REPORT

NATIONAL WEB PORTAL DEVELOPMENT OR REPRESSION?

/////////////////// **BURMA, NOVEMBER 2010** ///

REPORTERS
WITHOUT BORDERS
FOR PRESS FREEDOM

Yatanarpon Teleport, a company based in Yatanarpon IT City in Pyin Oo Lwin (Mandalay Division), launched the first National Web portal in October, portraying it as a significant step forward in the country's development of information technology and the Internet.

At the opening ceremony, attended by Prime Minister Thein Sein, other senior officials and IT technicians, Yatanarpon Teleport said it was offering Burmese users a high-tech communication FTTH (fiber to the home) system comprising Internet, VOIP telephone and IPTV channels. The triple services – VOIP telephone, Internet, IPTV – will be available from a single fiber cable network with a higher speed than Wi Max, ADSL and dial-up systems that are currently in use. Several IT companies including China's ZTE and Huawei, which have been involved in building the cyber city, displayed products that they said "suit" Burma (Myanmar). This report will analyze the Myanmar National Web Portal and determine whether it represents a true IT development for the nation or an attempt to extend the military's repression of its citizens.

INTERNET LINKS

The Internet link currently used in Burma is the Sea-Me-We-3 Cyber Link through Singapore. It also links with trans-border cables of China and Thailand via the Greater Mekong Sub-Region Information Superhighway Link and of India (Figures 1 & 2). Burma can communicate with 34 countries through these links

Figure 1: Myanmar Post and Telecommunication's International backbone Link

Figure 2: Burma's connection with Greater Mekong Sub-Region Information Superhighway Links and India

So far, more than 10,000 km of fiber-optic cable have been installed across Burma covering almost all states and divisions (Figure 3).
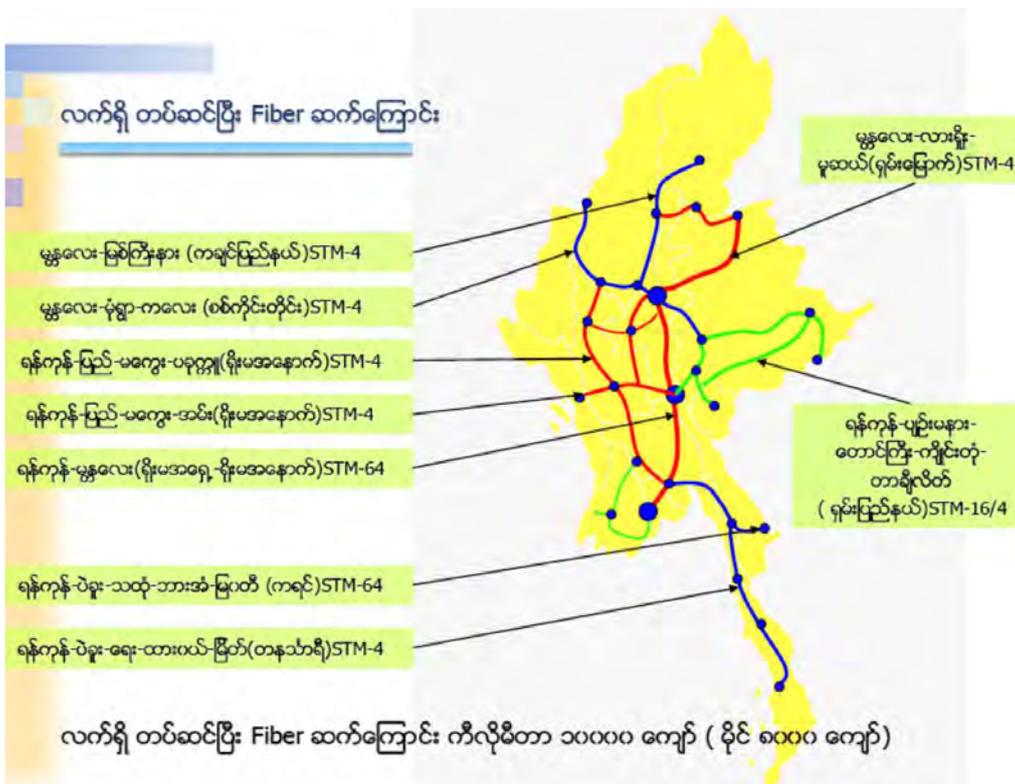

Figure 3: Current status of Burma's fiber-optic cable links (more than 10,000 km)

According to Yatanarpon Teleport, two main ISP centers in Naypyidaw and Yatanarpon, and regional sub-ISP centers in Rangoon, Myitkyina, Taungyi, Lashio, Monywa, Magwe and Myeik will provide Internet service to various regions of the country (Figure 4).
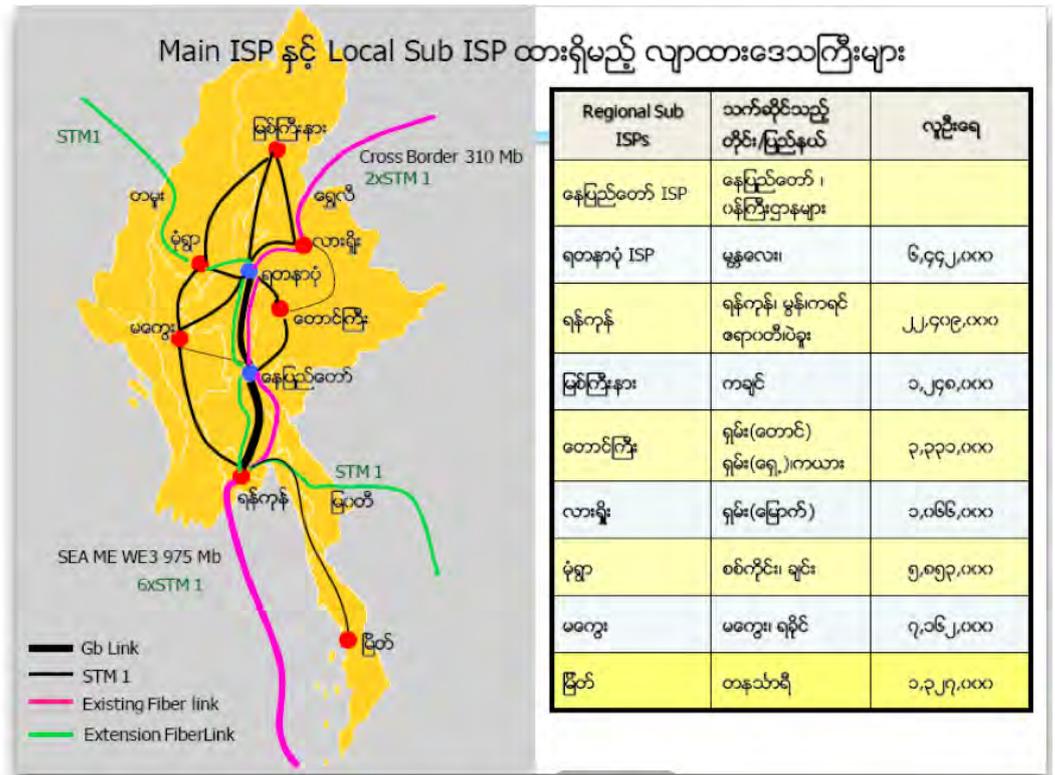
Figure 4: Planned Regions for Main and Sub ISPs

It is expected that the Hantharwaddy National Gateway will be able to provide a total bandwidth of 3.145 Gbps, a significant rise from the total bandwidth of 1.285 Gbps registered in March 2010 (Figure 5).
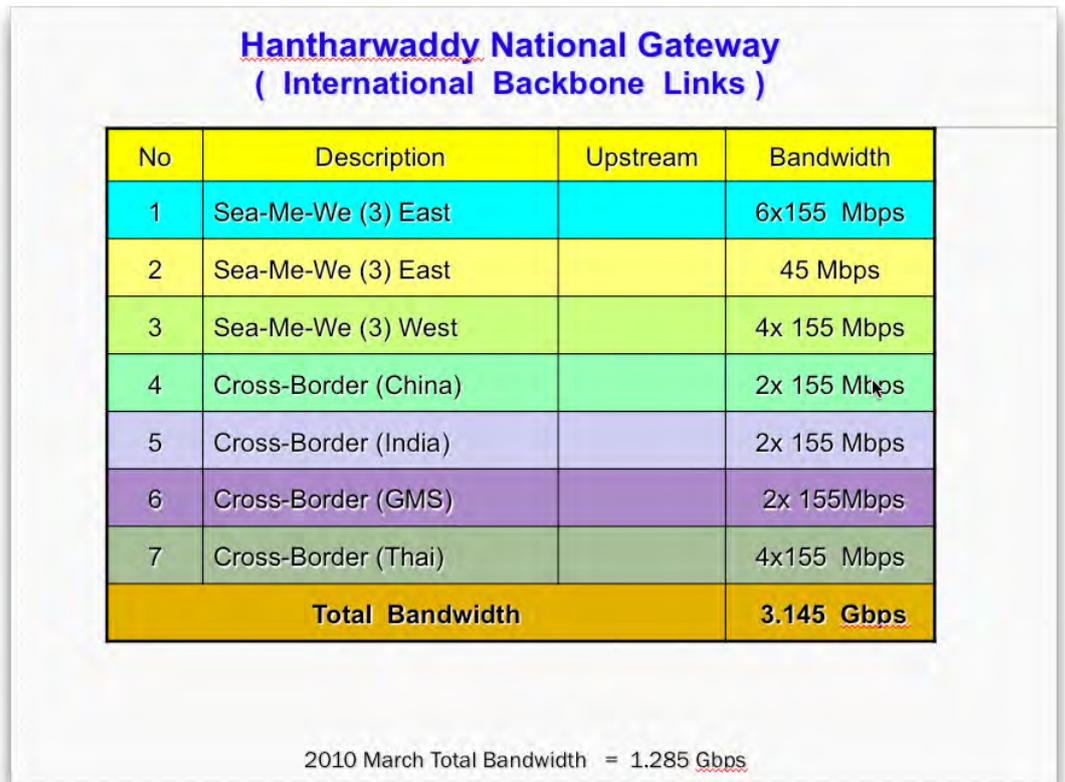

Figure 5: Total bandwidth provided by Hantharwaddy National Gateway

Yatanarpon Teleport has also planned to link with the Sea-Me-We-4 Cyber Link, an Asia-Europe submarine cable, via Bangladesh, which is the nearest country to the submarine cable. After completion of the project, the country will be able to communicate with other countries that link Sea-Me-We-4 via fiber-optic connection.

ISP SYSTEMS

Previous System *(Figures 6 and 7)*

From 2004 until October 2010, Burma used an ISP system that consisted of two ISP servers. A Ministry of Post and Telecommunications (MPT) ISP server provided Internet services to government ministries including the Ministry of Defence (MoD) and ADSL/dial-up private users. An ISP server from Yatanarpon Teleport also provided Internet services to private users (dial-up, ADSL, FTTH, wireless/broadband).

After passing through Hantharwaddy National Gateway, Internet users could connect to the global Internet via SEA-ME-WE 3 and China-Burma cross-border fiber-optic cables. Hantharwaddy National Gateway is directly controlled by the military.

Note: The ISP service of the Bagan Cyber Tech, created in 1990 by former Prime Minister Khin Nyunt, was taken over by Myanmar Teleport, which in 2004 was transformed into Yatanarpon Teleport.
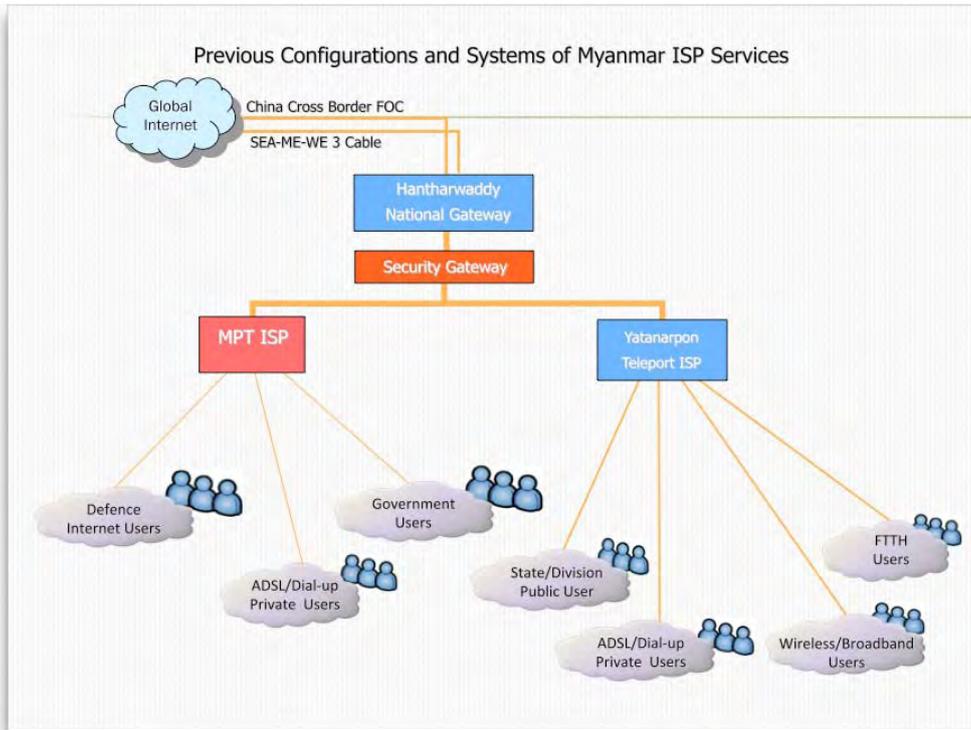
Figure 6: Configurations and systems of Myanmar ISP Services (2004-October 2010)

Previous ISP system required all Internet requests to go through proxy servers in Yangon (Rangoon). The old system also created a bottleneck for military and government users, as they had to share the same ISP with private users. Web performance was also less than impressive.

Figure 7: Previous ISP Processing System (2004-October 2010)

New System *(Figures 8, 9 and 10)*
The new ISP system consists of two main servers – the MPT ISP and the newly-created Ministry of Defence (MoD) ISP. The Yatanarpon Teleport ISP and the newly-established Naypyitaw ISP are placed under the MPT ISP. The MoD ISP will solely serve Internet users from the Ministry of Defence while the Naypyitaw ISP will provide Internet service to other government ministries. The Yatanarpon ISP on the other hand will only serve civilian Internet users. By using existing cables and newly linked SEA-ME-WE 4 cables, Burmese Internet users will be able to connect to the global Internet via Hantharwaddy National Gateway.

The new ISP system will decrease loading on the National Gateway and main ISP. There will only be router-to-router request between core network and aggregate network. It will also make more bandwidth available between local ISPs, giving better Web performance for end users. However, the new system requires Internet requests to go through even more ISP servers and therefore users are subjected to more screening and controls. In addition to other Web services, Yatanarpon Teleport will also offer Ymail and Ytalk, which they expect Burmese users would use in the future instead of Gmail and Gtalk.

Figure 8: Configurations and systems of Myanmar ISP Services (October 2010 onwards)

Figure 9: New ISP processing system (October 2010 onwards)

In addition, the MoD will not only control its own IP router and optical transport equipment, but will also control those of the Hantharwaddy National Gateway, giving the military an exclusive ability to control the country's Internet system (Figure 10).

Figure 10: ISP system map (October 2010 onwards)

POSSIBLE PERFORMANCE, RELIABILITY AND STABILITY PROBLEMS

In the earliest Burmese Internet system (before 2004), Internet requests were sent through modems to the PSTN (Public Switch Telephone Network), which in turn submitted them to the respective ISPs. An ISP proxy server would forward these requests to the proper domains (Figure 11).

Figure 11: Internet request processing system (before 2004)

From 2004 to October 2010, Internet requests had to go through Yatanarpon Teleport, the Security Gateway and the National Gateway before they could reach the intended domains (Figure 12).

Figure 12: Internet request processing system (2004-October 2010)

In the new Internet system, users are separated into three different groups sharing the total bandwidth of 3.145 Gbps. While fewer defence service users and government service users enjoy the entire bandwidth of the MoD ISP and Naypyitaw ISP, public users from the entire country have to share the Yatanarpon ISP (Figure 8). Assuming that all three ISPs equally share the entire bandwidth of slightly more than 1 Gbps, the military and the government will get better bandwidth than civilian users. If that is the case, public users are most likely to face performance problems such as bandwidth limitation controls, congested data traffic, reduced connection speed and connection time out, which in turn could destabilize the route.

POSSIBLE SECURITY IMPLICATIONS WITH NEW ISP SYSTEM

It is widely believed that the main reason for segregating users into different groups and allocating them to designated servers is to make it easier for the government to control Internet traffic. In time of civil unrest, for example, the government could shut down Yatanarpon ISP to block blogs and news reports by bloggers and journalists. Another security concern is the safety of Internet users' login credentials. The following two attack mechanisms are likely to be placed in the new ISP systems.

1.Sniffing or MITM (Man in the Middle) attacks (Figure 13)

Since user requests, server responses, login information and requested data are sent through the ISPs, the ISPs have opportunities to perform sniffing to capture packets and user information by installing a sniffer in their network. It is also possible for the ISP to perform MITM attacks to get user information and to change the actual data.

Figure 13: Sniffing attack

2.DNS spoofing / DNS poisoning (Figure 14)

ISPs may also perform DNS spoofing or DNS poisoning for the purpose of phishing (social engineering attacks). There has been speculation that military intelligence is already using such methods to watch popular webmail services such as Gmail and Facebook. In that system, login credentials that pass through the proxy of the ISP are intercepted by a fake Gmail/Facebook server. The fake server would then transfer the login request to the actual server, which would process the request and send feedback to the user. In most cases, users would not know that their login credentials have been logged by a fake server.

Figure 14: DNS spoofing / DNS poisoning

CONCLUSION

It is expected that the Yatanarpon Myanmar National Web Portal will provide faster bandwidth and improved Web services to Burmese Internet users. However, according to the current setup, only users from the government ministries, especially those from the Ministry of Defence, will enjoy faster Internet connection and consequently better Web services.

The FTTH high-tech communication system is an impressive development compared with the previous system. It can also be assumed that the new system will cost more. However, given the low per capita income in Burma, only a tiny fraction of the public will be able to enjoy the FTTH system.

The segregated nature of the new ISP system would also allow the authorities to shut down the civilian ISP without affecting the two other ISPs that serve the government and the military. The authorities are likely to use that opportunity to stifle freedom of press and expression.

The new system also grants the military exclusive control over the Hantharwaddy National Gateway. The military is therefore now in a position to spy on all Burmese citizens – civilians, soldiers and government service personnel.

For more information:
Burma Media Association / Maung Maung Myint: myintm@bma-online.org - www.bma.co.cc. Tel: +47 92061348. Fax: +47 52729174
Reporters Without Borders / Lucie Morillon - New Media Desk: internet@rsf.org
Contact Presse : presse@rsf.org - + 33 1 44 83 84 71