APrIGF.ASIA
ASIA PACIFIC
REGIONAL INTERNET GOVERNANCE FORUM
http://www.APrIGF.asia

APrIGF Macao 2015
Workshop Summary Report

Date: July 2
Time: 11:00-12:30
Workshop Title: Surveillance trends, challenges and opportunities in Asia Pacific
Reported by & Contact Email: Irene Poetranto, irene.poetranto@utoronto.ca
Gender Balance (approx. number of female vs. male participants): Approximately 15 female and 35 male participants
Moderators: Shahzad Ahmad, Bytes for All, Pakistan
Panelists:
Shahzad Ahmad, Bytes for All, Pakistan
Irene Poetranto, The Citizen Lab, University of Toronto, Canada
Arthit Suriyawongkul, Foundation for Internet and Civil Culture, Thailand
Donny Budhi Utoyo, ICT Watch, Indonesia
Ang Peng Hwa, Nanyang Technological University, Singapore

A brief summary of presentations (If any)

Shahzad Ahmad opened the session by situating the discussion in the context of the United Nations Human Rights Council's (UNHRC) decision to adopt a resolution appointing a special rapporteur on the right to privacy, and in light of the reports published by the Citizen Lab on surveillance, especially targeting civil society organizations in the global South, using technology produced by Western countries (e.g., FinFisher and Hacking Team).

Irene Poetranto from the Citizen Lab gave a brief summary of the group's research into the commercialization of surveillance. She first discussed FinFisher, a network intrusion suite which is marketed and sold exclusively to law enforcement and intelligence agencies by Gamma TSE, part of UK-based Gamma Group. FinSpy, a component of the FinFisher suite, for example, is capable of intercepting email, instant messaging and VoIP communications, as well as spying on users through webcams and microphones and transmitting the data to a command-and-control (C2) server. In August 2012 and after several preliminary reports, Morgan Marquis-Boire, Bill Marczak, John Scott-Railton, and Claudio Guarnieri, fingerprinted FinSpy's unique C2 protocol and scanned the Internet to identify instances of the C2 servers. This investigation resulted in the discovery of FinSpy C2 servers in a total of 36 countries, some of which are governed by authoritarian regimes. Poetranto then followed up with a discussion on Hacking Team, also known as HT S.r.l., a Milan-based purveyor of "offensive technology" to governments around the world. One of their products, Remote Control System (RCS), is a trojan that is sold exclusively to intelligence and law enforcement agencies worldwide. Results from a global scanning effort indicate that there are 21 countries that have deployed Hacking Team's Remote Control System monitoring solution.

Alongside other researchers, the Citizen Lab has uncovered a range of cases where these "lawful interception" tools have been used against political targets by repressive regimes. Political and civil society targets have included Mamfakinch in Morocco, human rights activist Ahmed Mansoor in the UAE, and ESAT, a US-based news service focusing on Ethiopia.

Poetranto's presentation was followed by Arthit Suriyawongkul of The Foundation for Internet and Civil Culture who gave an overview of the threats to freedom of expression in Thailand following the May 2014 coup. A military order was released the same day as the coup occurred, which called on ISPs to monitor and deter the publication of information online which may incite unrest in the country. In early June, Thai police warned users that showing support for anti-coup activities by liking a social media post constituted a crime, punishable by up to five years in jail. The junta has also adopted phishing techniques using a Facebook application to collect information on their citizens. After the coup, Thai Netizen Network, a digital rights group, noticed that the TCSD-maintained page that appears when netizens try to access certain blocked websites had a "Login with Facebook" icon. Users were then asked for permission to hand over information stored in their Facebook profile, without any indication, in Thai or English, as to where or for what purpose that data was being sent. EFF reported that the "Login" app was being run by TCSD itself, which used the Facebook app to collect personal details of Facebook users visiting the page.

Donny Budhi Utoyo from Indonesia's ICT Watch outlined the Citizen Lab's findings of FinFisher servers in Indonesia, which were found on the IP addresses belonging to operators such as PT Telkom, PT Matrixnet Global, and Biznet ISP, as part of a report entitled "You Only Click Twice: FinFisher's Global Proliferation." Following the report's publication, ICT Watch conducted advocacy activities to raise awareness on the threats to free expression and privacy posed by the government's lack of transparency and accountability in carrying out wiretapping and surveillance in Indonesia. These concerns were covered by the Indonesian press at that time, but he found that by and large members of the Indonesian public are still largely unaware and/or not too concerned with privacy issues.

Ang Peng Hwa from Nanyang Technological University gave a detailed overview of the history of surveillance in Singapore, a country which according to top secret documents leaked by intelligence whistleblower Edward Snowden is a key "third party" providing the Five Eyes (US, UK, Canada, Australia, and New Zealand) access to Malaysia's communications channel.

Shahzad Ahmad closed the presentations by giving an overview of the situation on surveillance in Pakistan. He outlined Bytes for All's ongoing lawsuit, submitted to the Lahore High Court, regarding the discovery of FinFisher in the country, which argues that the Pakistani government violated constitutional rights by indiscriminately spying on its citizens, which violates the Privacy Act.

A substantive summary and the key issues that were raised:

- Concerns with regard to surveillance technologies being used against political and civil society actors.
- Concerns with regard to the lack of transparency and accountability in how governments conduct surveillance.
- Concerns with regard to the general public's lack of awareness of privacy issues.
- The issue of what civil society actors can do to increase awareness and technical proficiency in digital security was raised, in addition to what advocacy activities can or should be carried out to inform the general public.

Conclusion & Further Comments:

To conclude, the issue of surveillance is a very timely and relevant topic in the Internet governance space. Research has shown that civil society organizations (CSOs) that work to protect human rights and civil liberties around the world are being bombarded with persistent and disruptive targeted digital attacks (e.g., surveillance)—the same sort of attacks reportedly hitting industry and government. Unlike industry and government, however, civil society organizations have far fewer resources to deal with the problem.