Safe and secure Internet environment of youth

Securing youth from the cyber threats is a responsibility of all of us. What are the best practices that we can follow for the Asia-Pacific region in this new Internet era?
There are few questions to be resolved.

1. Who should lead the discussion to protect the youth online?
2. Can they protect by themselves?
3. What are the additional/next steps?

There are few common areas which we should consider.

- Awareness and education
-Measurement and indexes
-Legislations and policies
-Non-government collaborations
-Cross-economy collaborations

In Japan all most all high school students use cell phone. 80% of them use smart phones.
Hence there is an Act on development of an environment that provides safe and secure Internet use for young people. Also it is understood that enhancing it literacy is a must. In addition Japan promotes the ISPs for providing filtering services to block the harmful content from the Internet.

Also they have a safe online operations center with a hot line to report illegal and harmful content.

In Taiwan there is a special office for online safety. It has been found that 60% of the people use social media. Facebook is very popular. Google has become the commonly used search engine. Hence international collaboration is essential as most of the incidents IP s belong to external countries.

Empowering teachers, parents and students on cyber security matters has been identified as top priority. In future it will be empowering digital citizens.

Private public partnerships established in Vietnam has helped them a lot to overcome cyber crimes.

Also it is essential to think globally and act locally. We have a collective responsibility to protect the youth from Internet related matters.

Security and Management of Internet Content from Overseas

In the asia-pacific region most the Internet content come from overseas. How are we going to manage them to protect our security?

Especially it should take measures to protect the children. Development of policies for securing the clients is essential for any organization which provides online services.

Regulation of Internet content is a must. But there are practical problems when regulating the content from overseas.

Local ISPs can play a major role on this. But there are limitations with access blockage to illegal content from overseas services providers through local ISPs.

Self regulation from overseas service providers has limitations too. As a result of all of these, content regulation in cyber space has become increasingly complicated.

There are International efforts on combating online sexual exploitation of children. NGOs can also play a main role to support this effort. Self regulation is essential.

Encryptions on mobile devices make it difficult to control illegal content. Developing new technologies for filtering, tracing and photo DNA etc will help to regulate the illegal /harmful Internet traffic.

Classifying and monitoring Internet content is essential. But freedom of speech of adult and child online safety should be paid equal attention.

Intrusive Surveillance technology could be justified?

- Surveillance technology with intrusive approach is used for investigation and intelligence activities
- Hacking tools have lot of advanced capabilities
- We don't know what are the hacking tools used by intelligence agencies to collect information
- There are reasons to do surveillance eg: counter terrorism
- But it shouldn't mean that everyone should be monitored
- In USA there are acts (FIFA, Patriot) which provide authority for surveillance
- There are malware targeting various groups to collect intelligence. They will collect any user behaviors to monitor them.
- It is a violation of privacy