UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Southeast Asia CyberWatch: January 2013

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

and Internet use in Southeast Asia

Table of Contents

CAMBODIA

- **Hackers breach two government websites**
  The Cambodia Daily reported that the websites of Cambodia's National Military Police and Supreme Court were hacked earlier this month. While an Indonesian hacker called "Hmei7" claimed responsibility for the National Military Police attack, no attribution could be made in the case of the attack on the Supreme Court's website. The Cambodian government has been subject to multiple cyber attacks in the past, including one in which Anonymous stole over 5,000 documents from the Ministry

of Foreign Affairs and leaked them online. Cambodian officials have warned that the government lacks the information security capabilities necessary to protect its data.

INDONESIA

- **“Anonymous Indonesia” launches attacks on government sites**
  A group identifying itself as "Anonymous Indonesia" has defaced more than twelve websites associated with the government of Indonesia. These attacks have followed the arrest of Wildan Yani Ashair, a 22-year old accused of hacking the website of the Indonesian president earlier in January. Websites that were attacked include the sites of the Business Competition Supervisory Commission (KPPU), the Central Statistics Agency (BPS), the Indonesian Embassy of Tashkent, the Ministry of Law and Human Rights, they Ministry of Social Affairs, the Ministry of Tourism and Creative Economy, and Indonesia.go.id. Security experts in Indonesia have highlighted this incident as indicative of weaknesses in security measures used to protect government sites.

MALAYSIA

- **CyberSecurity Malaysia and OIC-CERT collaborate to face 2013 cyber threats**
  CyberSecurity Malaysia and the Oman National Computer Emergency Readiness Team (OCERT) organized the fourth annual conference and AGM of the Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) in Oman to prepare for cyber threats in 2013. The OIC-CERT has opened up membership to commercial organisations to foster a public-private partnership in mitigating cyber threats. CyberSecurity Malaysia chairman and chair of OIC-CERT, General Tan Sri Dato' Seri Panglima Mohd Azumi Mohamed, said that next year, the OIC-CERT would be expanding its reach to the African continent with the signing of a Memorandum of Understanding with the Africa Computer Emergency Response Team (AfricaCERT).

MYANMAR

- **Report on media freedom in Myanmar**
  In January, Reporters Without Borders (RSF) released a report on the state of media freedom in Myanmar. The report, entitled “Burmese Media Spring” [PDF], has praised Myanmar’s previously reported move towards media reform and the diminishing of government monitoring over the press. The report has, however, raised concerns that a government trend toward suing media outlets for defamation will nullify these reforms by encouraging a climate of self-censorship. It has also recommended that Myanmar’s information ministry be abolished for having “no place in Burma’s new democratic environment.”

- **Government shutters press censorship organization**
  In a further step toward liberalization, the Burmese government has dissolved its "Press Scrutiny and Registration Division", a government body that was formerly responsible for reviewing and approving all material before publication. In an interview with Radio Australia, Zin Linn, Vice President of the Burma Media Association, explained that the government ordered the division to cease all pre-publication censorship in August 2012 and appointed a new information minister, Aung Kyi, just weeks later. Linn cautioned that the Burmese press would continue to face problems of self-censorship due to state ownership of media outlets and many of the vaguely worded laws that have been used to enforce censorship in the past remain in effect.

PHILIPPINES

- **High rate of Filipino cybercrimes victims**
  According to the Philippines' Department of Justice (DOJ), almost nine out of 10 Filipino Internet users have been victims of cybercrime at some point in their online experience. This statistic was released as part of a primer produced by the DOJ to increase awareness of cybercrime in the country. As previously reported, the country's Cybercrime Prevention Act was recently suspended to investigate how far the bill may undermine civil liberties. Recently, several government sites were vandalised in protest of the law, which activists continue to denounce.

- **Philippines set to regulate election advertising online**
  As part of an effort to regulate campaign financing, the government will limit candidates in May's general election to three days of online advertising per week. The decision, made by the Commission on Elections (Comelec), has been criticized by Senator Francis Escudero, a candidate for the upcoming election, as "vague," full of loopholes, and devoid of monitoring and government oversight.

- **Government admits cybercrime legislation is not constitutional**
  Lawyers representing the government of the Philippines have admitted that the country's proposed Cybercrime Prevention Act is "barely constitutional." Francis Jardeleza, Solicitor-General of the Philippines, himself has noted that Act is ill-defined, specifically with regards to wording that allows law enforcement to collect data with "due cause" without defining what that cause may be. Jardeleza, however, has disagreed with arguments that the law's provisions on libel may create "chilling effects" on free space, stating that "defamation is defamation" regardless of the mode of communication of that libelous speech. As previously reported, the Act has been met with opposition from many groups ranging from legal experts to "hacking collectives" like Anonymous Philippines. As of writing, discussions at the Supreme Court on the legality of the law are still underway.

SINGAPORE

- **Parliament passes amendments to Computer Misuse Act**
  Changes to the Computer Misuse Act, last amended in 2003, provide the government with greater ability to take action against cyber threats to Singapore's Critical Information Infrastructure, which are necessary to deliver essential services to the public like healthcare and transportation. One example of the amendment is that the Home Affairs Minister may issue a certificate to authorize a person or an organization "to take measures necessary to prevent, detect or counter cyber attacks." The certificate could require a person or entity to provide technical information relating to the "design, configuration, operation and security of computers, computer programs or computer services". The amendment also seeks to rename the Act as the Computer Misuse and Cybersecurity Act.

THAILAND

- **Arrest of international cyber-criminal in Thailand**
  Thai police have arrested Hamza Bendelladj, a 24 year old Algerian national wanted by American authorities for multiple cases of cybercrime. Bendelladj has been accused of allegedly making millions of dollars by "pirating the accounts of over two hundred US banks", using a trojan/botnet known as Zeus. Bendelladj will be extradited to the U.S. state of Georgia, where a local court has issued an arrest warrant.

VIETNAM

- **Blogger reports sexual assault, physical abuse**
  On January 5, Nguyen Hoang Vi, a blogger for Danlambao, posted a personal account of physical and sexual assault at the hands of Vietnamese police. Police and security officials chased and arrested Vi outside of a court house where three jailed bloggers were due to appeal their sentences. She was subsequently taken to a police station, beaten, stripped of her clothes, and humiliated. Vi had been covering the case of the three bloggers, who were sentenced to terms ranging between four and 12 years in September for "conducting propaganda against the state." The Vietnamese government has in the past ordered police to crack down on Danlambao, which regularly criticizes the ruling authorities.

- **Vietnamese court sentences 14 activists**
  On January 9, a Vietnamese court convicted 14 activists and bloggers for sentences of up to 13 years followed by long periods of house arrest in what the Washington Post has called the "largest single crackdown in recent years." They were accused of plotting to overthrow the government and of possessing ties to Viet Tan, a Vietnamese pro-democracy network based in the United States. The Vietnamese government considers Viet Tan a "terrorist organization," though the group officially eschews violence. Both the United States government and Human Rights Watch have criticized the decision and called for the charges to be dropped immediately.

- **Government uses propaganda agents to spread message online**
  The Vietnamese government recently admitted to employing teams of individuals to post propaganda on blogs, social media platforms, chatrooms, and message boards. Ho Quang Loi, Vietnam's "head of propaganda," said earlier this month that the government deploys almost 1000 "internet polemicists" and "public opinion shapers" over 18 websites and 400 accounts to surveil and influence online discussion. It is not clear whether the hired propagandists are on official state payrolls. The Vietnamese government's use of hired hands to counter free speech bears similarity to other Internet "armies," such as China's "Fifty Cent Party" and Iran's Basiji bloggers.

Read previous editions of the Southeast Asia CyberWatch.