gives the Japanese companies responsibility for the human rights violations directly linked to MPT's surveillance and censorship collaboration with the junta.

Under pressure, on 28 April 2025, Sumitomo Corporation[32] and KDDI[33] announced that KSGM had agreed to "amend its agreement with MPT" with a view to limit the scope of KSGM's support of MPT's telecommunications operations in Myanmar, although it remains invested in the telecoms operator.

This follows a prior, September 2021, statement by KDDI[34] and Sumitomo Corporation[35] expressing "deep concern about lawful interception in Myanmar" and statements that they had not been "subject to direct instructions from the regulatory authority with regard to interception". As has previously been disclosed by Justice For Myanmar, MPT has also worked with Israeli surveillance-for-hire corporation Cognyte Software Limited in 2020 for the instalment of an interception gateway that would allow the Myanmar military to tap calls in real time.[36]

Telecom International Myanmar Company Limited (Mytel)

Another of the four nationwide mobile network operators is Mytel, trading under the company Telecom International Myanmar Company Limited, which has implemented Geedge systems in its Yangon and Mandalay data centres. Mytel is a key pillar in the Myanmar military's business network, providing it with revenue, technology and surveillance capabilities. Mytel's shareholders are the military conglomerate Myanmar Economic Corporation, Vietnam’s Ministry of National Defence-owned Viettel Global Investment, and Myanmar National Telecom Holdings, which is an investment vehicle for Myanmar cronies.

War criminal Min Aung Hlaing attending a celebratory ceremony to inaugurate Mytel as the fourth telecom operator in Myanmar. Source: Myanmar military

As Justice For Myanmar has previously exposed, Mytel works in partnership with the Myanmar Army's Directorate of Signals, builds infrastructure on military bases, and provides the military with a lucrative source of off-budget revenue and a means to access international communications technology and credit.[37] Leaked correspondence between Geedge and MOTC confirms that in April 2024, Mytel experienced disruptions in their network links related to the "secure web gateway system project" (SWG). A flawed attempt by Mytel technicians to resolve the issue resulted in a meeting, on Mytel premises, between staff of NCSC and Mytel's technicians to address the network disruptions.

ATOM Myanmar Limited

ATOM Myanmar is one of the four national mobile network operators in Myanmar and has implemented TSG in its Yangon and Mandalay data centres.

ATOM Myanmar was formerly operating as Telenor Myanmar Limited, a subsidiary of Norwegian telecommunications company Telenor. Following the military's coup attempt, in June 2021, Telenor announced the sale of Telenor Myanmar Limited to Investcom Pte. Ltd.,[38] which became a joint venture between M1 Group, a Lebanon-based conglomerate, and Shwe Byain Phyu,[39] a military-linked crony conglomerate, in a widely criticised exit during which it shared sensitive data with

the junta. As has previously been exposed by Justice For Myanmar, Shwe Byain Phyu Group has business links to the military conglomerate Myanma Economic Holdings Limited (MEHL) including for the import to Myanmar of petroleum and the company and its founders are sanctioned by the USA and Canada.[40]

In a reply to Justice For Myanmar, Investcom claimed that ATOM does not “design, direct &/or conduct mass, unlawful surveillance” and that it applies internal human-rights due-diligence procedures aligned with the UN Guiding Principles”. The company noted that it was “aware of claims relating to third-party technologies in Myanmar” but, referring to company policy, refused to “confirm or deny the existence of third-party systems”.

Ooredoo Myanmar Limited

Ooredoo Myanmar Limited (OML) is one of the four nationwide mobile network operators in Myanmar. It has implemented Geedge systems in Yangon and Mandalay. It was established as a fully owned subsidiary of Ooredoo Q.P.S.C., domiciled in Qatar and majority owned by the state of Qatar.[41] Founded in 2014, OML along with Telenor entered Myanmar when there were no laws in place to regulate the use of interception technologies. Before and immediately after entering Myanmar, concerns were raised publicly regarding the human rights risks of operating a telecommunications company in Myanmar, including with Ooredoo Group's CEO directly.[42]

On September 8, 2022, Ooredoo announced the entry into a sales agreement for OML through its parent company, Ooredoo Asian Investments Pte. Ltd. (OAI), domiciled in Singapore, to Nine Communications Pte. Ltd., a Singapore-domiciled special project vehicle.[43] Ooredoo's exit was completed on May 31, 2024.[44] According to Singaporean registry data accessed in August 2025, Nine Communications biggest shareholder is Nyan Win through the Singapore-registered company, Sunny Aqua Mountain Pte. Ltd., followed by Aion Ventures Limited and then the Myanmar companies National Telecommunication Development Co. Ltd., Pyi Taw Tha Pyi Telecom Co. Ltd. and Mahar Kyunt Mong Co. Ltd. Aion Ventures Limited is domiciled in the British Virgin Islands, a jurisdiction that is required to comply with UK sanctions on Myanmar.

Frontiir Company Limited (Myanmar Net)

Frontiir is one of Myanmar's largest ISPs and it has implemented Geedge technology in Yangon. Founded in 2013 by two US citizens and a Canadian, it is led by Myanmar-born US citizen Godfrey Tan (Wai Lin Tun).[45] Frontiir provides

internet services through its Myanmar Net brand. Concerns about Frontiir's involvement in internet censorship in Myanmar were raised in 2020, when it was revealed that the company was blocking access to websites on the Myanmar government's orders.[46]

Like other ISPs, Frontiir shut off the internet in the commercial hubs of Yangon, Mandalay and the capital Naypyidaw on the military's orders on the day of its coup attempt. Since then, it has periodically blocked social media platforms, including Facebook, X (formerly Twitter) and Instagram, as well as independent media and civil society sites including Justice For Myanmar.

Frontiir is backed by governments that have otherwise condemned the military's coup attempt and commission of international crimes, through development finance. These include investments into Frontiir of US$26 million from British International Investments (BII); 26.9 million Norwegian krone (US$3 million) from Norway's Norfund, and 70.1 million Danish krone (US$10.5 million) from Denmark's Impact Fund (IFU). All of the investments have been made since 2019 – after the UK, Norway and the European Union imposed sanctions barring their companies from providing surveillance equipment to Myanmar.

ISP Frontiir denied that they have Geedge hardware on site in response to an investigation by Finance Uncovered and Myanmar Now.[47] InterSecLab and Justice For Myanmar both conclude that, based on the Geedge dataset, these denials are false.

In a reply to Justice For Myanmar, IFU responded, “together with the other investors, we are in dialogue with Frontiir regarding the situation and strive to ensure that they meet the requirements we have set and that they safeguard employee safety and customer data security. The provided information will be taken into consideration.”

A spokesperson for BII said, "we are in regular dialogue with Frontiir regarding customer data security. The information you provided will be reviewed carefully.”

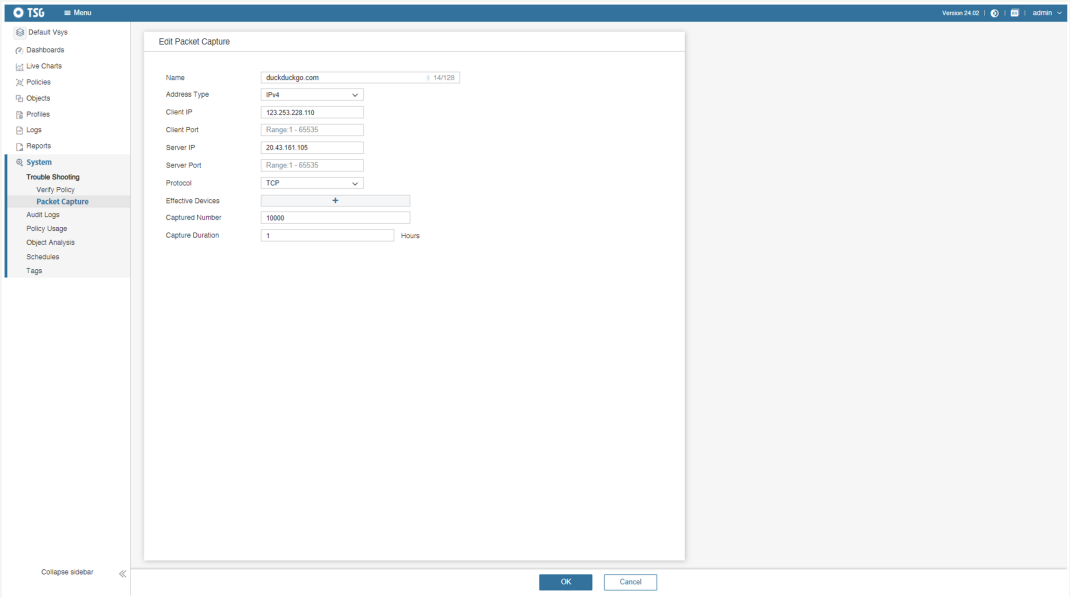
Campana Mythic Company Limited

Established in 2014, Campana is a multinational data network infrastructure operator. It has implemented Geedge systems at its data centre in Yangon. The company is privately owned and operates network and infrastructure in Singapore, Myanmar and Thailand. Campana Mythic received a license to operate in Myanmar in 2015.[48] Campana Mythic is a subsidiary of the Singapore company

Campana Group Pte. Ltd. According to documents obtained through Singapore's corporate registry, Campana Group's principal shareholders include chief executive officer Myo Myint Ohn and director Win Myint Ohn, both of whom are Canadian citizens; the Japanese company Mitsui & Co; and the Thai companies Advanced Information Technology Public Co. Ltd (AIT) and Loxley Public Co. Ltd.[49]

Campana has provided international gateway services in Myanmar via its trans-ASEAN network which connects Myanmar to Singapore via Thailand over terrestrial and submarine fibre optic cables. In 2023, the company also announced that it would start operating an international undersea submarine cable connection from Singapore to Myanmar in the Myanmar Special Economic Zone.[50]

According to research published for the 11th Workshop on Free and Open Communications on the Internet on internet censorship in Myanmar, Campana Mythic hijacked internet address space belonging to Twitter during a junta imposed internet shutdown days after the military's February 2021 coup attempt.[51]



A packet capture test with TSG conducted on the Campana network of the search engine DuckDuckGo in 2024, extracted from the Geedge dataset.

The company's actions had spillover effects beyond Myanmar with users in other countries also being unable to access Twitter. When the junta then blocked Twitter altogether in Myanmar, Campana Mythic announced the 104.244.42.0/24 prefix, belonging to Twitter. The researchers concluded, "the proximity of this hijacking event in time to the blocking of Twitter in other Myanmar ISPs suggests that the original intent was to blackhole traffic to Twitter for users of this Myanmar ISP."

In a reply to Justice For Myanmar, Campana shareholder Mitsui & Co. referred to its corporate human rights policy and noted that it conducts human rights due diligence concerning its investments.

Stream Net Company Limited (StreamNet)

Launched in 2017, StreamNet is a network service provider of fibre, wireless and satellite technology to businesses. It has implemented Geedge systems in its data centre in Yangon. StreamNet is a joint venture between Vietnam Post and Telecommunications Group (VNPT) and Elite Telecom.[52] Elite Telecom is closely linked to the crony Htoo Group conglomerate through shared directors. VNPT is a Vietnamese state-owned enterprise under the Committee for Management of State Capital at Enterprises, after being transferred from the Ministry of Information and Communications in 2019.[53]

According to Vietnamese media, StreamNet was established to boost VNPT's international investment and business.[54] As Justice For Myanmar previously exposed,[55] VNPT opened its representative office in Myanmar in 2014 and signed a memorandum of understanding (MoU) with Terabit Wave, an arms broker company registered with the military's directorate of procurement to provide communications technology services.[56]

2017 Launch of StreamNet in Yangon. Source: Ministry of Science and Technology, Vietnam

China Unicom (Myanmar) Operations Company Limited

China Unicom is a Chinese state-owned telecommunications operator that operates a fully owned subsidiary in Myanmar: China Unicom (Myanmar) Operations Co. Ltd.[57] It has implemented Geedge systems at its data centres in Yangon and Mandalay.

In 2022, the Federal Communications Commission (FCC) revoked China Unicom (Americas) Operations Limited's authority to provide telecommunications services in the United States, citing national security risks.[58] This action stemmed from concerns about potential threats to the nation's telecommunications infrastructure, the company's ties to the Chinese government and ability to safeguard data.[59] As a result, China Unicom was required to cease its domestic and international telecommunications services in the USA by 4 April 2022. The company has also maintained its operations in Russia, through its subsidiary China Unicom (Russia), following the Russian invasion of Ukraine and international sanctions.[60]

In 2014, China Unicom initiated a US$50 million China-Myanmar cross-border optical cable system, which was first put into operation in 2017.[61] China Unicom's activities in Myanmar also involve the construction of an AAE-undersea cable system in partnership with MPT.[62]

Golden TMH Telecom Company Limited

Golden TMH Telecom Company Limited was incorporated in October 2014 and provides fibre, wireless and satellite access technologies across ten data centres in Myanmar.[63] It has implemented Geedge technology in its Yangon data centre.

The company is part of Tah Moe Hnye Group Investment and Development Co Ltd, a Yangon and Naypyidaw-based conglomerate that operates dozens of joint ventures and subsidiaries across various sectors in Myanmar, including power, energy, petroleum, telecommunication, timber, mining, real estate, industry and tourism.[64] The Group lists, as its partners, multiple military-controlled ministries and entities and foreign partners from China, Taiwan, Singapore, Malaysia and South Korea.[65]

Golden TMH Telecom's sister company, Golden TMH International Company Limited, was formed in November 2021, after the military's coup attempt and is a registered supplier to the Myanmar military's directorate of procurement. Golden

TMH Telecom and Golden TMH International share the same office address in Yangon.

Golden TMH Telecom lists several of the ISPs that implemented Geedge Network-supplied surveillance and censorship systems in Myanmar among its key providers, partners and clients.[66] These include Frontiir, MPT, Mytel, Ooredoo and KDDI (linked with MPT).

Screenshot of Tah Moe Hnye Group Investment and Development website. Source: TMH Group

Tah Moe Hnye Group Investment and Development group activities described at the company website suggests that it also implements projects with various Chinese companies that work with the Myanmar junta.[67]

Myanmar Broadband Telecom Company Limited (MBT)

MBT was established in Myanmar in 2013 and provides internet and telecom services to businesses and households in Myanmar, with its transmission network claiming to cover over 90% of Myanmar.[68] The company has deployed Geedge systems at its data centres in Yangon, Myawaddy, Muse and Tachilek.

In 2017, the company signed a strategic cooperation agreement with the Chengdu-based Troy Information Technology to develop system integration services and "internet content construction", including through the physical construction of data centres in Myanmar.[69]

Publicly available information confirms that MBT is working with unspecified partners to "build a new generation cloud data centre that will use hardware brands from the PRC and a container cloud platform developed by PRC-ASEAN

Information Harbor Co."[70] Referred to as the PRC-ASEAN Information Harbor Myanmar Cloud Computing Center, the project is overseen by Wang Xiao Yu, the Chief Executive Officer of MBT.[71]

The China-ASEAN Information Harbor is a Guangxi-based information hub and information industrial base serving southwest and central South China as well as ASEAN countries.[72] At the origins of the Information Harbour is a joint 2014 proposal by the Guangxi government and the Cyberspace Administration of China which was approved by China's State Council in 2016 and led to the establishment of a specially created joint-stock company – the China-ASEAN Information Harbor Co., Ltd (CAIH).[73] The company is mandated to carry out the construction of the information harbor and also provides digital products and services. Its shareholders include China Unicom, the investment arm of Nanning Wuxiang New Area and Qianxun Spatial Intelligence, a high-tech company jointly founded by Alibaba and the Chinese arms company NORINCO.[74]

Reporting on the 2023 Dialogue on China-ASEAN Information Harbor, the junta controlled Global New Light of Myanmar quoted the junta Deputy Minister for Transport and Communications, Lu Mon, as addressing "disinformation and cybersecurity-related matters" at the conference.[75]

Global Technology Company Limited (GlobalNet)

Myanmar company Global Technology Group provides mobile, voice, and data infrastructure, managed services, cloud computing and IT services. It has installed Geedge systems at its data centres in Mandalay, Yangon and Tachilek. The group claims to work across various sectors, including media, technology, real estate, development finance services and trading.[76]

The company claims more than 30,000 households and 3,000 enterprises as its customers,[77] including the crony companies Max Myanmar, CB Bank and Myan Shwe Pyi Tractors, the latter of which is a registered supplier of the Myanmar military's directorate of procurement.[78]

As has been previously exposed by Justice For Myanmar, GlobalNet also supplies dark fibre to Mytel.[79] Dark fibre is unused, unlit physical fibre optic cables that are available for lease and that, unlike "lit" fibre where a service provider manages the network, allows lessee companies to operate their own network, controlling their own equipment, bandwidth, and security.[80]

Myanmar Telecommunication Network Public Company Limited (MTN)

Myanmar Telecommunication Network Public Company Limited (MTN) was incorporated in 2012 and claims to be the first publicly owned telecommunication company in Myanmar. It has implemented Geedge technology at its data centres in Yangon and Tachilek.

By its own account, MTN installs international gateway systems for international communication and connectivity between Myanmar and other foreign telecommunication companies.[81] The company has actively been pursuing its own internet getaway business and operation, with the view to provide backend services to Myanmar ISPs and "government agencies" and works with Japan's KDDI for a business-to-business fibre installation project.[82] The company also collaborates with Singaporean companies Singtel Satellite and WebSatMedia for the provision of satellite services in Myanmar.[83]

According to reporting by Myanmar Now, a current board member at MTN is Myint Maung Tun, a retired major and former general manager and director at No.2 Heavy Industries Enterprise under the former military junta.[84]

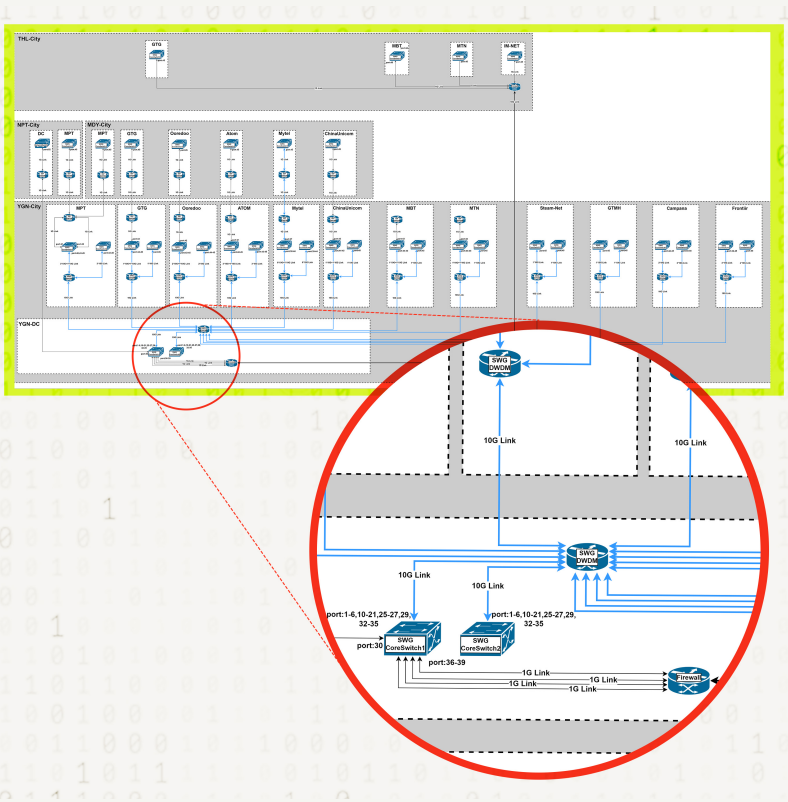
Internet Maekhong Network Company Limited (IM-Net)

IM-Net is an internet service provider operating in eastern Shan State. It has implemented Geedge products in its data centres in Kyaingtong and Tachilek. The company markets itself as a business of eastern Shan entrepreneurs.[85] The company is based in Tachileik, and has branches in Kyaingtong, Tarlay, Mong Phyak, Mong Young and Punarko.

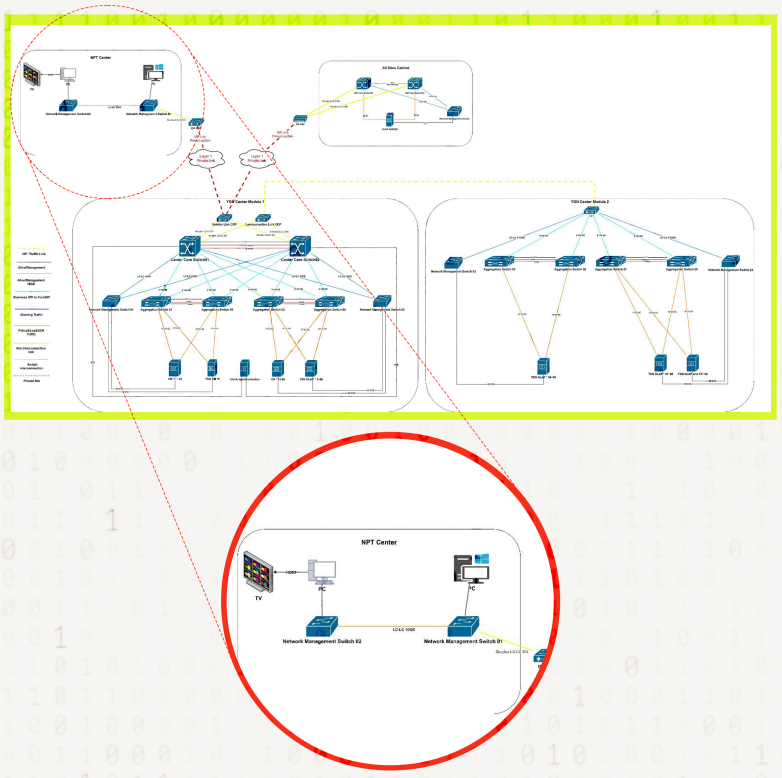
M22 现场工程实施进度表

城市	站点名称	站点到货	硬件	布线	割接链路	回传链路	标签	网络配置	系统和优化	CM	OLAP	NZ	TSGOS	大屏子系统DH	备注
YGN	Mytel临时副中心	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	MPT	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	Ooredoo	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	ATOM	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	China Unicom	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	GTG	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	Data Center	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	Stream Net	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	GTMH	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	MTN	100%	100%	100%	0%	0%	100%	100%	100%	0%	0%	0%	100%	\	24.02.16
YGN	Campana	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
YGN	Frontiir	100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	0%	100%	\	24.02.16
MDY	Mytel	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%	\	24.02.16
MDY	MPT	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
MDY	Ooredoo	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%	\	24.02.16
MDY	ATOM	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%	\	24.02.16
MDY	GTG	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
MDY	China Unicom	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
MDY	MBT	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
NPT	CCC	100%	100%	100%	100%	100%	100%	100%	\	\	\	\	\	\	24.02.16
NPT	MPT	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	\	24.02.16
NPT	POC环境	100%	100%	100%	100%	\	\	100%	100%	100%	100%	100%	100%	100%	24.02.16

Geedge project implementation progress for Myanmar as of February 2024, extracted from an HTML file in the Geedge dataset.



A diagram of the transit network topology between Myanmar ISP data centres and the junta controlled data centre in Yangon, extracted from the Geedge dataset.



A network diagram showing how junta control is centralised in Yangon and Naypyidaw using the Geedge surveillance and censorship system. The image is extracted from the Geedge dataset.

Legal Findings

Geedge designs, develops, markets and sells products that unjustifiably and excessively curtail internet users' digital freedoms and online expression, and expose civilians to real and significant risks to their physical safety. Its actions demonstrate a total disregard for human rights. Through enabling mass-scale internet control and surveillance in Myanmar, Geedge Networks is aiding the illegal junta's attempts to repress and control the civilian population.

By the nature of its business, Geedge presents itself as one of the most insidious and dangerous companies currently doing business in Myanmar. The fact that Geedge has developed custom features – based on a wish-list of the Myanmar junta – that enables arbitrary targeting through keyword filters and encryption backdoors show intent, while the seemingly total lack of respect for human rights is a testament to Geedge Networks' recklessness.

International standards on business and human rights such as the UN Guiding Principles on Business and Human Rights (Guiding Principles) consistently call for enhanced care and human rights due diligence for businesses operating in conflict-

affected environments because of the heightened risks of violations of international human rights law and international humanitarian law.[86] This is especially so in situations like present-day Myanmar, where a military junta is waging a terror campaign against civilians with repeated and significant disregard for international human rights law and international humanitarian law.

Notably, the Commentary to Guiding Principle 23 notes that conflict-affected areas may increase the risks of enterprises being complicit in gross human rights abuses committed by others and asks companies to treat this risk as a legal compliance issue, given the expanding web of potential corporate legal liability arising from extraterritorial civil claims, and from the incorporation of the provisions of the Rome Statute of the International Criminal Court in jurisdictions that provide for corporate criminal responsibility.[87] The commentary also makes clear that corporate directors, officers and employees may be subject to individual liability for acts that amount to gross human rights abuses. Geedge Networks' active engagement with the Myanmar military junta exposes individuals in directive positions within the company to criminal liability for aiding and abetting serious international crimes.

Justice For Myanmar considers that the available evidence points to a preliminary case that Geedge is aiding and abetting in the commission of international crimes carried out by members of the junta. Those international crimes are likely to be crimes against humanity including specific acts of torture and killing within a widespread or systematic attack by the junta on a primarily civilian population. In this nexus, if Geedge's technology assists the junta to identify and gather information on Myanmar's civilian internet users, a case for complicity can be made. In knowingly enabling this pipeline, individuals in directive or leadership positions within Geedge Networks become complicit in international crimes carried out by the Myanmar junta.

Under international criminal law, a company or individual is criminally liable if it provided practical assistance or means (in this case surveillance technology) that is more than likely to substantially contribute to the commission of a crime (such as torture of detained activists, whose activities and whereabouts have been identified using Geedge-supplied technology) with knowledge that their assistance would aid in the commission of the crime. The evidence is plentiful that crimes against humanity are being committed in Myanmar, and that acts, orders, and command can be attributed to individual members in, and associated with, the junta. With ongoing credible documentation and reporting at the United Nations of the human rights crisis in Myanmar,[88] Geedge Networks must have known that its collaboration with the the junta’s ministry of transport and communications is taking place in a context in which the military junta is committing repeated grave violations of international human rights and humanitarian law.

On the ground support, including support that, according to evidence in the Geedge dataset, is active and ongoing, for NCSC technicians to use Geedge Networks products for mass surveillance and targeting suggests facilitation of the junta's international crimes. Geedge Networks and individuals in directive positions within the company should therefore be investigated and, if responsible, held accountable for aiding and abetting serious international crimes. In the meantime, given Geedge Networks' knowing violations of international human rights laws, governments should impose international sanctions.

Geedge Networks is domiciled in China and is closely linked to the Chinese state. The Chinese government, under the banner of the Belt and Road Initiative, supports Geedge's expansionism and repression of the civilian population in Myanmar. The Chinese government bears liability for the actions of Geedge Networks in contributing to international law violations in Myanmar and has a responsibility to cease its exports and support. It must act now to end all Geedge collaboration with the junta.

The multiple telecommunications companies in Myanmar that have installed Geedge technology are also liable for their role in the junta's surveillance machinery and de facto human rights harms that have taken place. Telecommunication companies identified as actively facilitating junta surveillance with Geedge products should be investigated and appropriate actions – including sanctions – should be taken. In the most egregious cases, this involvement could also trigger criminal liability under international law.

Some of the telecommunications companies listed in this report have international partners and international investors. International expectations on responsible business conduct – including the Guiding Principles and the OECD Guidelines on Multinational Enterprises[89] – make clear that where a company contributes to, or may contribute to adverse human rights impacts, it should mitigate or prevent such impacts, including by using its leverage on business partners that cause the harm. These expectations also apply to investors. Investors should use their leverage to ensure that investee companies act responsibly, and, where no improvement is seen, to divest from companies that do not act responsibly.

Because the internet is broader than any physical public space, Geedge's operations in Myanmar prompt something more than alarm about systemic breaches of soft international law on business and human rights. The effect of Geedge's product is to repress the democratic power of the internet user population in Myanmar. Born in the original country of the "Great Firewall", Geedge has gone on to prioritise relationships with other repressive and authoritarian states. Through

its development of business relationships with the illegal Myanmar junta, Geedge is learning lessons about business in countries with compromised rule of law that it could potentially apply in strong democracies. Its “successes” in Myanmar should be a warning. The Federal Communications Commission (FCC) in the US has already revoked the authority of another Chinese company's authority to provide telecommunications services in the US.[90] Similar fates await the countries into which Geedge expands with the lessons it has learned, the companies it can partner with, and the case studies it can develop, in Myanmar. Geedge and its business partners in software, hardware, and technical services will only become more sophisticated against the interests of democratic countries and militarise the civilian public good that is widespread internet access. Democratic countries are at risk of allowing compromises to their own data sovereignty and regulatory control by failing to prevent the development of business models among its less democratic neighbours. These countries should urgently push back against the commercialisation of China's “Great Firewall” as a global threat.

Recommendations

Justice For Myanmar demands the following actions:

The Government of China:

1. Immediately cease the transfer of arms, equipment, technology and associated training and support to the Myanmar military junta, including software, hardware and technical assistance provided by Geedge Networks.
2. Immediately halt political and financial support for the junta and all entities under its control, including in relation to its planned sham election.
3. Recognise and support the National Unity Consultative Council (NUCC) as the highest consultative body and the National Unity Government (NUG) as the legitimate government of Myanmar, and Ethnic Resistance Organisations and federal units as key stakeholders in forming a federal union.

UN Member States:

1. Impose coordinated targeted sanctions on the Myanmar military junta and those enabling its surveillance and censorship. This must include the full networks of entities and individuals including:
    - State Security and Peace Commission (SSPC), the new name of the junta's governing body and the entity that controls the bodies responsible for the implementation of the Geedge systems, through the junta's ministry of transport and communications and its National Cyber Security Centre (NCSC). SSPC also illegally controls the telecom operator, Myanma Posts and Telecommunications (MPT).
    - Geedge Networks and its leadership, including Fang Binxing and Wang Yuandi.
    - Junta-owned and linked companies that collaborate in surveillance and censorship, prioritising Telecom International Myanmar, the operator of Mytel, which is partially owned by the military conglomerate Myanmar Economic Corporation, and the Mascots Group network, which Justice For Myanmar previously exposed.[91]
2. Provide increased support to Myanmar people to safely access the internet, bypassing surveillance and censorship, including through the funding and distribution of free tools to circumvent junta surveillance and censorship.
3. Encourage the UN Security Council to impose a global arms embargo on the Myanmar military junta, targeted sanctions on the junta's business interests, and refer the Myanmar situation to the International Criminal Court.
4. Recognise and support the National Unity Consultative Council (NUCC) as the highest consultative body and the National Unity Government (NUG) as the legitimate government of Myanmar, and Ethnic Resistance Organisations and federal units as key stakeholders in forming a federal union.
5. Consider whether they have jurisdiction to prosecute companies and individuals connected to Geedge's activities in Myanmar, and open preliminary investigations into the most serious cases thereof.
6. Australia, the European Union, Canada, United Kingdom and United States, which have imposed targeted sanctions on the military junta and its businesses, should ensure that sanctions are rigorously enforced and ensure that suspected breaches are fully investigated.

International business and investors:

1. Those already operating and invested in the telecommunications sector in Myanmar should carry out ongoing and heightened human rights due diligence to identify, mitigate and remedy harms, including from the implementation of Geedge Networks' systems, and make their findings public.
2. Investors and business partners of the telecommunication companies mentioned in this report should use their leverage to pressure companies to cease implementing surveillance on behalf of the junta and, failing that, responsibly exit.

Appendix: Geedge deployment in Myanmar

Month/ Year	Junta	Telecommunications companies
Jan 2022		**Early Operational Stage:** Six operators carried out log analysis in Yangon. The four largest ISP sites: MPT, ATOM, Ooredoo, and Mytel, and the two largest fibre optic operators: Frontiir and Campana, returned feedback to address incomplete traffic and event log collection across sites to improve network visibility and policy enforcement accuracy.
June 2022	**Proof of Concept (POC):** Geedge Networks (the provider) gave test procedures for TSG testing; POC lasts approximately 6 months. NCSC engineers received training during the POC. Provider gave two-day training on TSG architecture, policy enforcement, system logs, reports, customised signature function and VPN blocking. Joint troubleshooting and maintenance with NCSC engineers.	
	POC Environment Survey: Provider visited MPT and NCSC, checked internet topology, network interfaces, machine room; shared hardware, power and deployment documentation.	
	Hardware and Software Deployment: Installed TSG hardware at MPT and NCSC; set up software and prepared POC environment at NCSC conference room.	
	Initial tests: Provider introduced system functions, presented 18 test cases, explained VPN blocking; NCSC presented test cases to MOTC head.	
July 2022	**VPN/Application Blocking Demonstration:** Demo of TSG VPN blocking with 12 VPNs using signatures, captured and imported VPN traffic signatures into TSG.	
	Additional VPN Blocking Demo: Blocked paid VPN applications including NordVPN and ProtonVPN.	
	Rate Limiting Presentation: Presented rate limiting of YouTube on PC and smartphone.	
Aug-Sept 2022	**Function Testing by NCSC:** NCSC tested full TSG functionality for MOTC.	
Oct 2022	**Control Features Presentation:** Presented control of Psiphon, VPNs, and Viber voice calls per NCSC requirements.	
Nov 2022	**Proof of Concept ends:** Training during contract execution. Provider offered ongoing training on operation, management, and maintenance of all supplied equipment and software.	

March 2023	**Contractual period:** Drafting contract for Secure Web Gateway (SWG) system.	
Nov-Dec 2023		**SWG ISP Site Survey Report:** M22 On-site Network Planning and Program Deployment Planning.
Jan - March 2024		**M22 On-site Network Planning and Program Deployment Planning.**
April 2024	**Software licensing:** NCSC purchases licenses from Geedge Networks.	**Mytel network disruptions:** On April 29, 2024, Mytel experienced disruptions in their network links related to the SWG Project. Subsequently, their engineers removed some links from the Optical Bypass Protector (OBP) without prior notification. This action resulted in a loss of control over their traffic management. The following day, April 30, 2024,NCSC and Mytel's Technical Team met at Mytel's premises to address the network disruptions.
May 2024 onwards	**Surveillance and censorship system activation**: Junta publicly began blocking access to VPNs at the end of May 2024, an action confirmed by multiple independent reports and experienced by users nationwide	**Surveillance and censorship system activation**: Telecommunication operators implementing the Geedge system in their data centres. A July 2024 document shows the completion of infrastructure deployment at internet service providers.
Jan 2025	**Instruments of repression:** Illegal junta's "Cybersecurity Law" comes into force to underpin its attempts to control internet content and applications, and surveil user activities.	
July 2025	Junta introduces two more repressive laws: "Military Secrets Preservation and Protection Law" in an attempt by the junta to further control information flows and "Law on the Protection of Multiparty Democratic General Elections from Obstruction, Disruption, and Destruction" ahead of sham elections.	

Source: Geedge dataset, junta gazette and media reports

Endnotes

[1] Freedom House (2024), 'Freedom on the Net 2024: Myanmar,' Freedom House website, [accessed online], https://freedomhouse.org/country/myanmar/freedom-net/2024

[2] *Ibid.*

3 Rebecca L. Root (2025), 'In Myanmar, internet shutdowns hinder earthquake aid response,' Reuters website, 9 April, [accessed online], https://www.reuters.com/world/asia-pacific/myanmar-internet-shutdowns-hinder-earthquake-aid-response-2025-04-09/

[4] RFA Burmese (2024), 'Report: 1,500 arrested in Myanmar since 2022 in social media crackdown,' Radio Free Asia website, 22 February, [accessed online], https://www.rfa.org/english/news/myanmar/social-media-arrests-02222024144522.html/

[5] Human Rights Myanmar (2024), 'Myanmar's repressive use of AI to counter terrorism,' Human Rights Myanmar website, 20 August, [accessed online], https://humanrightsmyanmar.org/myanmars-repressive-use-of-ai-to-counter-terrorism

[6] NRK (2025), 'Telenors mareritt', NRK website, [accessed online], https://radio.nrk.no/podkast/radiodokumentaren/sesong/telenors-mareritt/

[7] VOA Burmese (2025), 'Myanmar's new cybercrime law will suppress information, say analysts,' Voice of America website, 3 January, [accessed online], https://www.voanews.com/a/myanmar-s-new-cybercrime-law-will-suppress-information-say-analysts/7923821.html

[8] 'Cybersecurity Law: State Administration Council Law No. 1/2025,' ICNL website, 1 January, [accessed online], https://www.icnl.org/resources/library/cybersecurity-law-state-administration-council-law-no-1-2025; JURIST (2025), 'Myanmar enacts cybersecurity law restricting digital communication,' JURIST website, 3 January, [accessed online], https://www.jurist.org/news/2025/01/myanmar-enacts-cybersecurity-law-restricting-digital-communication/

[9] JURIST (2025), 'Myanmar enacts cybersecurity law restricting digital communication,' JURIST website, 3 January, [accessed online], https://www.jurist.org/news/2025/01/myanmar-enacts-cybersecurity-law-restricting-digital-communication/

[10] 'Military Secrets Preservation and Protection Law: State Administration Council Law No. 44/2025,' Lincoln Myanmar website, 28 July, [accessed online], https://www.lincolnmyanmar.com/wp-content/uploads/2025/07/Military-Secrets-Preservation-and-Protection-Law.pdf

[11] The Irrawaddy (2025), 'First person charged under junta's draconian election protection law,' The Irrawaddy Facebook, 26 August, [accessed online], https://www.facebook.com/theirrawaddy/posts/first-person-charged-under-juntas-draconian-election-protection-lawaugust-26-202/1212226474265841/

[12] The Irrawaddy (2025), 'Myanmar junta planning joint security firm with China,' The Irrawaddy website, 15 November, [accessed online], https://www.irrawaddy.com/news/myanmar-china-watch/myanmar-junta-planning-joint-security-firm-with-china.html

[13] InterSecLab (2025), 'The Internet Coup: A Technical Analysis on How a Chinese Company is Exporting The Great Firewall to Autocratic Regimes,' InterSecLab organization website, 9 September, [accessed online], https://interseclab.org/research/8

[14] Amnesty International (2025) 'Shadows of Control: Censorship and Mass Surveillance in Pakistan,' Amnesty International website, 9 September, [accessed online], https://www.amnesty.org/en/documents/asa33/0206/2025/en/

[15] Sohu (2024), '海南省方滨兴院士工作站在海南生态软件园揭牌,' Sohu website, 11 January, [accessed online], https://www.sohu.com/a/751088620_121719902

[16] Tania Branigan (2011), 'China Great Firewall creator pelted with shoes,' The Guardian website, 20 May, [accessed online], https://www.theguardian.com/world/2011/may/20/china-great-firewall-creator-pelted-shoes

17 Sohu (2024), op. cit.; Chinese Academy of Sciences Institute of Information Engineering,' LinkedIn website, [last accessed on September 2, 2025], https://www.linkedin.com/company/%E4%B8%AD%E5%9B%BD%E7%A7%91%E5%AD%A6%E9%99%A2%E4%BF%A1%E6%81%AF%E5%B7%A5%E7%A8%8B%E7%A0%94%E7%A9%B6%E6%89%80?trk=ppro_cprof

[18] Sohu (2024), *op. cit.*

[19] Justice For Myanmar (2024), 'The Myanmar junta's partners in digital surveillance and censorship,' Justice For Myanmar website, 19 June, [accessed online], https://www.justiceformyanmar.org/stories/the-myanmar-juntas-partners-in-digital-surveillance-and-censorship

[20] Sohu (2024), *op. cit.*

[21] San Yamin Aung (2017), 'China Burma sign five agreements,' The Irrawaddy website, 17 May, [accessed online], https://www.irrawaddy.com/news/burma/china-burma-sign-five-agreements.html

[22] Thu Thu Aung and Poppy McPherson (2020), 'Myanmar China ink deals to accelerate Belt and Road as Xi courts an isolated Su,' Reuters website, 18 January, [accessed online], https://www.reuters.com/article/world/myanmar-china-ink-deals-to-accelerate-belt-and-road-as-xi-courts-an-isolated-su-idUSKBN1ZH053/

[23] Nan Lwin (2018), 'China Myanmar agree 15 point MOU economic corridor,' The Irrawaddy website, 6 July, [accessed online], https://www.irrawaddy.com/news/burma/china-myanmar-agree-15-point-mou-economic-corridor.html

[24] The Lowy Institute (2025) 'China's tightrope walk mediating Myanmar,' The Lowy Institute website, 19 March, [accessed online], https://www.lowyinstitute.org/the-interpreter/china-s-tightrope-walk-mediating-myanmar

[25] Council on Foreign Relations, 'Assessing China Digital Silk Road,' Council on Foreign Relations website, [last accessed on September 2, 2025], https://www.cfr.org/china-digital-silk-road/

[26] Sohu (2024), *op. cit.*

[27] Nay Lin Tun (2022), 'The Relationship Between ICT Development and Economic Growth In Myanmar,' Master Of Development Studies Programme, Department Of Economics, Yangon University Of Economics, October, [accessed online], https://meral.edu.mm/record/8533/files/Nay%20Lin%20Tun,%20EMDevS-30%20(17th%20Batch).pdf

[28] Elizabeth C Economy (2018), 'The great firewall of China: Xi Jinping's internet shutdown,' The Guardian website, 29 June, [accessed online], https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

[29] 'Tiangou Secure Gateway English,' Geedge Networks website, [last accessed on September 2, 2025], https://www.geedgenetworks.com/tiangou-secure-gateway-english/

[30] 'Encrypted Traffic Visibility,' Geedge Networks website, [last accessed on September 2, 2025], https://www.geedgenetworks.com/encrypted-traffic-visibility/

[31] InterSecLab (2025), 'The Internet Coup: A Technical Analysis on How a Chinese Company is Exporting The Great Firewall to Autocratic Regimes,' InterSecLab organization website, 9 September, [accessed online], https://interseclab.org/research/8

[32] Sumitomo Corporation (2025), ' Amendment of Telecommunications Business Agreement in Myanmar,' Sumitomo Corporation website, 28 April, [accessed online], https://www.sumitomocorp.com/en/mideast-africa/news/important/group/20250428

[33] KDDI (2025), 'ミャンマーにおける通信事業の契約改定について [Revision of telecommunications contracts in Myanmar],' KDDI website, 28 April, [accessed online], https://newsroom.kddi.com/news/detail/kddi_nr_s-34_3804.html

[34] KDDI (2021), 'ミャンマーにおける通信事業への取り組みについて,' KDDI website, 29 September, [accessed online], https://news.kddi.com/kddi/corporate/csr-topic/2021/09/29/5443.html

[35] Sumitomo Corporation (2021), Sumitomo Corporation's Stance on Telecommunications Business in Myanmar,' Sumitomo Corporation website, 29 September, [accessed online], https://www.sumitomocorp.com/en/jp/news/important/group/20210929

[36] Justice For Myanmar (2023), 'Israeli surveillance firm Cognyte's business in Myanmar exposed,' Justice For Myanmar website, 15 January [accessed online], https://www.justiceformyanmar.org/stories/israeli-surveillance-firm-cognytes-business-in-myanmar-exposed

[37] Justice For Myanmar (2020), 'Nodes of Corruption, Lines of Abuse,' Justice For Myanmar website, 20 December, [accessed online], https://www.justiceformyanmar.org/stories/nodes-of-corruption-lines-of-abuse-how-mytel-viettel-and-a-global-network-of-businesses-support-the-international-crimes-of-the-myanmar-military

[38] Telenor Myanmar (2021), 'Telenor Group sells Telenor Myanmar to M1 Group,' Telenor website, 8 July, [accessed online], https://www.telenor.com/media/newsroom/telenor-group-sells-telenor-myanmar-to-m1-group/

[39] Justice For Myanmar (2021), 'Military linked company Shwe Byain Phyu has taken control of Telenor Myanmar,' Justice For Myanmar website, [accessed online], https://www.justiceformyanmar.org/press-releases/military-linked-company-shwe-byain-phyu-has-taken-control-of-telenor-myanmar

[40] I*bid.*

[41] Ooredoo (2023), 'Ooredoo Q.P.S.C: Group structure and presence,' Ooredoo website, 8 May, [accessed online], https://www.ooredoo.com/wp-content/uploads/2023/05/Ownership-structure-.pdf

[42] Human Rights Watch (2013), 'Letter to Dr. Nasser Marafih, CEO Ooredoo,' Human Rights Watch website, 3 May, [accessed online], https://www.hrw.org/news/2013/05/03/letter-dr-nasser-marafih-ceo-ooredoo; MCRB, IHRB and DIHR (2015), 'Myanmar ICT Sector-Wide Impact Assessment,' Myanmar Centre for Responsible Business website, September [accessed online], https://www.myanmar-responsiblebusiness.org/pdf/SWIA/ICT/complete.pdf

[43] Ooredoo (2022), 'Ooredoo Group announces the sale of its telecom business in Myanmar to Nine Communications Pte Ltd at an enterprise value of USD 576 million,' Ooredoo website, 8 September, [accessed online], https://www.ooredoo.com/en/media/news_view/ooredoo-group-announces-the-sale-of-its-telecom-business-in-myanmar-to-nine-communications-pte-ltd-at-an-enterprise-value-of-usd-576-million/

[44] Ooredoo (2025), 'Ooredoo Group achieves sustainable growth reflecting operational strength and strategic investments,' Ooredoo website, 30 July, [accessed online], https://www.ooredoo.com/en/media/news_view/ooredoo-group-achieves-sustainable-growth-reflecting-operational-strength-and-strategic-investments/

[45] 'Overview,' Frontiir website, [last accessed on September 2, 2025], https://www.frontiir.com/about_us/overview/; 'Founder and Co-Founders,' Frontiir website, [last accessed on September 2, 2025], https://www.frontiir.com/about_us/governance-of-frontiir/

[46] Nick Mathiason and Christian Eriksson (2020), 'Revealed: UK's overseas aid fund is major investor in company linked to media crackdown in Myanmar,' Finance Uncovered website, 9 June, [accessed online], https://www.financeuncovered.org/stories/revealed-uks-overseas-aid-fund-is-major-investor-in-company-linked-to-media-crackdown-in-myanmar

[47] Caroline Henshaw and Aung Naing (2025), 'British Norwegian and Danish governments back internet provider in military run Myanmar which hosts notorious Chinese surveillance system,' Finance Uncovered website, 21 May, [accessed online], https://www.financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system

[48] MOTC (2017), 'Telecommunication Licence Issued List,' Ministry of Transport and Communications Myanmar website, 6 July, [accessed online], https://www.motc.gov.mm/sites/default/files/Telecommunication%20Licence%20Issued%20List%20%285-7-2017%29PDF.pdf

[49] James Pearce (2018), 'Campana raises 40M to fund network expansion in ASEAN region,' Capacity Media website, 18 September, [accessed online], https://www.capacitymedia.com/article/29ot42ikril15nn07ww4o/news/campana-raises-40m-to-fund-network-expansion-in-asean-region

[50] ZMS (2023), 'First Singapore private submarine cable project to start facilities in Myanmar,' ZMS Cable website, 29 January, [accessed online], https://m.zmscable.com/new/First-Singapore-Private-Submarine-Cable-Project-To-Start-Facilities-In-Myanmar

[51] Ramakrishna Padmanabhan, Arturo Filastò, Maria Xynou, Ram Sundara Raman, Kennedy Middleton, Mingwei Zhang, Doug Madory, Molly Roberts, and Alberto Dainotti (2021), 'A multi-perspective view of Internet censorship in Myanmar,' Ramakrishnan SR website, 27 August, [accessed online], https://ramakrishnansr.com/assets/myanmar.pdf

[52] Ministry of Science and Technology (2017), 'VNPT launches StreamNet in Myanmar,' Vietnam's Ministry of Science and Technology website, 30 October, [accessed online], https://english.mic.gov.vn/vnpt-launches-streamnet-in-myanmar-197135901.htm

[53] Justice For Myanmar (2020), 'Nodes of Corruption, Lines of Abuse,' *op. cit.*

[54] Trung Ngoc (2017), 'Vietnam Posts and Telecommunications Group invests abroad to set up a JV in Myanmar,' The Leader Vietnam website, 1 November, [accessed online], https://e.theleader.vn/vietnam-posts-and-telecommunications-group-invests-abroad-to-set-up-a-jv-in-myanmar-d2853.html

[55] Justice For Myanmar (2020), 'Nodes of Corruption, Lines of Abuse,' *op. cit.*

[56] Myanmar Business Today (2014), 'Vietnamese Telecom Firm Enters Myanmar,' Myanmar Business Today website, 28 September, [accessed online], https://mmbiztoday.com/vietnamese-telecom-firm-enters-myanmar/; Terabit Wave Company Limited, 'VNPT signed MOU with Terabit Wave,' Terabit Wave website, [last accessed on September 2, 2025], https://www.terabitwave.com/news.html

[57] China Unicom (Hong Kong) Limited (2024), 'Annual Report 2024,' China Unicom website, [accessed online], https://www.chinaunicom.com.hk/en/ir/reports/ar2024.pdf

[58] Federal Communications Commission (2022), 'China Unicom Stop US Services,' FCC website, [accessed online], https://www.fcc.gov/consumers/guides/china-unicom-stop-us-services

[59] The Select Committee on the CCP (2025), 'House Committee subpoenas Chinese telecom giants after refusal to disclose CCP and military links,' House Select Committee on the CCP website, 24 April, [accessed online], https://selectcommitteeontheccp.house.gov/media/press-releases/house-committee-subpoenas-chinese-telecom-giants-after-refusal-disclose-ccp

[60] China Unicom (Hong Kong) Limited (2024), 'Annual Report 2024,' China Unicom website, [accessed online], https://www.chinaunicom.com.hk/en/ir/reports/ar2024.pdf

[61] Xinhua News Agency (2017), 'China Unicom's Myanmar cable project completes first commercial circuit,' IM Silk Road website, 26 October, [accessed online], https://en.imsilkroad.com/p/66334.html

[62] *Ibid.*

[63] DataCenter Map, 'Golden TMH Telecom Co Ltd GTMH,' DataCenter Map, [accessed online], https://www.datacentermap.com/c/golden-tmh-telecom-co-ltd-gtmh/

[64] Tah Moe Hnye Group, 'About Us,' TMH Group website, [last accessed on September 2, 2025], https://tmhgroupmm.com/about-us/

[65] Tah Moe Hnye Group, 'Business Scope,' TMH Group website, [last accessed on September 2, 2025], https://tmhgroupmm.com/business-scope/

[66] GTMH Telecom, 'Partners,' GTMH Telecom website, [last accessed on September 2, 2025], https://www.gtmh-telecom.com/partners/

[67] Tah Moe Hnye Group, 'Business Scope,' TMH Group website, [last accessed on September 2, 2025], https://tmhgroupmm.com/business-scope/

[68] 'Myanmar Broadband Telecom Co Ltd,' LinkedIn website, [last accessed on September 2, 2025], https://mm.linkedin.com/company/myanmar-broadband-telecom-co--ltd

[69] TROY Information Technology (2017), 'Announcement of collaboration strategy,' China Next website, 22 November, [accessed online], http://chinext.zqrb.cn/pdf/20171121/news-182-444953.pdf

[70] Greater Mekong Subregion Economic Cooperation Program (2024), 'Regional Investment Framework 2025-2027' Greater Mekong website, September [accessed online], https://www.greatermekong.org/g/sites/default/files/SERC-RIF%202025-2027_final%20web%20PDF_4OCT.pdf

[71] *Ibid.*

[72] China-ASEAN Information Harbor website, [last accessed on September 2, 2025], https://www.caih.com/?lang=en_US

[73] Dr Ngeow Chow-Bing (2021), 'China-ASEAN Information Harbor: The Digital Silk Road from Guangxi to Southeast Asia,' Friedrich Ebert Stiftung, August [accessed online], https://library.fes.de/pdf-files/bueros/indonesien/18185.pdf; 'CAIH Info Tech Malaysia,' LinkedIn website, [last accessed on September 2, 2025], https://www.linkedin.com/company/caih-info-tech-malaysia

[74] 'China-ASEAN Information Harbor Co Ltd,' CN Verify website, [last accessed on September 2, 2025], https://www.cnverify.com/company/China-Asean-Information-Harbor-Co-Ltd; Luz Ding (2020), 'Is Alibaba backed navigation service Qianxun at risk from US sanctions?' The China Project website, 16 November, [accessed online], https://thechinaproject.com/2020/11/16/is-alibaba-backed-navigation-service-qianxun-at-risk-from-u-s-sanctions/

[75] KTZH (2023), 'Myanmar's active participation in China-ASEAN Information Harbour process,' Global New Light of Myanmar website, 10 November, [accessed online], https://www.gnlm.com.mm/myanmars-active-participation-in-china-asean-information-harbour-process/

[76] Global Technology Company Limited, 'About Us,' GlobalNet Myanmar website, [last accessed on September 2, 2025], https://www.globalnet.com.mm/about-us/

[77] Global Technology Company Limited, 'Solution,' GlobalNet Myanmar website, [last accessed on September 2, 2025], https://www.globalnet.com.mm/solutions/

[78] Global Technology Company Limited, 'Industries,' GlobalNet Myanmar website, [last accessed on September 2, 2025], https://www.globalnet.com.mm/industries/

[79] Justice For Myanmar (2020), 'Nodes of Corruption, Lines of Abuse,' *op. cit.*

[80] 'What is dark fiber?' Spectrum Enterprise website, [last accessed on September 2, 2025], https://enterprise.spectrum.com/support/faq/internet/what-is-dark-fiber.html

[81] 'IGW Services,' MTN PCL website, [last accessed on September 2, 2025], https://mtnpcl.com/igw-services/

[82] 'Fiber Services,' MTN PCL website, [last accessed on September 2, 2025], https://mtnpcl.com/fiber-services/

[83] 'MTN Profile,' MTN PCL website, [last accessed on September 2, 2025], https://mtnpcl.com/mtn-profile/; 'Asia,' WebSat Media website, [last accessed on September 2, 2025], https://www.websatmedia.com/coverage/asia

[84] Khin Moh Moh Lwin and Thaw Zin Myo (2020), 'The PPP, a party of NLD defectors, military men and ultranationalists,' Myanmar Now website, 4 November, [accessed online], https://myanmar-now.org/en/news/the-ppp-a-party-of-nld-defectors-military-men-and-ultranationalists/

[85] Internet Maekhong, 'Our Services,' Internet Maekhong website, [last accessed on September 2, 2025], https://www.internetmaekhong.com/

[86] Office of the United Nations High Commissioner for Human Rights (OHCHR) (2011), 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,' [accessed online], OHCHR website, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[87] *Ibid.*

[88] Special Rapporteur on the situation of human rights in Myanmar (2025), 'Situation of human rights of Rohingya Muslims and other minorities in Myanmar,' OHCHR website, 29 August, [accessed online], https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session60/advance-version/a-hrc-60-20-aev.pdf; Special Rapporteur on the situation of human rights in Myanmar (2025), 'Address to the 58th session of the UN Human Rights Council,' OHCHR website, 19 March, [accessed online], https://www.ohchr.org/sites/default/files/documents/countries/myanmar/statements/2025-03-19-tom-andrews-address-to-58th-hrc.docx; Special Rapporteur on the situation of human rights in Myanmar (2024), 'Banking on the Death Trade: How Banks and Governments Enable the Military Junta in Myanmar,' OHCHR website, 26 June, [accessed online], https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session56/a-hrc-56-crp-7.pdf; Special Rapporteur on the situation of human rights in Myanmar (2023), 'The Billion Dollar Death Trade: The International Arms Networks that Enable Human Rights Violations in Myanmar,' OHCHR website, 17 May, [accessed online], https://www.ohchr.org/sites/default/files/documents/countries/myanmar/crp-sr-myanmar-2023-05-17.pdf.

[89] Organisation for Economic Co-operation and Development (OECD) (2023), 'OECD Guidelines for Multinational Enterprises on Responsible Business Conduct' OECD website, [accessed online], https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_a0b49990/81f92357-en.pdf

[90] Federal Communications Commission (FCC) (2022), 'Order On Revocation', FCC website, 2 February, [accessed online], https://docs.fcc.gov/public/attachments/FCC-22-9A1.pdf

[91] Justice For Myanmar (2024), 'The Myanmar junta's partners in digital surveillance and censorship,' *op. cit*

JUSTICE FOR MYANMAR

justiceformyanamr.org