UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Southeast Asia CyberWatch: May 2013

A monthly report on trends in online censorship, information operations,

and Internet use in Southeast Asia

Table of Contents

BRUNEI

Internet users complain of slow speeds

Internet users are complaining about connection speeds in Brunei, comparing the effects of poor connectivity to censorship. A recent article in the Brunei Times asserted that the country has the most expensive Internet rates among ASEAN (Association of Southeast Asian Nations) member countries, with a monthly average charge of $81.20 for broadband Internet service. While Brunei's bandwidth is not the lowest in the region, a Brunei Times Twitter survey revealed many users' complaints that they do not get what the pay for.

CAMBODIA

Cambodian Center for Human Rights releases briefing on Internet Censorship
The Cambodian Center for Human Rights (CCHR), a Phnom Penh-based non-governmental organization, has released a report on freedom of expression in Cambodia. The report [PDF] deals primarily with Internet censorship in the country, detailing technical and legal restrictions on free speech via new media. While the CCHR points out that the Cambodian constitution guarantees the right to freedom of expression in accordance with the Universal Declaration of Human Rights, it expresses concern for recent indications that the Cambodian government is drafting "its first ever cyber law to regulate and to limit the use of the internet." It outlines several cases of Internet censorship since the beginning of 2011 and proposes several recommendations to ensure the free flow of information online, including better legal approaches toward dealing with illegal content.

INDONESIA

Indonesia and Australia open joint cybercrime office
The Indonesian National Police and Australian Federal Police have opened a second joint cyber crime office in Jakarta. The partnership began in 2011, when the two police forces launched the Cyber Crime Investigation Center, also in Jakarta. Both countries will use the offices to share information with each other and coordinate investigation efforts in order to battle increasingly frequent and complex cyber crimes originating from inside Indonesia. Commander General Nanan Sukarna, the deputy police chief, stated that Indonesia would seek out similar partnerships with other countries. Indonesia and fellow ASEAN member-countries formed a cyber defense network with Japan in November 2012.

MALAYSIA

Network interference ahead of the Malaysian general election
Ahead of the 2013 General Elections, the Malaysian Communications and Multimedia Commission (MCMC) assured Malaysians that it had not detected any restrictions on user access by Internet service providers as suspected. At the same time, the commission cautioned that Internet users might experience slower speeds as a result of a significant increase in traffic "related to GE13." It did not, however, rule out the possibility that some websites could be knocked offline by DDoS attacks and warned citizens to steer clear of the "crossfire of the cyberwar waged by cybertroopers." Access, a non-governmental organization, contested the MCMC's claims and found compelling evidence of "DPI or HTTP path based interference" at the local ISP level. On May 25, two weeks after the elections, the Democratic Action Party (DAP) submitted an official complaint to the MCMC that websites, YouTube videos, and social media pages related to DAP had experienced an "Internet blockade." DAP specifically cited evidence of Deep Packet Inspection and filtering tools built by Arbor Networks and branded by Telekom Malaysia.

Government to investigate social media use

The MCMC has stated that it will "review all aspects of the law, control and education, pertaining to the abuse of social media." Datuk Seri Ahmad Shabery Cheek, minister of the MCMC, asserted that the review would aim to ensure that current Malaysian law adequately addresses social media use. At the same time, the Malaysian Home Ministry announced that it would work together with the MCMC and Malaysian Cyber Security to "ensure that information channelled by individuals or cyber groups through the various social media... were transparent and correct." The initiative is allegedly in response to complaints and media reports about slander on social media.

MYANMAR

Aung San Suu Kyi a likely target of hackers

Representatives from Anonymous have announced a new Internet campaign aimed at supporting Myanmar's Muslim Rohingya community. The campaign will focus on the Burmese government sites, the United Nations (for not involving itself through peacekeeping operations), and even potentially pro-democracy leader Aung San Suu Kyi over her lack of action regarding widespread anti-Rohingya violence. As previously reported, Anonymous has previously raised awareness on the plight of the Rohingya community through a massive Twitter campaign.

Foreign telecom firms compete for Myanmar's market

Burma's leaders are reportedly holding a license competition for 12 of the world's leading telecommunications firms, including Digicel, Vodafone, China Mobile, Qatar Telecom. Of those international firms competing for licensing rights, the country will award only two mobile phone licenses. The results of the competition are slated to be announced on June 27. In response, Human Rights Watch (HRW) has issued a warning that international firms who enter the current Burmese telecommunications market "risk being linked to human rights abuses." In a report, HRW outlines a number of measures necessary to ensure that mobile phone and Internet users in Myanmar are protected from such abuses and to "foster responsible investment in Burma's telecommunications and Internet sectors." It is currently estimated that only 1 million people of Burma's population of 60 million have access to mobile networks.

Philippines

"Cyber battle" between Filipino and Taiwanese hackers

After a Taiwanese fishing boat was shot by members of the Philippine Coast Guard, Taiwanese and Filipino "hackers" have conducted a "cyber battle" with the websites of the Taiwan's Ministry of National Defense (MND), Ministry of Economic Affairs, and Coast Guard Administration (CGA) compromised after an attack on the website of the Filipino president. A Taiwanese group, Anon TAIWAN, claimed responsibility for the releasing of DNS information of various Filipino government websites on Pastebin, a text sharing website. Relations between the two countries have deteriorated since the incident.

Philippines may soon adopt online voting for overseas citizens

The Philippines' Commission on Elections (Comelec) has announced that it is considering implementing Internet voting for citizens living abroad. In the most recent elections, only 117,383 of a total 737,759 (or 16 percent) registered overseas voters cast their ballots. Comelec Chair Brillantes estimated that Internet voting could potentially increase overseas voter turnout by 60 to 70 percent.

SINGAPORE

Scores of victims in Singapore fall prey to online-banking malware

A report by Trend Micro Smart Protection Network has revealed that more than 900 Singapore citizens have fallen prey to online banking scams during the first quarter of 2013. The report surveyed various citizens on their online practices and found most respondents did not clear their caches after online transactions, making their online activities, including financial transactions, particularly vulnerable to cybercrime. As previously reported, Singapore's Deputy Prime Minister recently announced that Singapore would bolster its infrastructure against threats such as cyberattacks, cyberespionage, and cybercrime.

THAILAND

Thailand extradites malware developer to United States

Thailand has extradited Algerian national Hamza Bendelladj to the United States on charges of developing and marketing malware designed to steal private information. The malware, a derivative of the Zeus botnet toolkit called SpyEye, has been described as "among the most widely-used financial fraud malware packages in the world." Bendelladj was arrested earlier this year by Thai authorities.

Prime Minister urges ministry to tackle “baseless accusations” made online

Prime Minister Yingluck Shinawatra recently ordered the Information and Communications Technology Ministry to take action against "baseless accusations" made on the Internet. She argued that intervention is warranted when criticisms and accusations go "too far" or are outside "the boundaries of rights and freedoms." ICT Minister Anudith Nakornthap responded by reiterating the ministry's commitment to protecting the prime minister and other Thais from "unfair online criticism." Defamation laws, including lèse majesté, are frequently used in Thailand to prosecute critics of the ruling powers and curtail freedom of speech. Notably, the Thai government just recently admitted to the United Nations that lèse majesté laws "add to the chilling effect on free speech."

VIETNAM

Vietnamese dissidents form online activist group

A group of Vietnamese dissidents, most of whom have spent time in jail, have established the "Brotherhood for Democracy." The group, which so far exists only online and is comprised of around 70 members, was co-founded by Nguyen Van Dai and Pham Van Troi. The will seek to bring democracy to the country by using information technology to coordinate many disparate individual and petition-based efforts. The co-founders believe that, by limiting their existence to the Internet, the group need only "adhere to the rules set by Facebook, service providers, U.S. law and international law" and is not in violation of Vietnamese laws.

Read previous editions of the Southeast Asia CyberWatch.