Intermediary Liability and Freedom of Expression

Call for amendments to Section 79

Centre for Internet and Society
Jyoti Panday

IT Rules 2011

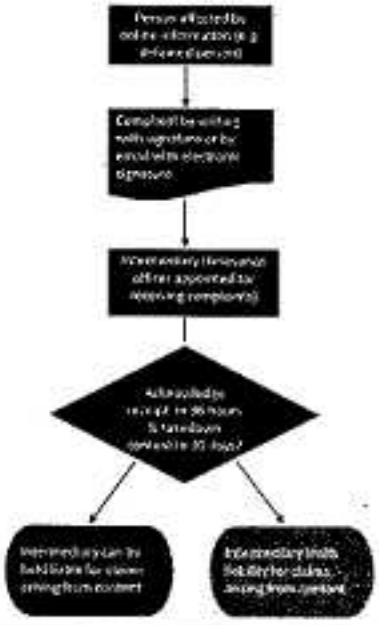
11th of April 2011, the Government of India notified the 'Information Technology (Intermediaries Guidelines) Rules 2011

Guidelines for the 'post-publication redressal mechanism' for removal of user generated content that violates reasonable restrictions to the right to freedom of expression as envisioned in the Constitution of India

Guiding principles for post-publication redressal

- Quick
- Cheap
- Provides safeguards against abuse
- Conform to all forms of natural justice
- Uphold freedom of expression
- Shall not result in a chilling effect on freedom of expression
- Recognise the different functions performed by different classes of intermediaries

Current redressal mechanism



Criticisms of the current mechanism

No natural justice

- Third party provider/creator of information is not given a chance to be heard by the intermediary
- No requirement to give a reasoned decision
- No procedure for putting back content

Uncertainty in content criteria

- Includes terms like "disparaging" and "objectionable" which are not defined and go beyond the reasonable restrictions envisioned by the Constitution of India

Criticisms of the current mechanism

Intermediaries are all treated alike

- Different classes of intermediaries perform different functions and therefore should have different roles and responsibilities e.g., BSNL is treated at par with YouTube
- Removal of content by upstream intermediaries will result in undue over-blocking

Criticisms of the current mechanism

Private censorship

- Censorship, domain of the judiciary or the executive, delegated to private intermediaries
- Incentive to remove expressions in order to limit liability
- Private intermediaries lack sufficient legal resources to subjectively determine the legitimacy of a legal claim as a result of which they err on the side of caution

Criticisms of the current mechanism

No safeguards to prevent abuse

- Complainant may send frivolous complaints and suppress legitimate expressions without any fear of repercussions

CIS tested the efficacy of the redressal mechanism in a sting operation in 2011

Research

- Takedown notices sent to 7 intermediaries
- Intermediaries included information location tool and hosts
- 6 intermediaries over-complied with the notices, despite the apparent flaws in them

Learnings from takedowns

- No obligation to provide a reasoned decision for rejecting or accepting a takedown notice
- No codified recourse to claim damages even if takedown process is being abused
- No requirement of disclosure or transparency in the takedown process
- Content restrictions not defined resulting in varied interpretations of the same restriction by different intermediaries
- Tendency to prioritise the allocation of resources for determining legal validity of expressions according to the perceived importance of the expressions
- No established procedures, such as those prescribed in the CPC or CrPC, thereby creating procedural uncertainly
- Claimants are not required to state their entire cause of action and provide reasonable level of proof (prima facie)

Key takeaways

- Uncertainty in subjective determination
- Uncertainty in criteria
- Uncertainty in procedure
- Absence of natural justice in procedure
- Absence of safeguards against abuse

Paradigm shift

Why should a private intermediary determine what is right or wrong, especially when it doesn't have the legal competence to do so?

Ideally, the intermediary should continue performing the role of an intermediary and ask the creator of expression whether he is willing to defend his expression in court... and remove the expression only if he refuses to defend his expression

Proposed redressal mechanism

Hosting Services

- On receiving a complaint, the intermediary issues a "***notice***" to the third party provider of information along with a copy of the complaint
- Third party provider may choose to contest the notice by filing a "***counter-notice***" within 48 hours
  - ***If the third party provider chooses to contest*** the notice by responding with a counter-notice then the intermediary is required to continue hosting the information and share the counter-notice with the complainant, so that the complainant may directly approach the court against the third party provider of information. However, the intermediary may voluntarily remove the information under contention if in its good faith it feels the expression is not legitimate despite the counter-notice of the third party provider
  - ***If the third party provider chooses to accept*** the allegations in the complaint, the intermediary is required to remove the information under contention
  - ***If the third party provider fails to reply*** within the counter-notice deadline, the intermediary is required to remove the information under contention and replace such removed information with a general notification about the removal. However, in such a case, the complainant is required to get a court order to back the complaint within 180 days, the failure of which will render the original complaint redundant and require the intermediary to restore the removed information
- Regardless of the counter-notice deadline, the third party information provider may contest the notice by responding with a counter-notice within a period of 60 days of receiving the notice
- If the information has already been removed by the intermediary, then the information is required to be restored and the complainant is required to be provided with the counter notice

Information Location Tool

- Within 48 hours of receiving a complaint, the intermediary determines whether the information hosted at the other end of the communication link has been instructed to be removed pursuant to a court order or any direction under the Act
- If the complaint is accompanied with a copy of any such order or direction then the communication link should be removed, else it should be retained

Caching Services

- Within 48 hours of receiving a complaint, the intermediary determines whether the information for which the transmission is sought to be made more efficient has been removed at its source
- If it has been removed then the cached information should also be removed, else it should be retained

Access Providers

Redressal mechanism should not be applicable to prevent upstream over-blocking

The Amendment of Section 79

We call for the shift of the liability regime from it's current status which is "immune from liability if proven so" to a regime which holds online intermediaries "immune from liability until proven otherwise"

Thank you

NSA, exactly what was wrong? : Learning from Korea Case

K.S. Park
Professor, Korea University Law School
Litigation Director, Open Net

What was exactly wrong with NSA?

- all approved by Foreign Intelligence Surveillance Court(FISC), in turn set up by Foreign Intelligence Surveillance Act(FISA), a Democrats' response to the uncovering of FBI surveillance of human rights activists such as Martin Luther King
- Thoroughly "legal" and politically correct!
- At least no mass wiretapping, just mass metadata acquisition.
- Maybe, INDISCRIMINATE NATURE was the problem

2 Unresolved Issues

- ISSUE 1: Isn't suspicion-less mass surveillance better than targeted surveillance?
  - What is more stigmatizing?
  - What has more infringing consequences? Direct risk of criminal punishment v. mere risk of further investigation (user unidentified)
- ISSUE 2: What to do with INTRA-EXTRAterritorial surveillance? From which court do we obtain a warrant?
  - In-country foreigners : non-discrimination principle
  - overseas-located targets: MLAT
  - How about overseas targets' IN-COUNTRY COMMUNICATIONS

Korea Case (Lesson for Issue 1)

- Korea – population of 50 M
- In 2011 alone,
  - 7,167 phone numbers wiretapped (per capita, 15 times U.S., 287 times Japan)
  - 37.3 M metadata acquired (Maybe Snowden has the final data on US ☺)
  - 5.84 M subscriber identifying data

What is up with Metadata?

- Investigation in Search of a Crime
- 98% of metadata for cell tower search
- Why do "cell tower search"? -- when related communications go a cell tower, e.g., anti-government demonstration

→ Implication of metadata for democracy

Back to morality of mass surveillance

- Non-stigmatizing? Bottom-line is TREATMENT of people like POTENTIAL CRIMINALS
- Non-privacy infringing? Depending on ANONYMITY protection
- In Korea, subscriber data disclosure 6M/yr
- In US, the disclosure is MANDATORY but not as many in Korea

ANONYMITY AND METADATA MASS SURVEILLANCE

- USA, UK, Germany, France (commonality?) very low protection of subscriber identifying data → metadata becomes more privacy-infringing, more tempting targets
- **Protect Anonymity to Stop NSA-like mass surveillance!**
- **Call for international reforms for subscriber-identifying data!**
- **Recent Canadian Case:** R. *v.* Spencer, 2014 SCC 43 (June 2014)

Online Intermediary Liability and *Google Spain* through Korean experience

K.S. Park
Professor, Korea University Law School
Litigation Director, Open Net

Lesson from Korean case

- Network Act 44-2 : "take out all rights-infringing material upon demand"
- Seems Innocuous?
- Asymmetry in Incentives -> always better to err on the side of deleting than keeping it → Rampant Private censorship in Korea

Korea's private censorship

- 2012 Rights-infringing takedown: about 100,000 in Korea vs. 2,000 in whole world (Google) vs. less than 10,000 Korean gov takedowns
- A posting critical of a Seoul City mayor's ban on assemblies in the Seoul Square
- A posting critical of a legislator's drinking habits and introducing his social media account;
- Clips of a television news report on Seoul Police Chief's brother who allegedly runs an illegal brothel-hotel;
- A posting critical of politicians' pejorative remarks on the recent deaths of squatters and police officers in a redevelopment dispute
- A posting calling for immunity from criminal prosecutions and civil damage suits on labor strikes.
- A posting by an opposition party legislator questioning a conservative media executive's involvement in a sex exploitation scandal related to an actress and her suicide.

Korea's online intermediary landscape

- Search engine: Naver 75% Daum 20% Google 10%, etc.
- Twitter : decreasing use, political fatique?
- Facebook : dominant but vs. Kakao Story)
- Application platform: 90% Google Play
- UCC
  - Uploading : Naver 70% Miscellaneous 10%
  - Viewing: Youtube 60% Miscellaneous 40%
- Korea special: KakaoTalk, is it private or public?

Let's relearn why Internet is God

- Individual's ability to post and download UNAPPROVED -> always possibility of ILLEGAL CONTENTS -> "must take out noticed illegal content"
- Is that enuf? No, asymmetry of incentives -> also need a rule "must restore if noticed legal content." → But too risky for Intermediaries → Instead of double liability, DOUBLE IMMUNITY which includes RESTORATION as well → Full Notice and Takedown
- Do not make intermediary an ADJUDICATOR but MEDIATOR (True InterMEDIARY)

How to Adapt to Google v Spain

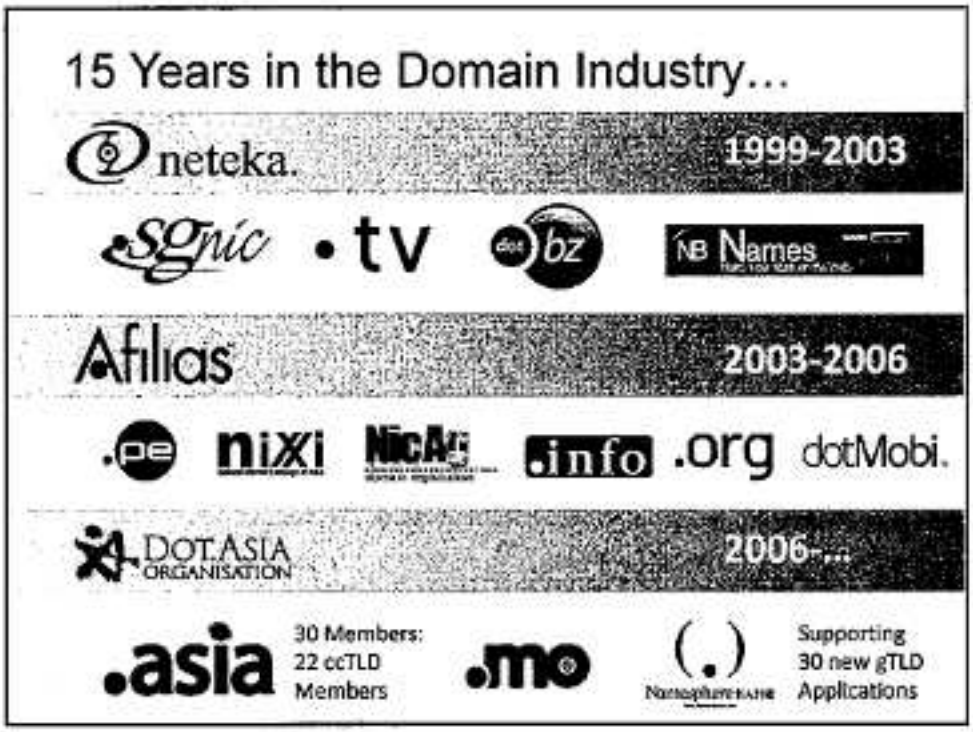
- Problem w/ Google Spain:
  - Did not recognize Google search "journalism" and yet require Google to "edit"
  - Turns an NON-EDITTING intermediary into something else
  - Punishes an intermediary for being an intermediary: Internet IS about mass data processing.
  - Future: (1) probably need RESTORATION RIGHT to make it a "true intermediary" OR (2) do not recognize "right to be forgotten"
  - Let's expand on (2): Right to be forgotten currently based on data protection law built on the concept of DATA OWNERSHOP ("You own data about oneself")

Peculiar idea of one's owning data about oneself

- Distinguish
  (1) "X was built by someone who built Y, which crumbled down (no personal data)."
  (2) "X was built by Gonzales. Y which crumbled down was built by Gonzales" (personal data)
- Most of times, (2) is the only way to get (1)
- Also, we are "born into" a society"
- One's ownership data about oneself is impossible
- Also, Alan Westin, the inventor of data ownership, thought it up as a response to "data surveillance" -> which applies only data you kept private before submitting to govt' agencies or companies → Data ownership requires LIMITING INTERPRETATION

Participation at ICANN

from.Asia / for.Asia



August 1999 Santiago

from.Asia / for.Asia

1999-2001: ccTLD Constituency

From DNSO to ccNSO

Connecting Asia with One Domain .asia

GNSO

ALAC / At-Large

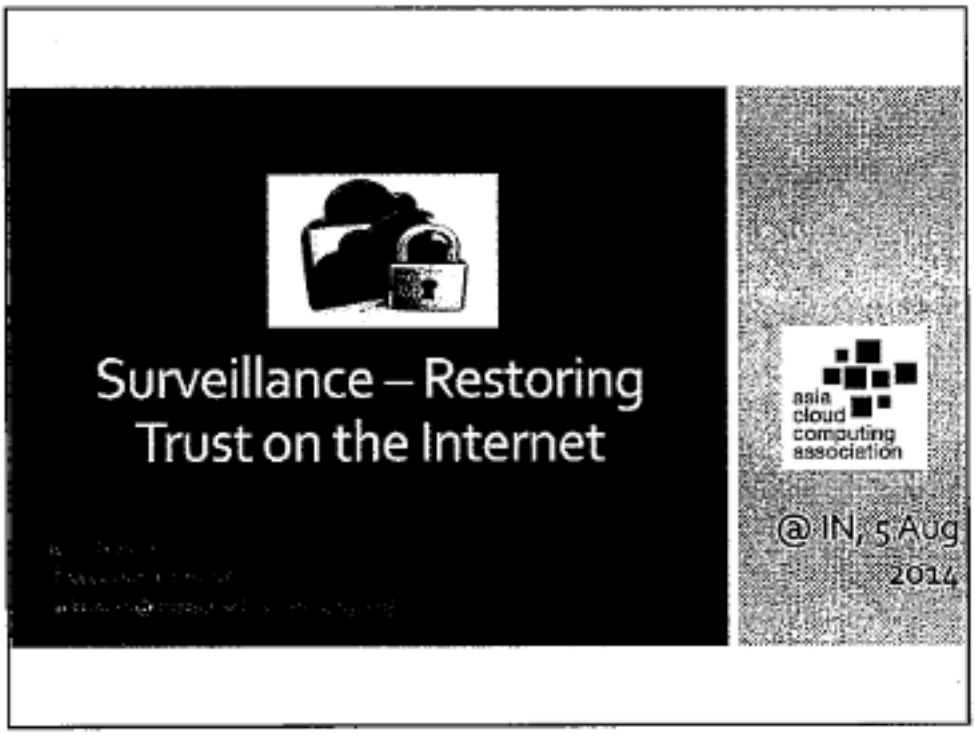
2002-2007: APRLAO (ISOC HK)
2010-2012: ALAC (from APRALO)
2010-2014: IDN Liaison

Challenges for Participation

- Costs & Return on Investments
- Volume of Activity
- Language & Timezone
- Culture & Sociopolitical Environments

DOT.ASIA ORGANISATION

promote Internet development and adoption in Asia


Surveillance – Restoring Trust on the Internet
asia cloud computing association
@ IN, 5 Aug 2014


@accacloud
is.gd/accacloud
About the Asia Cloud Computing Association
We are a leading influential industry voice on cloud computing – we involve business, government and people in Asia – the public, private and people sectors
Mission: to accelerate cloud computing adoption across Asia Pacific
Engaging stakeholders, providing tools to educate, and advocate to remove barriers to using cloud computing and other technology tools
http://www.asiacloudcomputing.org
(new!)
Contact the Secretariat at info@asiacloudcomputing.org
Working Groups and Thought Leadership
Public Policy & Regulation
Data Governance
Cloud Market Segments
Big Data & Analytics
Cloud Assessments
Cloud Readiness Index 2011, 2012, 2014; regular touchpoint meetings with policymakers
Impact of Data Sovereignty on Cloud Computing; Financial Services Industry and Cloud
Small and Medium Enterprises and the Cloud Computing Market
NEW! Collection, Storage, Use and Query of Data
Cloud Assessment Tool; looking into awarding APAC Cloud Service of the Quarter

@acccacloud
is.gd/acccacloud

Rules around Restoring Trust/ Restoring Trust in Rules

Businesses are aware, and are complying with laws -- ACCA Research on Cost of Compliance

ACCA and APCC joint report release: Report on Cloud Data Regulations – a contribution on how to reduce the compliancy costs of cross-border data transfers

Security and compliance concerns are transforming the services cloud providers are rolling out

Challenges: security, sovereignty, protection, privacy, confidentiality, compliance, government intercept

Solutions: data classification, rules of (data) origin, bonded warehouse, quarantine or "safe harbour" data zones

@acccacloud
is.gd/acccacloud

- EU-yes, "location-based"
- APEC-yes, "accountability based"
- US-"risk-based"

Table 1: Summary of Data Privacy Laws and Data Transfer Provisions

Country	General law on personal data privacy protection	Separate regulator	Register of data controller	Sector-specific legislation	"White list" countries or requirement on data controllers to ensure protection on data transfers	Individual consent required for data transfers	Contract obligations accepted as reason for data transfers	Companies required to appoint "Data Protection Officer"
Australia	Y	Y	Y	Y	Y	Y	Y	N
New Zealand	Y	Y	N	Y	Y	Y	Y	Y
India	N	N	N	Y	Y	Y	Y	Y
Indonesia	Proposed	N	N	Y	N	Proposed	N	N
Hong Kong	Y	Y	Y/N	Y	Y/N	Y	Y	N
Japan	Y	N	N	Y	Y	Y	Y	N
Malaysia	Y	Y	Y	Y	Y	Y	Y	N
Philippines	Y/N	Y/N	N	Y	Y	Y	Y	Y
Singapore	Y	Y	N	Y	Y	Y	Y	Y
South Korea	Y	N	N	Y	Y	Y	Y	Y
Taiwan	Y	N	N	Y	Y	Y	Y	N
Thailand	Y	N	N	Y	Y	Y	Y	N
EU	Y	Y	Y	Y	Y	Y	Y	Proposed
UK	Y	Y	Y	Y	Y	Y	Y	Y
USA	N	FTC	N	Y	N	By sector	Y	Varies

Note: (i) Y/N means it is on the statute book but not yet implemented.

Cnts around liability and compliance: Who are the "data controllers"? Businesses who use data services, the data vendor, the data protection officer? What is "sensitive data"? Who "owns" the data? V expensive to comply across jurisdictions

@acccacloud
is.gd/acccacloud

Compliance Cost: Codes of Practice/Sector-Specific Rules

e.g. Credit Reporting code (CR code) – case study

* MY and AU have exempted credit rating agencies under their sector-specific cross-border data transfer regulations

BUT

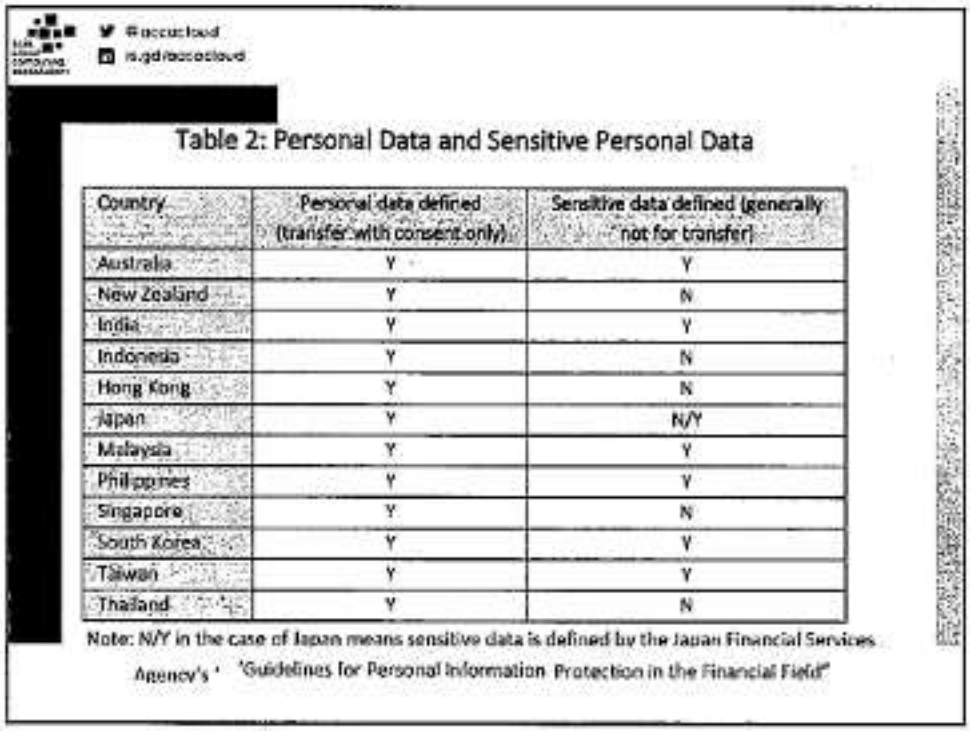
Whose rules reign in a global, interconnected economy?

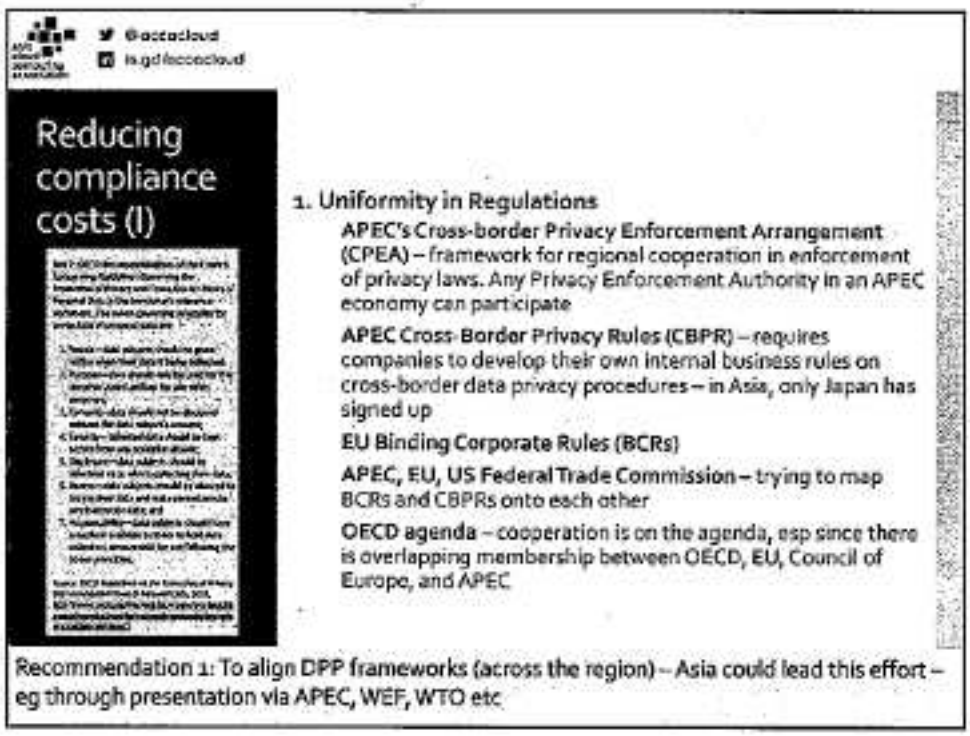
Case 2: French Lawyer caught between French and US Law
A French lawyer was convicted in France of "the crime of disclosure of economic, commercial, industrial, financial or technical documents or information that are to constitute evidence for a foreign proceeding", when he sent documents to the U.S. pursuant to a U.S. court discovery order without receiving the proper consent in France to do so. This action, despite being required by a U.S. court, violated French law, and the French attorney was criminally prosecuted in France as a result. The resulting sanctions case went to the French Supreme Court, which upheld the conviction and the €10,000 fine. This may be the first case where a litigant has been tried in another jurisdiction for attempting to comply with a U.S. discovery order, but the example illustrates the importance of finding an appropriate balance between the requirements of effective cross-border judicial co-operation (in this case, the taking of evidence abroad) and data protection laws.
Source: http://www.hcch.net/upload/wop/genaff2010pd13e.pdf

@acccacloud
is.gd/acccacloud

Compliance Costs IV: Who's In Charge?

- Jurisdictionally – local vs other c
- Definitional challenges: "person "sensitive personal data"; new ideas such as data trails, data audits, "right to be forgotten", data retention policies, metadata
- "Data Controller" – who "owns" the data? Who is responsible/liable? Who makes these decisions?
  - Cloud customer? Cloud vendor? Telco vendor? Data protection officer?
  - Shift from regulating the *collection* of data (consent), to *data use*?


@accacloud
is.gd/accacloud
Table 2: Personal Data and Sensitive Personal Data
Country | Personal data defined (transfer with consent only) | Sensitive data defined (generally not for transfer)
Australia | Y | Y
New Zealand | Y | N
India | Y | Y
Indonesia | Y | N
Hong Kong | Y | N
Japan | Y | N/Y
Malaysia | Y | Y
Philippines | Y | Y
Singapore | Y | N
South Korea | Y | Y
Taiwan | Y | Y
Thailand | Y | N
Note: N/Y in the case of Japan means sensitive data is defined by the Japan Financial Services Agency's 'Guidelines for Personal Information Protection in the Financial Field"


@accacloud
is.gd/accacloud
Reducing compliance costs (I)
1. Uniformity in Regulations
APEC's Cross-border Privacy Enforcement Arrangement (CPEA) – framework for regional cooperation in enforcement of privacy laws. Any Privacy Enforcement Authority in an APEC economy can participate
APEC Cross-Border Privacy Rules (CBPR) – requires companies to develop their own internal business rules on cross-border data privacy procedures – in Asia, only Japan has signed up
EU Binding Corporate Rules (BCRs)
APEC, EU, US Federal Trade Commission – trying to map BCRs and CBPRs onto each other
OECD agenda – cooperation is on the agenda, esp since there is overlapping membership between OECD, EU, Council of Europe, and APEC
Recommendation 1: To align DPP frameworks (across the region) – Asia could lead this effort – eg through presentation via APEC, WEF, WTO etc

@acccloud
is.gd/acccloud

Reducing compliance costs (II)

2. Data Categorization

Three broad categories of data: **personal data** ("personally identifiable information"), **commercial data** (sector-specific – e.g. banking, health, defence etc), **state-owned data** (national security)

3. Bonded Warehousing of data

To remove liability of intermediary/data controllers

Recommendation 2: Call for classification for diferent types of data – eg non-strategic data, non-security-sensitive – while still recognising that there is national security data that should be protected

Recommendation 3: Bonded warehousing of data model could be considered; "quarantine zone"

@acccloud
is.gd/acccloud

Conclusion

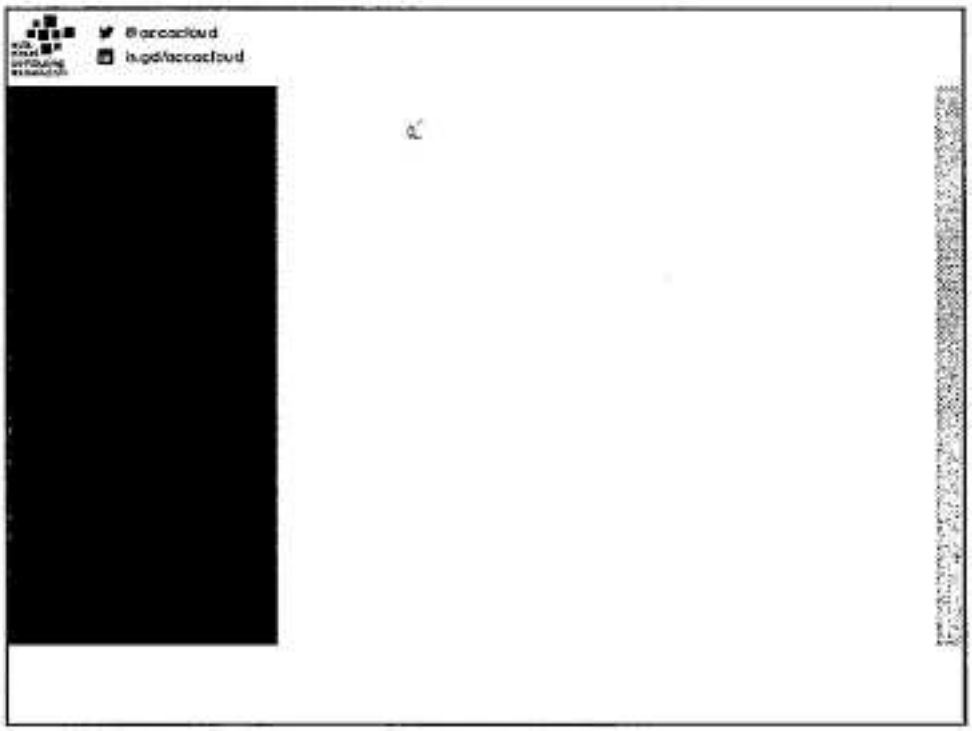
Thank you for your time!

Building trust requires structures and institutions to work together, and build systems which inspire, demand, and require confidence.

Director
puting.org
5) 9847

etariat
25 4237

asia cloud computing association


@arcacloud
is.gd/arcacloud

IANA Stewardship Transition and the Asia Pacific Community

Izumi Aizu, Sivasubramanian M., Kuo-Wei Wu

APrIGF New Delhi meeting

August 5th, 2014

ICANN

Process for this session

Briefing "what the purpose and rule" (3 minutes)

Topics collect from floor (<5 minutes)

+ Please name a topic (should be few words < 5) or two (no more than two each person), such as timeline, process,…
+ Please don't repeat topic which is raised by other
+ No more than 6 topics

Comments on the topics (75 minutes)

+ Prioritize the topics in 2 minutes (please show hands)
+ One topic at a time, and 12 minutes (the most) for each topic
+ Not try to debate viewpoints, but collect viewpoints for CG to consider
+ 90 seconds comment per person

The U.S. Government's Announcement

+ On 14 March 2014, the U.S. Government (USG) announced its intent to transition its stewardship of the IANA functions to the global multistakeholder community
+ As the first step, it asked ICANN to convene global stakeholders to develop a proposal to transition the current role played by the US
+ ICANN was asked to serve as a convener based on its role as the IANA functions administrator (since 1998) and the global coordinator for the Internet's Domain Name System (DNS)
+ The multistakeholder community has set the policies implemented by ICANN for more than 15 years

Transition Proposal' s Guiding Principles

NTIA has communicated to ICANN that the transition proposal must have broad community support and address the following four principles:

1. Support and enhance the multistakeholder model
2. Maintain the security, stability, and resiliency of the Internet DNS
3. Meet the needs and expectation of the global customers and partners of the IANA services
4. Maintain the openness of the Internet

NTIA also specified that it will **not** accept a proposal that replaces the NTIA role with a government-led or an intergovernmental organization solution.

What are the IANA Functions?

The IANA functions involve the coordination of unique Internet identifiers, including:

+ Maintenance of the protocol parameter registries on behalf of the IETF
+ Allocation of Internet Numbers in cooperation with the Regional Internet Registries
+ Management of the .ARPA and .INT domains
+ Administrative responsibilities of the DNS root zone
+ Coordination of root zone management

As of 29 March 2014:

ICANN launched a multistakeholder (global in scope) process at the ICANN 49 Meeting in Singapore.

Based on initial input, from 8 April – 8 May 2014, ICANN issued a call for public comment on the draft principles, mechanisms and process to develop a proposal (translated into 5 official UN languages, plus Portuguese).

Community response to draft process:

+ 700 email exchanges
+ 60 process contributions
+ Participation from global stakeholders, including government, private sector, civil society, technical, academic community and end users
+ Submissions made in different languages

As of 24 April 2014:

A special session was held at NETmundial conference in Brazil.

+ Over 1,000 attendees from 116 countries
+ 1168 remote participants from 33 worldwide remote hubs in 23 countries
+ Participation from global stakeholders, including government, private sector, civil society, technical, academic community and end users

ICANN' s GSE team and partner organizations have been and continue to engage in a series of regional dialogues with global stakeholders.

As of 6 June 2014:

Informed by input on the draft process and subsequent dialogues, the Process to Develop a Proposal and Next Steps was posted online, echoing community feedback.

+ Renamed the proposed "Steering Group" to "Coordination Group"
+ No role for the Chair of the ICANN Board and Chair of the GAC in selection of members
+ Direct representation
+ Eliminated the distinction between affected and non-affected parties
+ Revised composition to ensure greater balance and representation, including indirect stakeholders non-prescriptive about the roles and responsibilities of the Coordination Group
    - Coordination Group will establish its own working methods and modes of operation
+ ICANN maintains neutral role as convener and facilitator of process
+ Coordination Group encouraged to adhere to diversity standards as they undergo internal selection processes

As of 26 June 2014

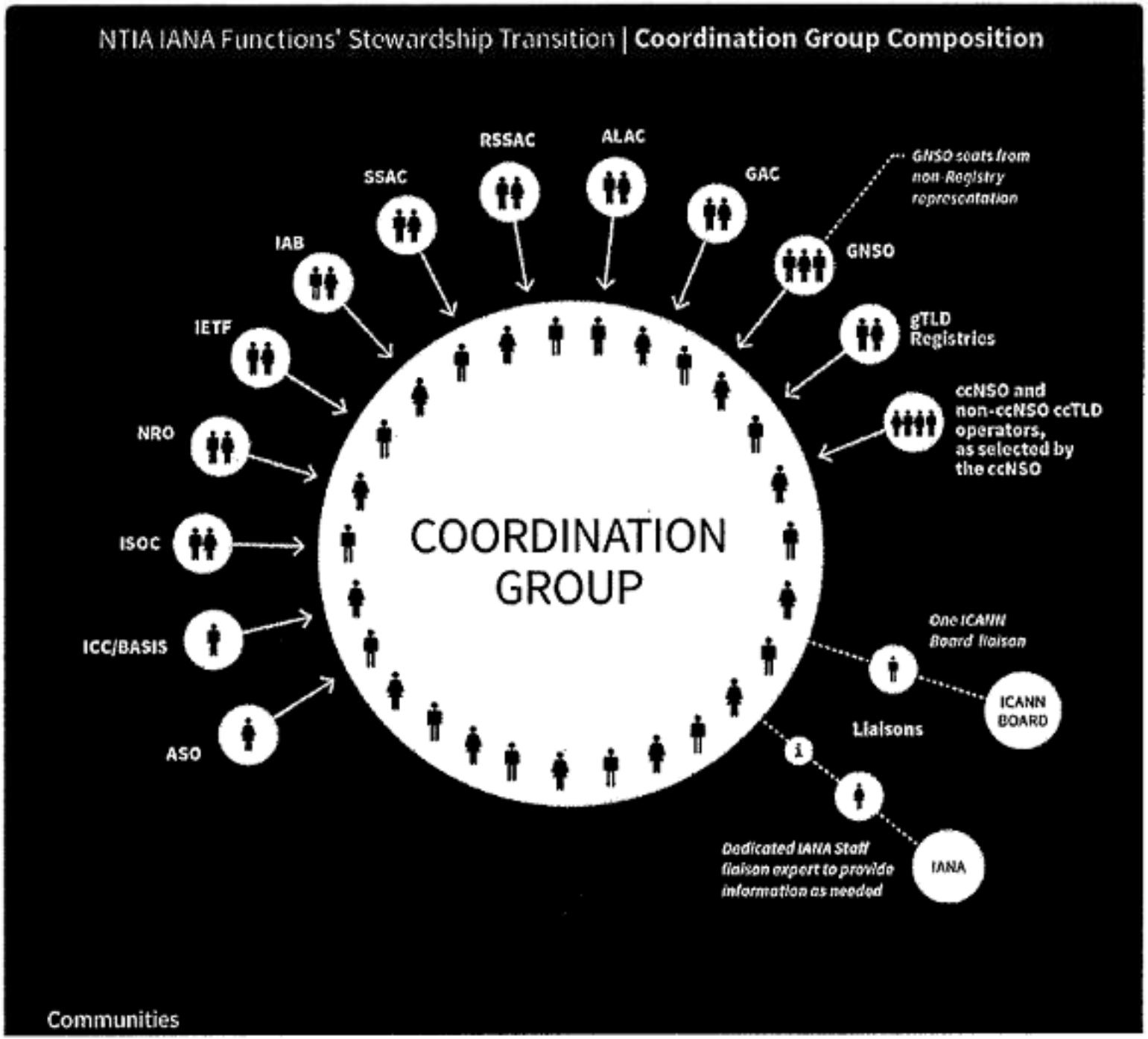
ICANN held a special community run session entitled Transition of NTIA's Stewardship of IANA Functions at the ICANN 50 Meeting in London.

Provided the community the opportunity to discuss all elements of the transition process.

Agenda:

+ Role of communities vs. the Coordination Group
+ Engaging participants outside of the traditional ICANN, IETF, and RIR participants
+ Defined success criteria
+ Relationship of the work on Accountability and NTIA Transition
+ Open Discussion

Sessions engaged in dialogue and received comments from a live-streaming chat room and over a dozen interactive hubs around the world.


NTIA IANA Functions' Stewardship Transition | Coordination Group Composition
RSSAC
ALAC
SSAC
GAC
GNSO seats from non-Registry representation
IAB
GNSO
IETF
gTLD Registries
ccNSO and non-ccNSO ccTLD operators, as selected by the ccNSO
NRO
COORDINATION GROUP
ISOC
ICC/BASIS
One ICANN Board liaison
ICANN BOARD
Liaisons
ASO
1
Dedicated IANA Staff liaison expert to provide information as needed
IANA
Communities

ICANN

As of 3 July 2014

Composition of IANA Stewardship Transition Coordination Group (ICG) announced.

Community	Member Name
ALAC	Mohamed El Bashir
ALAC	Jean-Jacques Subrenat
ASO	Hartmut Glaser
ccNSO	Xiaodong Lee
ccNSO	Mary Uduma
ccNSO	Keith Davidson
ccNSO	Martin Boyle
GAC*	Manal Ismail
GAC*	Heather Dryden
GAC*	Kavouss Arasteh
GAC*	Michael Niebel
GAC*	Jandyr Ferreira dos Santos
GNSO	Wolf-Ulrich Knoben
GNSO	Milton Mueller
GNSO	James Bladel
gTLD Registries	Keith Drazek

Community	Member Name
gTLD Registries	Jon Nevett
ICC/Basis	Joseph Alhadeff
IAB	Russ Housley
IAB	Lynn St Amour
IETF	Jari Arkko
IETF	Alissa Cooper
ISOC	Narelle Clark
ISOC	Demi Getschko
NRO	Adiel Akplogan
NRO	Paul Wilson
RSSAC	Daniel Karrenberg
RSSAC	Lars-Johan Liman
SSAC	Patrik Fältström
SSAC	Russ Mundy
ICANN Board Liaison	Kuo-Wei Wu
IANA Staff Expert	Elise Gerich

*17 July 2014 – The ICG accepted the GAC' s request to increase the number of GAC representatives in the ICG from two to five.

As of 18 July 2014

The ICG met for the first time on 17-18 July 2014 in London, United Kingdom.

In this first face-to-face meeting, the ICG:

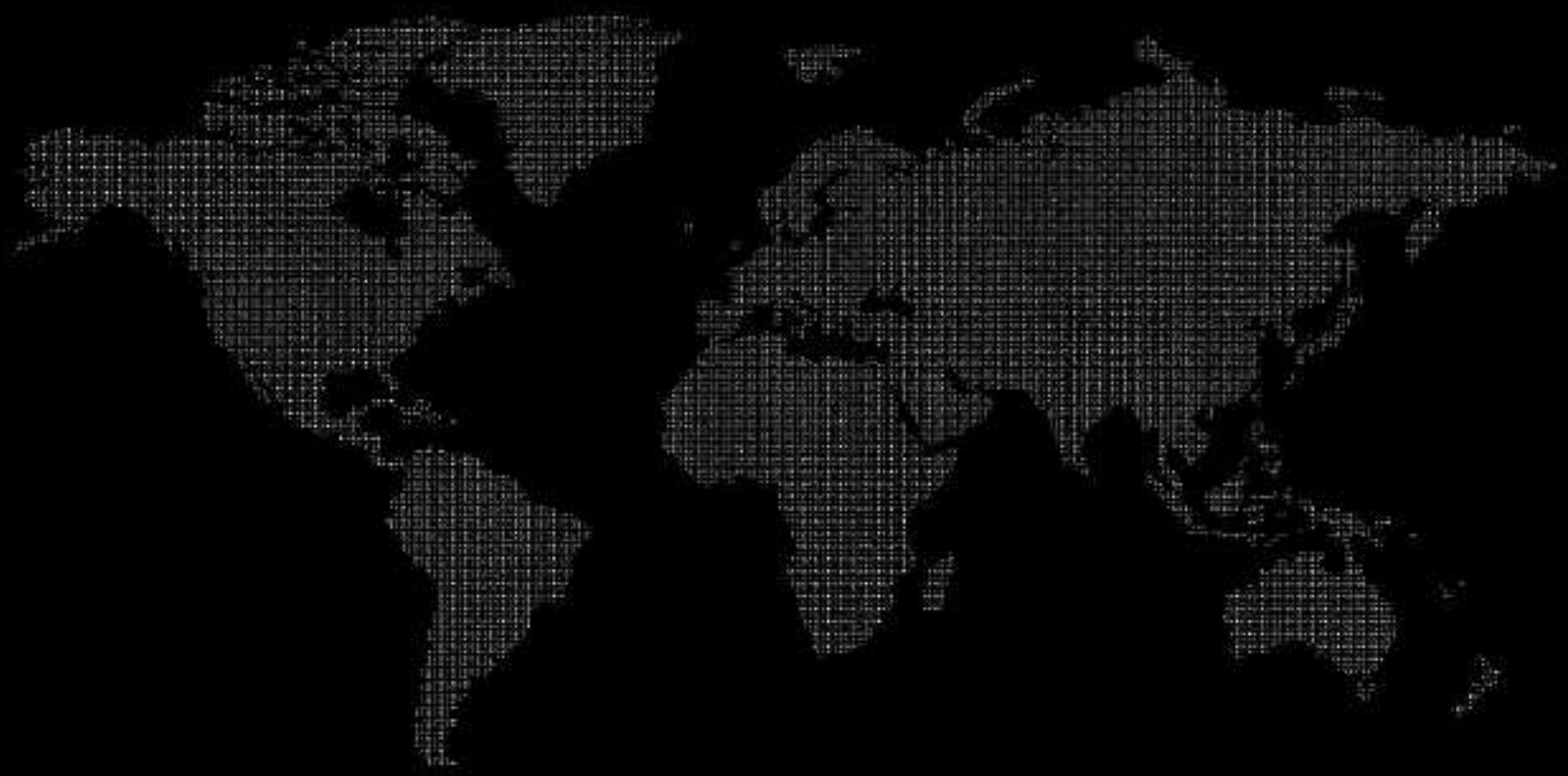
+ Developed a proposed charter and scope for its future work in support of the community's development of a proposal
+ Conducted an initial discussion of a draft timeline for development of the transition proposal
+ Worked on its internal organization, communications needs and participation processes

20 Members of the ICG attended in-person, one of whom was a GAC interim representative, and 2 liaisons; 5 participated remotely; 2 were unable to attend

Resources from the ICG meeting, including the meeting agenda, transcripts and audio translations can be found here:
https://www.icann.org/resources/pages/coordination-group-resources-2014-07-18-en

+ One topic at a time
+ 90 seconds comment per person
+ Please line up mic for each topic
+ Don’ t comment for different topic at a time
+ Give others a chance to comment
+ Don’ t repeat when someone already did

Thank You!



IANA Stewardship Transition and the Asia Pacific Community

Izumi Aizu, Sivasubramanian M., Kuo-Wei Wu
APrIGF New Delhi meeting
August 5th, 2014

Process for this session

Briefing "what the purpose and rule" (3 minutes)

Topics collect from floor (<5 minutes)

- Please name a topic (should be few words < 5) or two (no more than two each person), such as timeline, process,…
- Please don't repeat topic which is raised by other
- No more than 6 topics

Comments on the topics (75 minutes)

- Prioritize the topics in 2 minutes (please show hands)
- One topic at a time, and 12 minutes (the most) for each topic
- Not try to debate viewpoints, but collect viewpoints for CG to consider
- 90 seconds comment per person

The U.S. Government's Announcement

- On 14 March 2014, the U.S. Government (USG) announced its intent to transition its stewardship of the IANA functions to the global multistakeholder community
- As the first step, it asked ICANN to convene global stakeholders to develop a proposal to transition the current role played by the US
- ICANN was asked to serve as a convener based on its role as the IANA functions administrator (since 1998) and the global coordinator for the Internet's Domain Name System (DNS)
- The multistakeholder community has set the policies implemented by ICANN for more than 15 years

Transition Proposal's Guiding Principles

NTIA has communicated to ICANN that the transition proposal must have broad community support and address the following four principles:

1. Support and enhance the multistakeholder model
2. Maintain the security, stability, and resiliency of the Internet DNS
3. Meet the needs and expectation of the global customers and partners of the IANA services
4. Maintain the openness of the Internet

NTIA also specified that it will **not** accept a proposal that replaces the NTIA role with a government-lad or an intergovernmental organization solution.

What are the IANA Functions?

The IANA functions involve the coordination of unique Internet identifiers, including:

+ Maintenance of the protocol parameter registries on behalf of the IETF
+ Allocation of Internet Numbers in cooperation with the Regional Internet Registries
+ Management of the .ARPA and .INT domains
+ Administrative responsibilities of the DNS root zone
+ Coordination of root zone management

As of 29 March 2014:

ICANN launched a multistakeholder (global in scope) process at the ICANN 49 Meeting in Singapore.

Based on initial input, from 8 April – 8 May 2014, ICANN issued a call for public comment on the draft principles, mechanisms and process to develop a proposal (translated into 5 official UN languages, plus Portuguese).

Community response to draft process:

+ 700 email exchanges
+ 60 process contributions
+ Participation from global stakeholders, including government, private sector, civil society, technical, academic community and end users
+ Submissions made in different languages

As of 24 April 2014:

A special session was held at NETmundial conference in Brazil.

- Over 1,000 attendees from 116 countries
- 1168 remote participants from 33 worldwide remote hubs in 23 countries
- Participation from global stakeholders, including government, private sector, civil society, technical, academic community and end users

ICANN' s GSE team and partner organizations have been and continue to engage in a series of regional dialogues with global stakeholders.

As of 6 June 2014:

Informed by input on the draft process and subsequent dialogues, the Process to Develop a Proposal and Next Steps was posted online, echoing community feedback.

- Renamed the proposed "Steering Group" to "Coordination Group"
- No role for the Chair of the ICANN Board and Chair of the GAC in selection of members
- Direct representation
- Eliminated the distinction between affected and non-affected parties
- Revised composition to ensure greater balance and representation, including indirect stakeholders non-prescriptive about the roles and responsibilities of the Coordination Group
  - Coordination Group will establish its own working methods and modes of operation
- ICANN maintains neutral role as convener and facilitator of process
- Coordination Group encouraged to adhere to diversity standards as they undergo internal selection processes

As of 26 June 2014

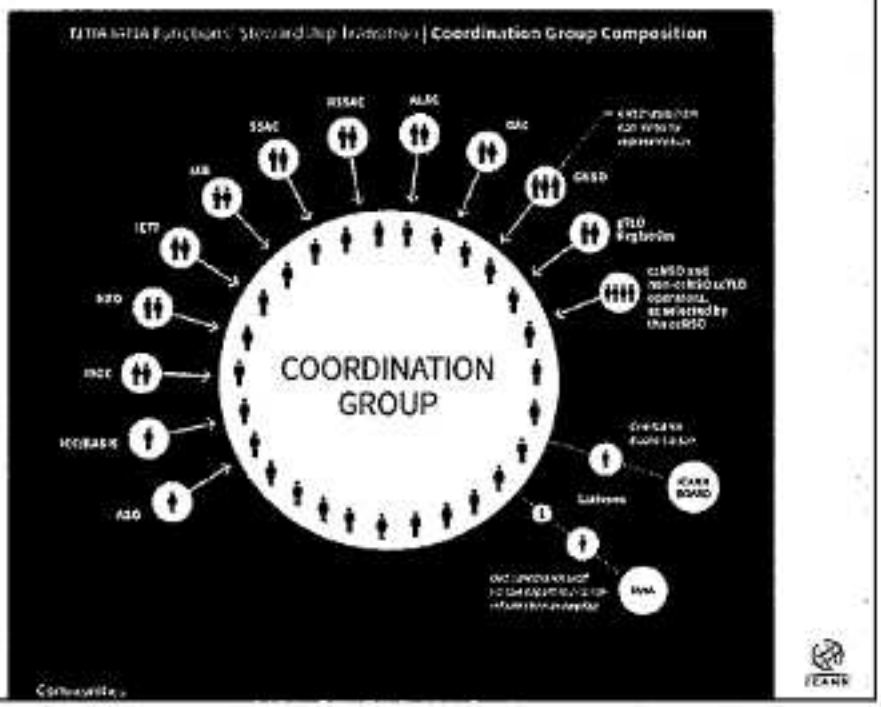
ICANN held a special community run session entitled Transition of NTIA' s Stewardship of IANA Functions at the ICANN 50 Meeting in London.

Provided the community the opportunity to discuss all elements of the transition process.

Agenda:

+ Role of communities vs. the Coordination Group
+ Engaging participants outside of the traditional ICANN, IETF, and RIR participants
+ Defined success criteria
+ Relationship of the work on Accountability and NTIA Transition
+ Open Discussion

Sessions engaged in dialogue and received comments from a live-streaming chat room and over a dozen interactive hubs around the world.



As of 3 July 2014

Composition of IANA Stewardship Transition Coordination Group (ICG) announced.

Community	Member Name
ALAC	Mohamed El Bashir
ALAC	Jean-Jacques Subrenat
ASO	[illegible]
ccNSO	Xiaodong Lee
ccNSO	Mary Uduma
ccNSO	Keith Davidson
ccNSO	[illegible]
GAC*	Manal Ismail
GAC	[illegible]
GAC	Lars-Johan Liman
GAC	Suzanne Radell
GAC	[illegible]
GNSO	Wolf-Ulrich Knoben
GNSO	[illegible]
GNSO	James Bladel
gTLD Registries	Keith Drazek

Community	Member Name
gTLD Registries	[illegible]
ICC/Basis	Joseph Alhadeff
IAB	Russ Housley
IAB	[illegible]
IETF	Alissa Cooper
IETF	[illegible]
ISOC	Dewi Gettchew
ISOC	[illegible]
NRO	Paul Wilson
NRO	[illegible]
RSSAC	Lars-Johan Liman
RSSAC	[illegible]
SSAC	Russ Mundy
SSAC	[illegible]
IANA Staff Expert	Elise Gerich

*17 July 2014 – The ICG accepted the GAC's request to increase the number of GAC representatives in the ICG from two to five.

As of 18 July 2014

The ICG met for the first time on 17-18 July 2014 in London, United Kingdom.

In this first face-to-face meeting, the ICG:

- Developed a proposed charter and scope for its future work in support of the community's development of a proposal
- Conducted an initial discussion of a draft timeline for development of the transition proposal
- Worked on its internal organization, communications needs and participation processes

20 Members of the ICG attended in-person, one of whom was a GAC interim representative, and 2 liaisons; 5 participated remotely; 2 were unable to attend

Resources from the ICG meeting, including the meeting agenda, transcripts and audio translations can be found here:
https://www.icann.org/resources/pages/coordination-group-resources-2014-07-18-en

+ One topic at a time
+ 90 seconds comment per person
+ Please line up mic for each topic
+ Don't comment for different topic at a time
+ Give others a chance to comment
+ Don't repeat when someone already did

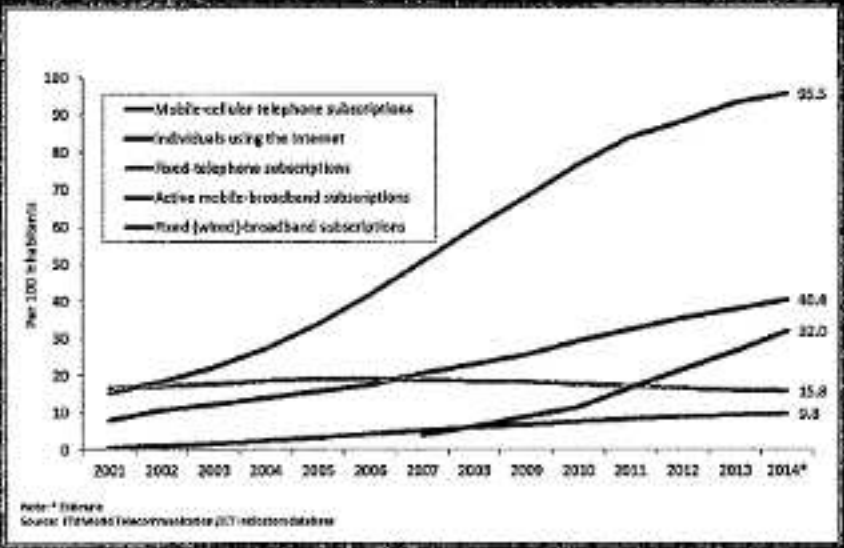
Thank You!

Creating a Culture of Cybersecurity for Innovations

Lailani Alcantara, Ph.D.
Ritsumeikan Asia Pacific University

Asia Pacific Regional Internet Governance Forum (APrIGF) 2014, India

Global ICT developments, 2001-2014



of the world population use internet

in Asia Pacific

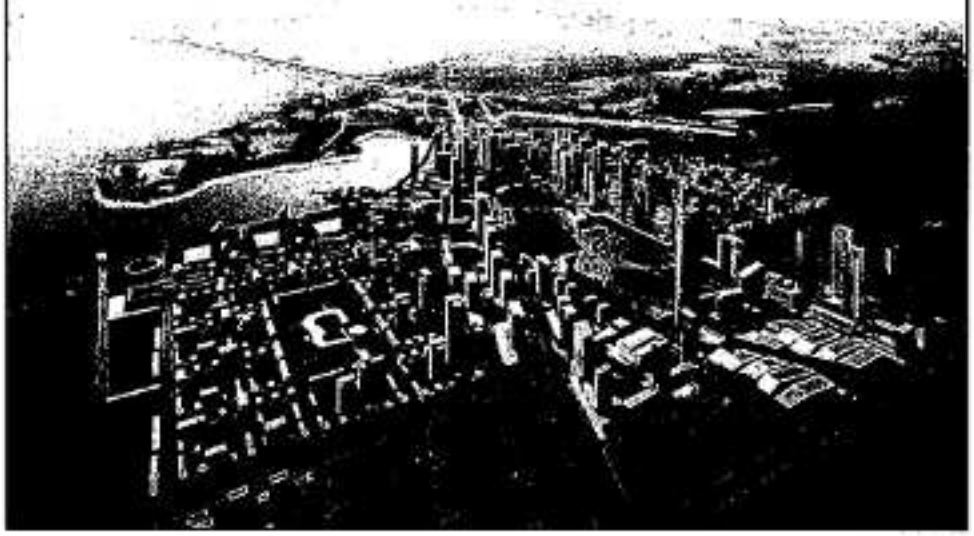
NEC $1.2 billion

HP $1 billion

Cisco $1billion

IBM $3 billion

Ubiquitous City in Songdo, Korea



Promise of
ICT Innovations

Threat to
Cybersecurity

Cybercrime bill in 24 countries:

Billion

victims/hour; 14 victims/second

million victims in 24 countries

Source: Norton Cybercrime Report, 2012

ACCA's Cloud Readiness Index, 2014

Country & ccTLD	1. Privacy	2. International Connectivity	3. Data Sovereignty	4. Broadband Quality	5. Government Regulatory Env	6. Power Grid and Green Policy	7. IP Protection	8. Business Sophistication	9. Data Centre Risk	10. Freedom of Information	CRI 2014 SCORE	RANK	CHANGE
Japan JP	9.5	5.5	8.0	9.1	5.0	7.1	8.1	8.2	6.6	9.7	76.8	1	-
New Zealand NZ	8.8	4.6	7.9	7.6	5.6	9.2	8.6	6.8	7.8	9.5	76.3	2	+4
Australia AU	8.8	4.4	7.6	8.0	5.3	7.8	7.6	6.7	9.4	9.6	75.1	3	+4
Singapore SG	6.0	8.2	7.8	8.8	6.1	5.9	8.7	7.3	7.4	8.6	74.8	4	-
Hong Kong HK	6.8	7.7	7.6	9.3	5.1	5.6	8.1	7.5	7.4	9.6	74.7	5	-2
South Korea KR	9.7	5.5	7.2	9.4	5.1	6.6	5.7	6.9	8.6	8.6	73.3	6	-4
Taiwan TW	4.6	6.3	6.8	8.5	5.0	6.7	7.4	7.4	6.9	8.0	68.2	7	-2
Malaysia MY	5.8	5.8	6.7	7.1	5.2	4.9	6.9	7.2	8.5	8.2	66.2	8	-
Thailand TH	4.0	5.0	6.2	8.0	3.7	6.3	4.4	6.3	7.6	7.8	59.3	9	+4
Philippines PH	5.8	5.4	5.9	4.1	3.7	5.5	5.1	6.1	5.5	9.0	56.1	10	+2
China CN	5.9	9.0	4.8	5.9	4.5	4.3	5.6	6.2	6.5	7.0	53.3	11	-1
Indonesia ID	4.4	2.9	6.2	3.1	3.9	5.7	5.6	6.3	6.4	7.9	52.4	12	-1
India IN	4.6	2.3	6.5	3.6	4.1	5.0	5.3	6.3	3.4	7.8	48.8	13	-4
Vietnam VN	3.6	3.2	5.6	4.3	3.8	4.7	4.1	5.3	6.4	7.0	47.8	14	-1

Source: Asia Cloud Computing Association (ACCA), 2014

Global cybersecurity spending:

$46 billion in 2013

Source: Yadron, 2014 (WSJ)

Hard measures are of course important, but **Soft measures** also matter.

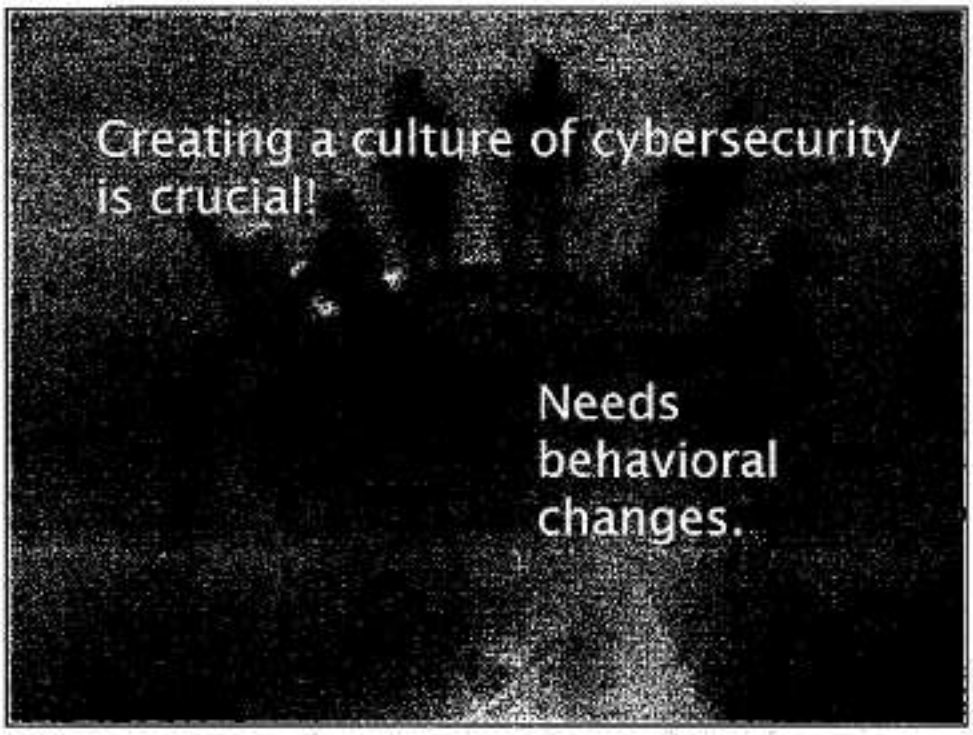
Internal Threats

"The question is not who is the enemy, the question is where are the vulnerabilities?"

Christy Wyatt, Good Technology CEO

Many companies, employees, don't realize the value of data, security.

- Websites from low context cultures are more likely to collect private information and disclose/consent such action compared with those from high context cultures (Reay, Beatty, and Miller, 2011)
- People from individualistic cultures are more comfortable/less uncomfortable with disclosing private information online (Bellman et al., 2004; Liu et al., 2013)
- People from cultures with low uncertainty avoidance are less concerned about privacy (Milberg, 2000)



Kotter's 8 Steps to Change

1. Establish a sense of urgency	Discussing with people the threats to cybersecurity and how business can be undermined
2. Form a guiding coalition	Assemble a team/division/office that handles cybersecurity
3. Create a vision	Creating a vision of cybersecurity
4. Communicate the vision	Making speeches, Providing cybersecurity manuals and trainings

Kotter's 8 Steps to Change

5. Empower others	Investing in cybersecurity technologies and services
6. Planning for and creating short-term wins	Surveying periodically individuals' attitude toward cybersecurity or customers' trust in information security
7. Consolidate improvements	Revising cybersecurity policies, developing and hiring cybersecurity experts
8. Institutionalize new approaches	Developing a formal cybersecurity training and education, strong leadership in cybersecurity

Kotter's 8 Steps to Change

1. Establish a sense of urgency.
2. Form a guiding coalition
3. Create a vision
4. Communicate the vision
5. Empower others
6. Create short-term wins
7. Consolidate improvements
8. Institutionalize new approaches

To enable and capitalize on ICT innovations, creating a culture of cybersecurity is crucial.

Thank you!

Cybersecurity policy, strategy and implementation in the Asia Pacific region: The nature of the heterogeneity and its implications

Nir Kshetri
University of North Carolina—Greensboro

APrIGF Delhi 2014

August 4, 2014

Panelists

- Lailani Alcantara, Ritsumeikan Asia Pacific University
- Kamlesh Bajaj, Data Security Council of India
- Hideyuki Fujii, InfoCom Research
- Nir Kshetri, University of North Carolina--Greensboro
- Aroop Menon, SolarWinds, Industry
- Sunanda Sangwan, Shantou Business School (SBS)
- Hong Xue, Institute for Internet Policy & Law

High profile policy initiatives to strengthen cybersecurity in Asia

- China: A body to coordinate CS headed by President Xi Jinping.
- India: NCSP 2013: developing 500k skilled CS professionals by 2018.
- Japan: 2014 New Year's message, PM Abe: constitution limits the use of military to situations involving self-defense: could be amended by 2020.
  - Cyber-threats: a rationale behind the proposed amendment.
- South Korea: 2013 announced: $8.76b spending by 2017 and train 5,000 CS experts.

Key differences among major economies in the region

- Relative focus on a given dimension of CS
- Significant variation in the power and influence of various stakeholder groups.
- Membership in international organizations related to cybersecurity.
- Devotion of resources in cybersecurity.
- Cybersecurity-related relationship with Western countries

SECURITY

EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers

Nir Kshetri, *University of North Carolina at Greensboro*
San Murugesan, *BRITE Professional Services*

To secure information systems and protect vital national and global infrastructure, IT professionals need to understand key elements of national cybersecurity strategies and their impact and coordinate their efforts at local, national, and global levels.

CLOUD COVER

Cloud Computing and EU Data Privacy Regulations

Nir Kshetri, *University of North Carolina at Greensboro*
San Murugesan, *BRITE Professional Services, Australia*

To leverage the cloud's power, EU authorities must revisit policies related to various types of personal data and their associated privacy risks.

SECURITY

Japan's Changing Cybersecurity Landscape

Rie Kubota
University of North Carolina at Greensboro

Japan's cybersecurity efforts have been lacking compared to other advanced economies, but the country is now taking more aggressive steps to address this deficiency.

As late as 2012, Japan hadn't officially acknowledged cyber-attacks as a national

Once Cabinet members started changing the conversation to increase Japan's cyberdefense as well as traditional military defense capabilities

moment in Mitsubishi Heavy Industries most eye-opening event in both policymakers and business executives. According to Mitsubishi

CS in Japan: Similarities and differences with EU and US

	EU	US
Similarities	• No sector specific regulations • Concerns about privacy/data protection, Japan's use of Big Data/cloud limited.	• To some extent relies on private sector self-regulation • Facing major cyber-attacks originated from foreign countries
Differences	• Collection, processing and transfer of personal data do not require the individual's consent. • Businesses no general obligation to delete personal data after use. • Company offering online services not required to report cyber-attacks.	• No privacy commission or agency equivalent to FTC. • CS specialists have an extremely low tendency to move across the private sector, public sector, and the academia.

PRIVACY IN CHINA

China's Data Privacy Regulations:

A Tricky Tradeoff between ICT's Productive Utilization and Cybercontrol

Ali Ibahrine | University of North Carolina at Greensboro

China's data privacy regulations contrast sharply with other major economies owing to internal and external pressures the Chinese government faces. Whereas the EU places high priority on protecting personal data and the US emphasizes self-regulation by businesses, China's regulations focus on cybercontrol measures.

Comparison of China, EU and the US

Dimension	China	EU	US
Salient feature	China encourages purely economic use of information and currently sustains limited rules and stricter cybercontrol measures.	EU policies indicate strict enforcement of privacy rights through legislation.	The US shows a preference to rely mainly on voluntary self-regulations but with sector-specific regulations for sensitive data.
Key driving factors	China aims to balance economic modernization and maintenance of unity and stability through political control.	Primarily due to World War II era fascist and post-War communists' use of secret files as the basis for nefarious activities, Europeans are more fearful of the prospects of personal information abuse.	The US encourages marketing and innovation.
Effects on IT providers	Chinese policies lack the specificity required for accurate understanding and compliance. The 2012 Online Data Protection Regulation is broad and vague and leaves guiding principles with law. Many provisions, such as do parents or agency to supervise and enforce, are unclear. No specific details are provided about the actions and amounts of penalties.[4] Lack of enforcement means that there's little legal recourse the state study by employees or employers are also during police inspections.	Requirements for compliance with strict regulations and the lack of economies of scale due to market fragmentation have impaired marketplaces and acted as a barrier to incentive for the development and diffusion of cloud and other technologies. The EU Directive, which is stricter than US regulations, is likely to have more wide-ranging impact on all business types. It would require more than 42,000 firms in banking, transport, energy, and healthcare sectors and Internet and public administrations to inform their respective national network and information security authorities if their networks are breached.	There is a deep concern among EU-based consumers and activists that US cloud service providers are required to disclose data stored in clouds to their government without the data owner's consent or knowledge. Although US officials and vendors have emphasized that such concerns are exaggerated and overblown, convincing EU-based customers and activists that the Patriot Act doesn't present a risk has been a challenge for US providers.
Effects on IT users	Unavailability of some services has been a concern. Some Bridge Data have focused their servers in neighboring countries, which has caused a severe negative impact on service quality.	Users enjoy a high level of privacy but due primarily to the lack of choices and quality of cloud services, consumers are slower to adopt the cloud. According to Gartner, from 2011 to 2016, North America (led by the US) is expected to account for 58 percent of public cloud spending ($77.9 billion), compared to Western Europe's 22 percent share.	There have been some concerns related to the government's monitoring and companies' misuse of citizens' information.

Kshetri, Nir (2014). "India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership" *IEEE Security & Privacy* (forthcoming)

Kshetri, Nir (2014). "Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses", *East Asia* (forthcoming).

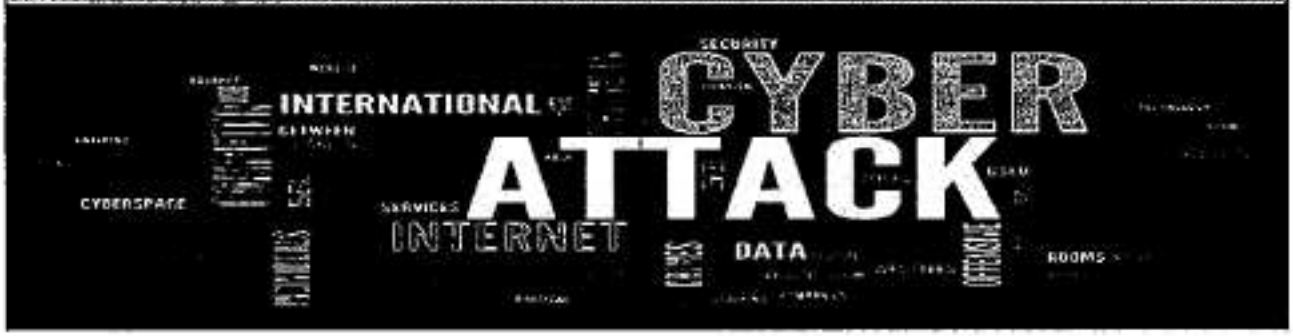
South Korea's recent initiatives and actions

- Cyber-command (2010), cyber-protection policy team at the Defense Ministry (2011), Cyber Policy Department (2013), plan to have a secretary of cybersecurity
- Psychological warfare against the North: posting to NK's social networking websites
- Teamed up with KU: cyber-defense school
- CS cooperation with the U.S.
- Intention to develop weapons similar to Stuxnet

Asia Pacific Regional Internet Governance Forum

INDIA'S CYBERSECURITY STATUS

Contexts and Mechanisms



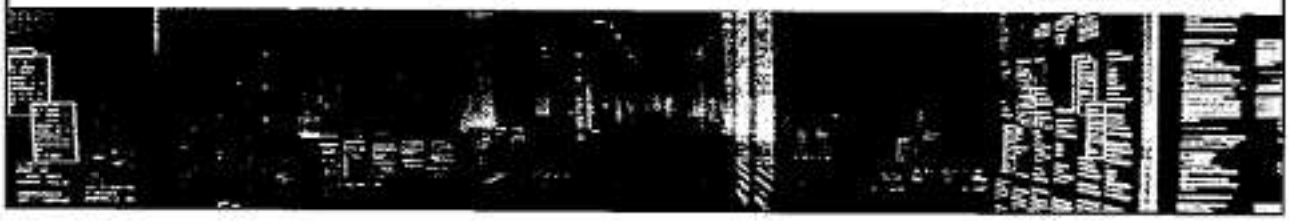
OBJECTIVE

- Insights into Indian Government's constraints in strengthening cybersecurity
- Examine the motivations, contexts and mechanisms to strengthen cybersecurity vis-à-vis Private Sector and Government
- The need and imperative for the Public Private Partnership
- Role being played by Indian Government for strengthening PPP in Cybersecurity

In a Nutshell, we try to analyze the appropriateness of a public private partnership as an institutional means of dealing with underdeveloped cybersecurity related institutions - Case study on India

CURRENT CYBERSECURITY LANDSCAPE OF INDIA
SOME FACTS

- Government of India released **National Cybersecurity policy (NCSP)** July 2013 -14 key objectives including:
  i. Enhanced protection for critical infrastructure
  ii. Developing 500,000 skilled cybersecurity professionals
  iii. Emphasis on the development of public-private partnership (PPP)
- Various instances of data breaches reported from the IT and BPM sectors. E.g. Threat of Insider Abuse
- Unprecedented Pressure from foreign offshoring clients to improve cybersecurity. E.g. Contractual Clauses
- 2011, India and U.S sign MoU to promote cybersecurity –related cooperation.
- 2012 bilateral talks (India-US)- Emphasis on India's ability to detect and investigate cybercrime incidents



KEY REASONS WHY INDIA NEEDS CYBERSECURITY PREPAREDNESS

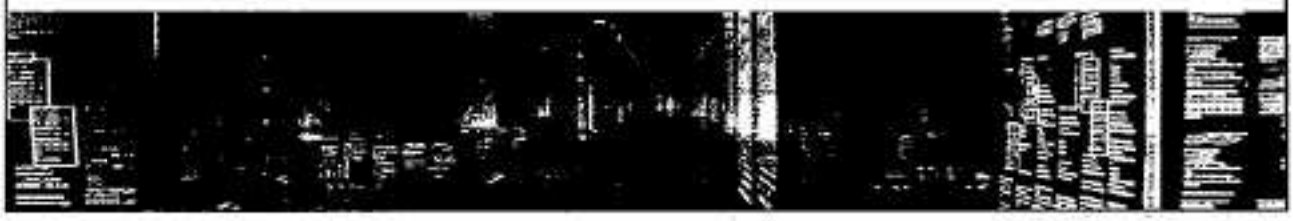
- Rapidly growing IT and Business Process Management Sectors
- Increasing use of Social Networking and Mobile Computing Make India Vulnerable to cybercrime
- Lack of resources for development and enforcement of cybersecurity-related regulations and standards
  I. In 2011, Delhi Police cybercrime cell had only 2 inspectors
  II. In 2012: Delhi High Court criticized the lack of functionality of the Delhi Police website
  III. In 2004, of the 4,400 police officers in Mumbai city, only five worked in the cybercrime division
  IV. The conviction rate in cybercrime cases is estimated at 2%
- Lack of technical skills/knowledge of police stations
- Lack of training to collect evidence required for court cases
- Similar scenario within the legal institutions-Lack of Awareness

SO WHAT'S BEING DONE CURRENTLY?

- India's IT&BPM sector is managing the cybersecurity risks through effective industry self-regulation.
- Highly visible private sector actor National Association of Software and Services Companies (NASSCOM) and Data Security Council of India
- Exemplary institutions that have played key role in enhancing and strengthening cybersecurity orientation of th IT&BPM sector
- They have been working with the government and law enforcement agencies in the formulation and enforcemer of cybersecurity-related legislation

CONSTRAINTS FACING THE GOVERNMENT IN A DEVELOPING ECONOMY IN STRENGTHENING CYBERSECURITY

- Underdeveloped regulatory structures for Nascent sectors such as cybersecurity
- There is no template for policy development, assessment and analysis.
- Weak public administration, inadequate technical competence and weak political leadership
- Positioning of the Government (its subject position) – "Art of Playing Politics"
- Allocation of disproportionately more resources to develop the modern sectors IT&BPM face stiff opposition. For e.g.: Chandrababu Naidu Government of Andhra Pradesh in 1998.



WHAT IS PUBLIC-PRIVATE PARTNERSHIP?

Cooperative relationships between Public and Private sectors, under which the latter undertakes actions that have been traditionally performed by the former

THE NEED AND IMPERATIVE FOR PUBLIC-PRIVATE PARTNERSHIP (PPP)

Private and Public actors have different goals agendas and interests

Why team up with the State :

•Most important institutional and powerful actor

•Has the ability to impose harsh sanctions/penalties

•Can act against perpetrators who violate laws and regulations

Why team up with Private Bodies like Trade associations such as NASSCOM :

•They have access to technology and resources

•They do not face some of the constraints that those which limit state's ability to monitor and control cybercrime activities

THE NEED AND IMPERATIVE FOR PUBLIC-PRIVATE PARTNERSHIP (PPP)

Why Public-Private Partnership

Allows Public sector to

- Employ private sector's capital and technology
- Share risks with the private sector in order to provide the delivery of public services or goods

Allows Private sector

- To increase profits by gaining support/trust of Public sector
- State plays a key role in creating a conducive institutional environment for PPP
- State helps with the enactment and enforcement of necessary laws

THE NEED AND IMPERATIVE FOR PUBLIC-PRIVATE PARTNERSHIP (PPP)

- The Indian government and the private sector actors (e.g., the NASSCOM and the DSCI) have partly overlapping motivation and objectives in strengthening cybersecurity
- IT&BPM sector plays a strategic role in the national economy/ most high-profile and widely publicized cybercrimes are mainly concentrated in the sector
- PPP in cybersecurity is especially important in India as NASSCOM and DSCI are widely renowned and acknowledged for their technical expertise and understanding on the subject.

Analysis of the Current PPP Scenario

Role Played by the Indian Government in Public-Private Partnerships and the Impact

Conduciveness of the Institutional Environment for PPP

I. Regulatory Role

II. Participatory Role

III. Supportive Role

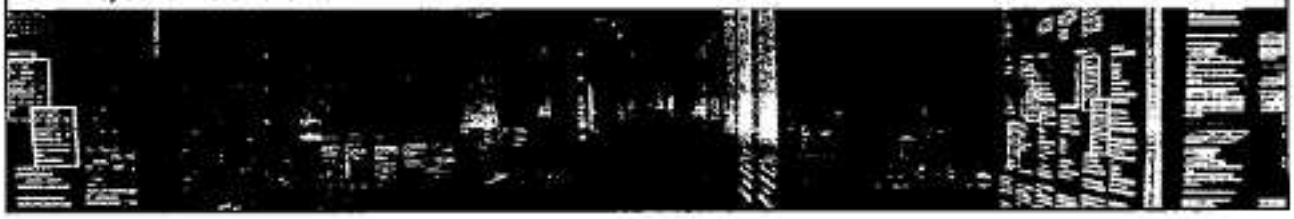
THE REGULATORY ROLE

Set of factors that influence

- The enforcement of contracts
- Sound political institutions and the rule of law
- A clean government that is free from corruption
- Bureaucratic quality
- A strong and effective court system and
- Citizens' willingness to accept the established institutions

WEAK REGULATORY ROLE PLAYED BY THE STATE

- Inability to upgrade legal infrastructure and court facilities due to budget constraints
- Failure of states to comply with federal directives to hire judges.
- Factors such as ineffective national legal systems
- Ambiguous laws-on-the-books
- Unsupportive attitude among law enforcement agencies, technological illiteracy and low level of cyber crime awareness.



NEGATIVE IMPACT OF STATE'S WEAK REGULATORY ROLE

- Low reporting of cybercrime incidents
- According to unscientific estimates, about 10% of cybercrimes are reported
- Rule of law is weak and ignored with impunity e.g. fake resumes submitted

POSITIVE OBSERVATIONS

- Lacks standard identifiers like the U.S. Social security number making it difficult to check potential employees' backgrounds- National Skills Registry was formulated by NASSCOM
- Indian Computer Emergency Response Team (CERT-In) established in 2004
- CERT- In Acts as an advisory for alerts and threats-create an incident response model
- Number of seminars and workshops launched to train law enforcement and Judiciary
- Judicial officers are being trained to handle cases involving intellectual property
- Greater cyber diplomacy with U.S, European Union and countries like Japan

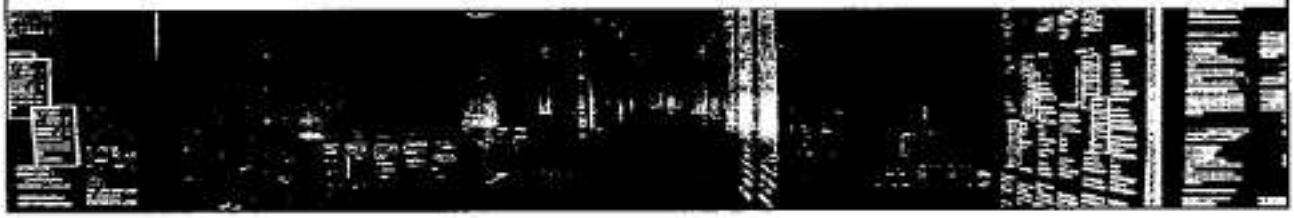
PARTICIPATORY ROLE

The participatory state captures the extent to which policies and institutions represent the wishes of the members of society

In such a state, businesses may participate in the national policy making and work closely with state agencies to protect their independence and autonomy

POSITIVE OBSERVATIONS

- The Economic Liberalization : Major driving force behind the growth/importance of trade associations.
- A strong mutual interdependence between the state and the private economic actors has developed quickly
- The liberalization thus resulted in more room for associations to flourish and to have a strong voice
- Created a conducive environment for Private actors towards increased participation in Policy Development
- Created an increasingly favorable climate for a higher participatory involvement in cybersecurity
  - Joint Working Group (JWG) on Cyber Security
  - The JWG released its report "Engagement with Private Sector on Cyber Security" in October 2012



THE SUPPORTIVE ROLE

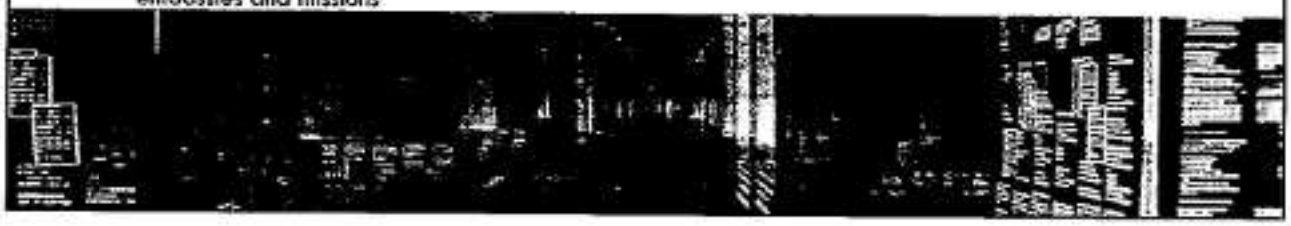
A government can carry out supportive roles in the development of a specific industry (e.g., cybersecurity)

- By legal and non-legal influences
- Address barriers related to skills, information, market, technology and infrastructures

POSITIVE OBSERVATIONS

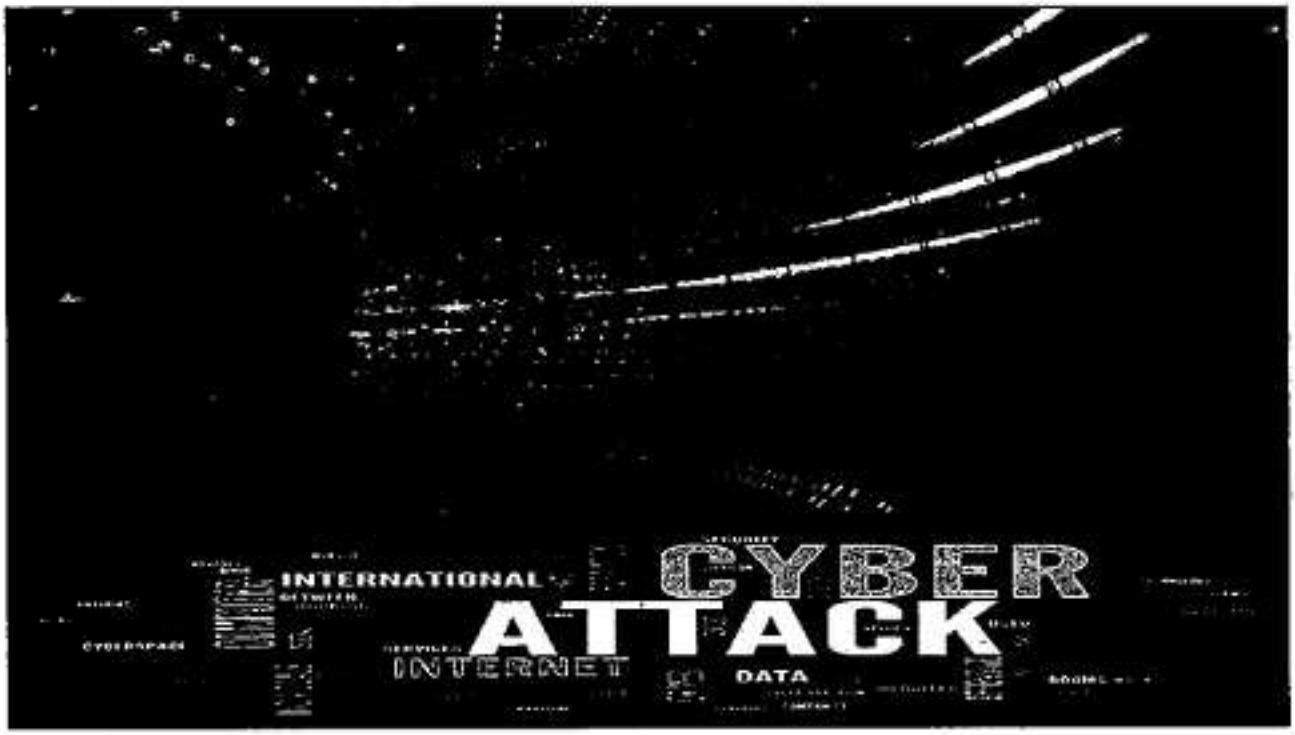
The Indian government has shown a higher level of support and commitment to cybersecurity

- For instance, the NASSCOM asked the government to create a special court to try people accused of cybercrimes.
- As a response, in 2009, the government inaugurated the first cyber regulation court in Delhi.
- The Indian government announced the possibility of providing financial assistance to Indian firms for acquiring foreign firms with high-end cybersecurity technology.
- The Ministry of External Affairs would explore possible targets worldwide through Indian embassies and missions



CONCLUDING THOUGHTS

- PPP is the most notable feature of India's cybersecurity landscape
- PPP in Cybersecurity in India has been a success within IT & BPM sectors
- NASSCOM and DSCI has played a key role in this –Driving force
- PPP has resulted in enactment of rules on cybersecurity- Pressure from the Private actors
- The success within IT & BOM sectors needs to spillover to other sectors within the economy
- Some of the vacuum from a weak regulatory role by the state can be filled by Private actors
  - Bring order and regulations to members
  - A decentralized enforcement can be initiated


INTERNATIONAL
CYBER
ATTACK
INTERNET
DATA

Cybersecurity Strategies and Policies in Japan

2014/8/4

Hideyuki Fujii
InfoCom Research

AGENDA

1. Cybersecurity in Japan
- 1-1. What does "cybersecurity" mean in Japan?
- 1-2. Cyber risks are increasing in Japan
- 1-3. Japanese government's approach

2. Cybersecurity Strategy 2013
- 2-1. About strategy
- 2-2. Coordination Framework
- 2-3. Cybersecurity and Secrecy of Communication

3. Hot issues
- 3-1. Public-Private cooperation
- 3-2. Global cooperation
- 3-3. 2020 Tokyo Olympic/Paralympic

1. Cybersecurity in Japan

1-1. What does "cybersecurity" mean in Japan?
1-2. Cyber risks are increasing in Japan
1-3. Japanese government's approach

1-1. What does "cybersecurity" mean in Japan?

- Most of the countries published their own "national cybersecurity strategy" or, a alternatively named, a "national information security strategy".
- But the understanding of "cybersecurity" differs greatly among countries.

"only eight of the 18 nations define the cyber security notion. Two nations descriptively characterise cyber security using a descriptive text."
Luiijf and Basseling (2013)

The lack of a common definitions across nations may cause confusion between nations when discussing international approaches to the global cyberspace threats!

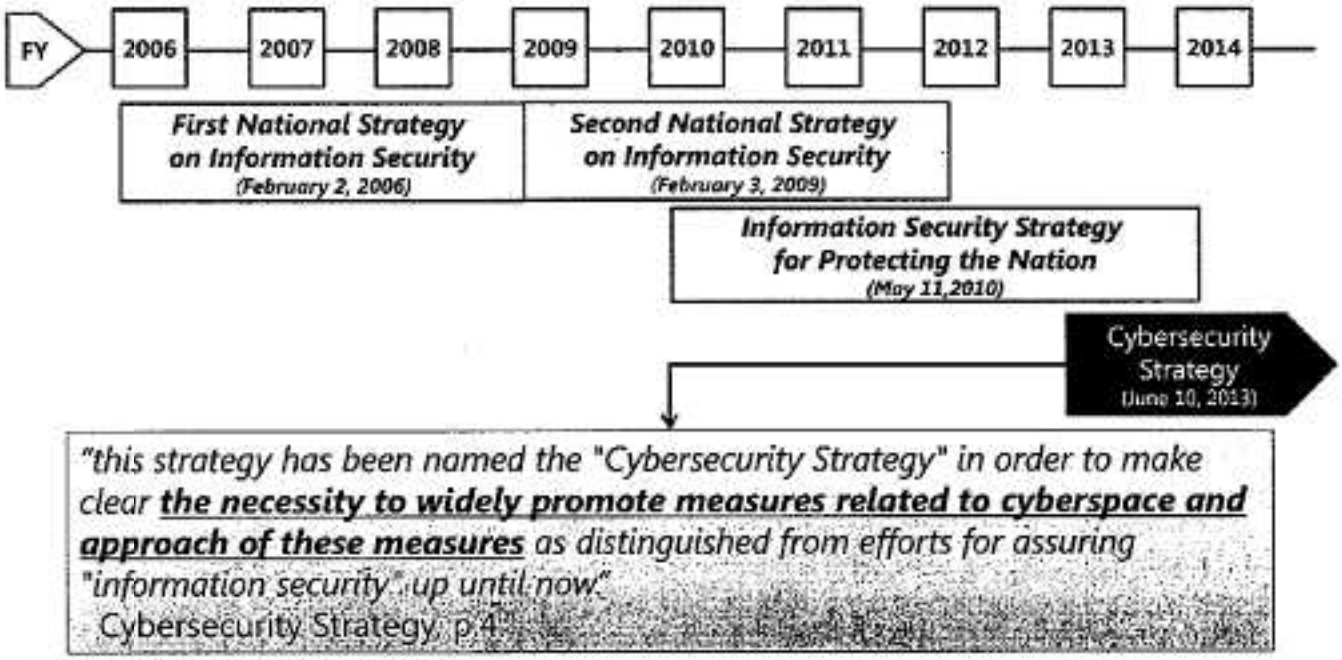
Reference: Eric Luiijf and Kim Besseling, "Nineteen national cyber security strategies," Int. J. Critical Infrastructures, Vol.9, No. 1/2, 2013.

Table 1 National understanding of "cyber security" (when defined or described)

	Definition?	Cyber Security
AUS	definition	Are measures relating to the confidentiality, availability, and integrity of information that is processed, stored and communicated by electronic or similar means.
CAN	description	Is an appropriate level of response and/or mitigation to cyber attacks – the intentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.
DEU	definition	Is the aim of objectives of the EU security situation, in which the risk of (global) cyberspace has been reduced to an acceptable minimum. Here, German, civil, and military cyber security are defined in similar wordings.
FRA	definition	Is an information system allowing to resist likely events resulting from cyber space which may compromise the availability, the integrity or confidentiality of data stored, processed or transmitted and of the related services that information and communication (ICT) systems offer.
GBR	description	Embraces both the protection of national interests in cyber space and also the exploitation within national security policy through exploitation of the many opportunities that cyber space offers [UK (2009), p.9].
IND	definition	Is the security of protecting information and information systems (networks, computers, databases, data centres and applications) with appropriate procedural and technological security measures.
NLD	definition	Is to be free from danger or damage due to the disruption or destruction of ICT, or due to the abuse of ICT.
NZL	definition	Is the practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability, and integrity of information, detecting intrusions and incidents that occur, and responding and recovering from them.
RUS	definition	Is necessity arising from applying a set procedures and decision measures that ensure confidentiality, integrity, availability, authenticity and non-repudiation of electronic information, and the private and public resources and services in cyberspace.
USA	implicit	References to "information security", the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
ZAF	definition	Is the collection of tools, policies, security concepts, security guards, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisations and user assets.

1-1. What is "cybersecurity" mean in Japan?

➢ Japanese government use the word "Information Security" until 2013 in national security strategy.



Reference: Cybersecurity Strategy (June, 2013)
http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

4

1-2. Cyber risks are increasing in Japan

➢ Risks have become remarkably **more "severe", "widespread" and "globalized"** and we are facing a new situation of "increasingly serious risks".

■ **More severe risks**

✓ **Risks which are a threat to national security as well as the lives, bodies, properties and other interests of people have appeared.**

*for examples: cases where TPP related information may have been leaked from government institutions, cases where issues arose related to the possible theft of technical information, etc. from critical infrastructure providers.

■ **More widespread risks**

✓ The rapid propagation of **smartphones** and other devices among people, expansion of **M2M/sensor networks**, the advent of conditions where everything is connected to the internet (**Internet of Things**) and other situations, have increased the spread of the risks by introducing conditions where the devices which can be **targeted by cyber attacks are present in every possible place and situation around us.**

■ **More globalized risks**

✓ In Japan, a greater level of handling is required for borderless, globalized risks as **many activities in real-space come to depend upon cyberspace.**

Reference: Cybersecurity Strategy (June, 2013)
http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

5

1-3. Japanese government's approach

➢ Previous framework (until 2013)

> In the previous strategies, each actor would maintain awareness of their own responsibilities and appropriately divide roles in accordance with their positions, situations and capacities.

⇨ based on a premise of each actor existing in a vertically divided structure.

➢ Cybersecurity Strategy (from 2013)

> It is thus imperative to strengthen the dynamic response capabilities of society as a whole by **having the wide variety of actors who depend on cyberspace to each continue to perform their own roles** while also **mutually cooperating and providing mutual aid**.

Reference: Cybersecurity Strategy (June, 2013)
http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

1-3. Japanese government's approach

OBJECTIVES

■ By 2015

✓ increasing the coverage of cyber attacks related **information sharing networks** in government institutions and critical infrastructure fields

✓ improving CSIRT installation

✓ reduce malware infection and people's anxieties

✓ Increasing the number of nations possible of participating in **international incident coordination** and the numbers of partners such as nations for **international collaboration and dialog** on response to cyber attacks by 30% increase.

■ By 2020

✓ doubling the size of domestic information security market

✓ halving the deficiency ratio in security professionals

Reference: Cybersecurity Strategy (June, 2013)
http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

2. Cybersecurity Strategy

2-1. About strategy
2-2. Coordination Framework
2-3. Cybersecurity and Secrecy of Communication

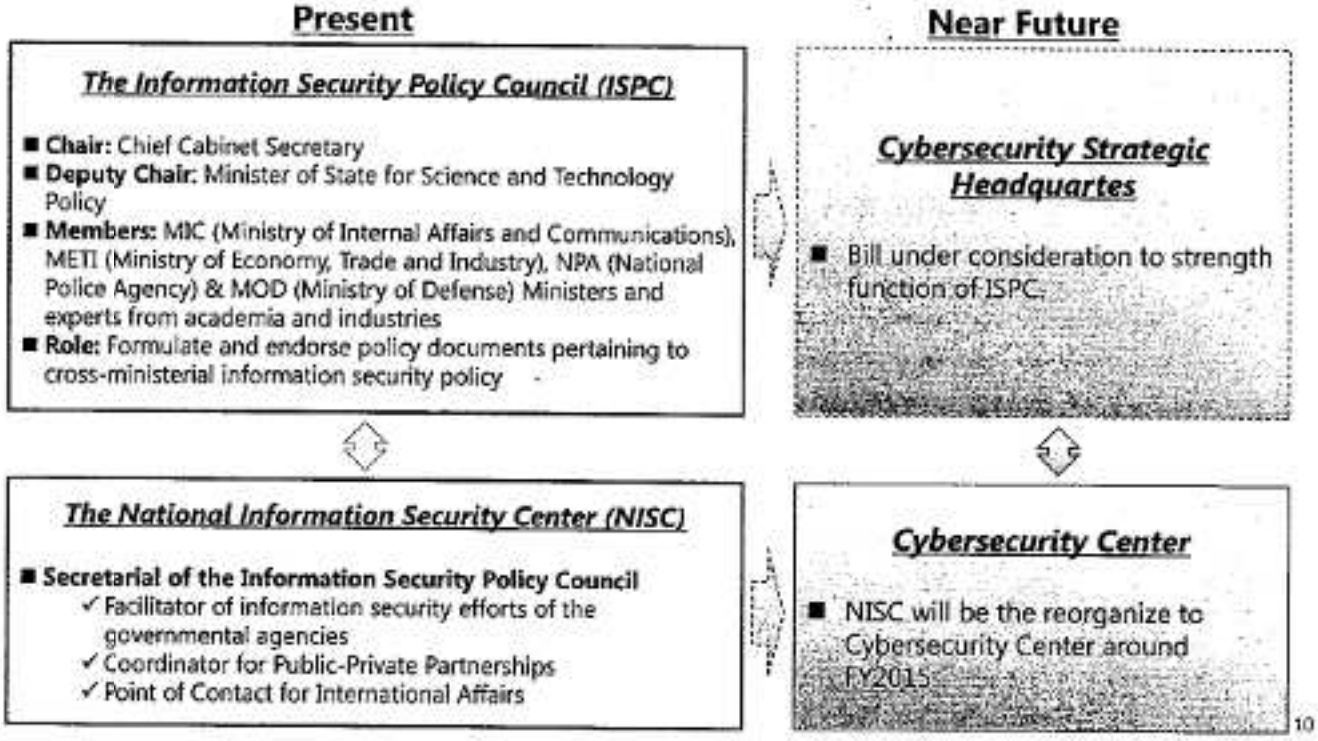
2-1. About Strategy

- On June 10, 2013, the Information Security Policy Council (ISPC) adopted the Cybersecurity Strategy.

http://www.nisc.go.jp/active/sihon/pdf/cybersecuritystrategy-summarizing-en.pdf

2-2. Coordination framework

- Although ISPC and NISC manage cybersecurity issues, current framework lack legal basis and authorities to enforce other government authorities to comply.



10

2-3. Cybersecurity and Secrecy of Communication

- In Japan, MIC regulates Internet and IP-based services under the Telecommunications Business Act.
- The Act emphasize protection of the "Secrecy of Communication".
  - ✓ Currently telecommunications carriers cannot examine e-mails containing viruses without the consent of users, although they can issue warnings in advance to prevent cyber attacks.

> Consideration will be given to measures for **preserving logs such as communication histories**, and promotion of digital forensics at relevant operators **in order to assure traceability for cybercrimes after the fact**.
> Regarding saving of communication histories in particular, **consideration will be carried out on their use in cybercrime investigations with due consideration given to the secrecy of communications**, types of effective communication histories for security, burdens of the communications operator saving the logs, storage periods of logs in foreign countries, and the diverse opinions of people as general users.
> (Cybersecurity Strategy, p. 41)

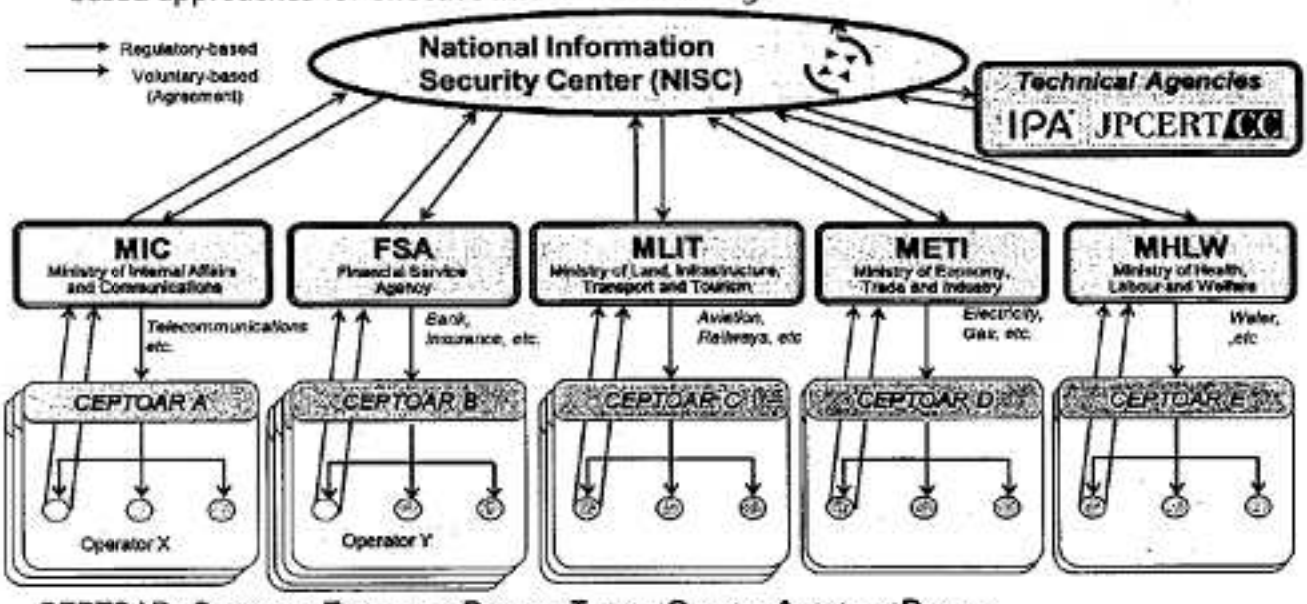
- **How to ensure effective investigations while safeguarding the secrecy of communications?**

3. Hot issues

3-1. Public-Private Cooperation
3-2. Global Cooperation
3-3. 2020 Tokyo Olympic/Paralympic

3-1. Public-Private Cooperation

➢ The Japanese government has deployed combined regulatory-based and voluntary-based approaches for effective information sharing.



CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response

Source: NISC

The CEPTOAR Council
- A private organization for voluntary information sharing
- Formed in February 2009

3-1. Public-Private Cooperation

- Efforts have been underway to establish Public-Private Cooperation, or Public-Private Partnerships (PPP) for cybersecurity.
- It's not easy to establish PPP in Japan because of segmented administrative system and competent minister own their cooperation system (CEPTER).

【US's PPP】
- "Improving Critical Infrastructure Cybersecurity" Executive order in 2013.
- DIB (Defence Industrial Base) Collaborative Information Sharing Environment

【EU's PPP】
- New EU cybersecurity directive (2013)
- European PPP for Resilience (P3R)

◆ There are many approach for regulating PPP and it depends on countries policy.

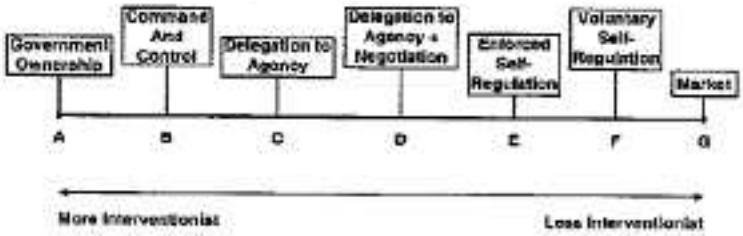


Fig. 1 – Regulatory continuum.

D. Assel, "Models of critical information infrastructure protection", International Journal of Critical Infrastructure Protection 1 (2008) 6-14.

3-2. Global Cooperation

- International Strategy on Cybersecurity - j-initiative for Cybersecurity – (October 2013)

【Asia Pacific】
- Close cooperation with the Asia Pacific region is crucial due to geographical proximity and close economic ties
- Continuing to strengthen the relationship with the ASEAN through:
  - ✓ Policy dialogues such as ASEAN-Japan Ministerial Meeting on Cybersecurity Cooperation, ASEAN-Japan Information Security Policy Meeting, and ASEAN-Japan Ministerial Meeting on Transnational Crime
  - ✓ Promoting Initiatives such as capacity building for human resources development
  - ✓ Promoting joint projects such as JASPER and TSUBAME
- Promoting Japan-India Cyber Dialogue, etc.

【U.S. and Europe】
- Deepening partnership with the U.S. centered on Japan-U.S. Security Arrangements
  - ✓ Promoting such policy dialogues as the Japan-U.S. Cyber Dialogue and the Japana-U.S Policy Cooperation Dialogue on the Internet Economy
  - ✓ Promoting cooperation in the area of cyber incident response
- Strengthening cooperation with European countries
  - ✓ Conducting policy dialogues such as the Japan-UK Cyber Dialogue and the Japan-EU Internet Security Forum
  - ✓ Conclusion of the Convention on Cybercrime

Reference: Reiko Kondo, "International Strategy on Cybersecurity Cooperation –j-initiative for Cybersecurity –
https://www.itsuai.jp/wp-content/uploads/2014/01/nb26-1_5_ssc.pdf

3-2. Global Cooperation

【Other regions】

- Extending cooperation to countries in regions such as South America and Africa where the use of cyberspace has rapidly progressed
  - ✓ e.g. Support for establishing CSIRTs
  - ✓ In regions such as South America and Africa, the use and application of cyberspace has also rapidly progressed. As consequence, a number of cybersecurity issues have surfaced including an increase in malware infections and other cyber threats. Japan has extended cooperation to countries in these regions, such as through provision of support for the establishment of CSIRTs. Going forward, Japan will further expand these efforts.

【Multilateral frameworks】

- Actively contributing to international rulemaking of cybersecurity:
  - ✓ Rulemaking at various forums such as the U.N., G8, OECD, and APEC.
  - ✓ Global initiatives with respect to critical infrastructure protection and rapid incident response undertaken at the Meridian, rWWN, and FIRST (e.g. Hosting the Meridian in 2014)

Reference: Keiko Kondo, "International Strategy on Cybersecurity Cooperation –j-Initiative for Cybersecurity–
https://www.isc.i.u-tokyo.ac.jp/wp-content/uploads/2014/01/sb26-1_5_sec.pdf

ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation (Tokyo, September 12-13, 2013)

- Address from the Prime Minister Shinzo Abe in the Meeting.

…

Japan, as a leading country in the field of ICT, has been pushing ahead of the world to take on the various, serious issues of cybersecurity. I hope that the wealth of knowledge that we have gained in that process can be shared overseas and that people will actively make use of it.

Cybersecurity is an issue of the utmost importance that we must not wait to act upon. In other words, I strongly feel the need for each country to join together, collaborate, and work on this issue. I believe that Japan and the countries of ASEAN should ensure the free flow of information, and at the same time, **we should pool our efforts, and work together toward creating a safe and vibrant cyberspace structure.**

……

- "Joint Ministerial Statement of the ASEAN-JAPAN ministerial policy meeting on cybersecurity cooperation"

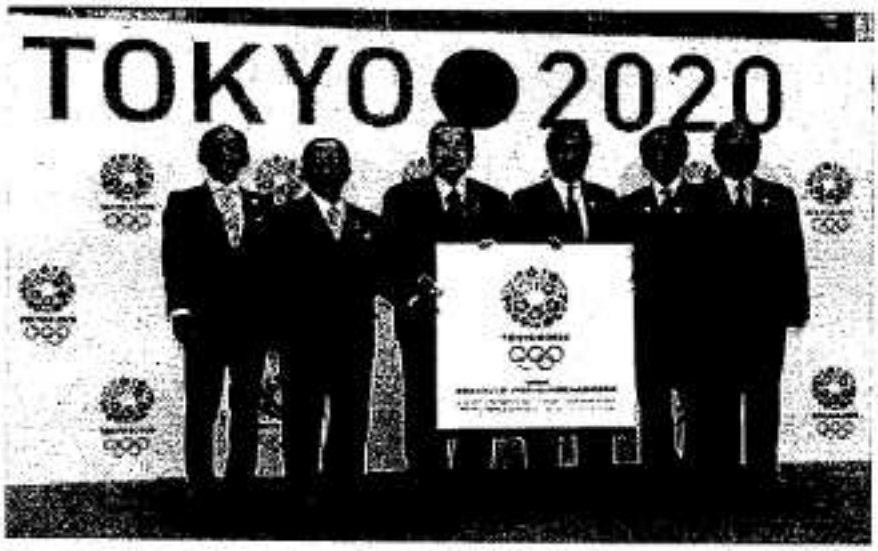
Encourage our senior officials to promoter our joint efforts further in the following areas:

1. **Creating a Secure Business Environment**
   - Encouraging public and private entities to enhance the level of cybersecurity through referencing best practices such as Information Security Management System (ISMS);
2. **Building a Secure Information and Communication Network**
   - Enhancing network security through activities such as information exchanges on anti-botnet and anti-spam measures;
3. **Enhancing Capacity for Cybersecurity**
   - Establishing a mechanism for ASEAN Member States and Japan to enable information sharing, and quick responses to cyber incidents through activities such as cyber exercises;

Source: http://japan.kantei.go.jp/96_abe/actions/201309/12asean_e.html
http://www.soumu.go.jp/main_content/000249127.pdf

3-3. 2020 Tokyo Olympic/Paralympic

- Tokyo is playing **host to the 2020 Summer Olympic/ Paralympic**.
- Reinforcing cybersecurity measures for the 2020 Tokyo Olympics is a pressing need.
  - ✓ Japan held a government-wide cyber security drill on March 2014, in a bid to improve coordination among public agencies and major businesses.



Source: http://www.japantimes.co.jp/news/2014/05/19/national/tokyo-to-boost-cybersecurity-role/#.UBPTeZRv7hk
http://www.reuters.com/article/2014/03/18/japan-cybercrime-idUSL3N0MF12920140318

THANK YOU!

Hideyuki Fujii
InfoCom Research, Inc.
h.fujii@icr.co.jp

Network Neutrality – Asia Pacific

ADAM PEAKE

CENTER FOR GLOBAL COMMUNICATIONS,
INTERNATIONAL UNIVERSITY OF JAPAN

Net Neutrality: a definition

The principle of "net neutrality" means that traffic should be treated equally, without discrimination, restriction or interference, independent of the sender, receiver, type, content, device, service or application.

European Parliament, proposed regulation, 26 March 2014

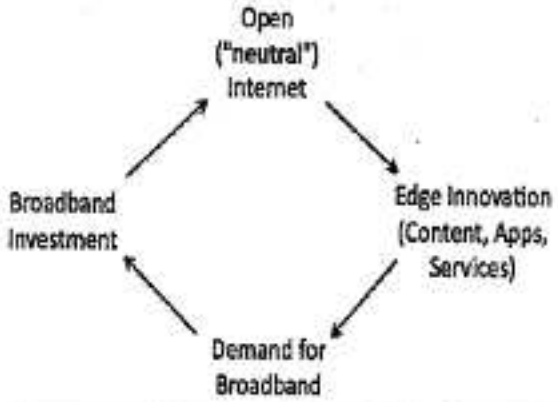
Net Neutrality: value

... the internet's open character has been a key driver of competitiveness, economic growth, social development and innovation –which has led to spectacular levels of development in online applications, content and services– and thus of growth in the offer of, and demand for, content and services, and has made it a vitally important accelerator in the free circulation of knowledge, ideas and information, including in countries where access to independent media is limited.

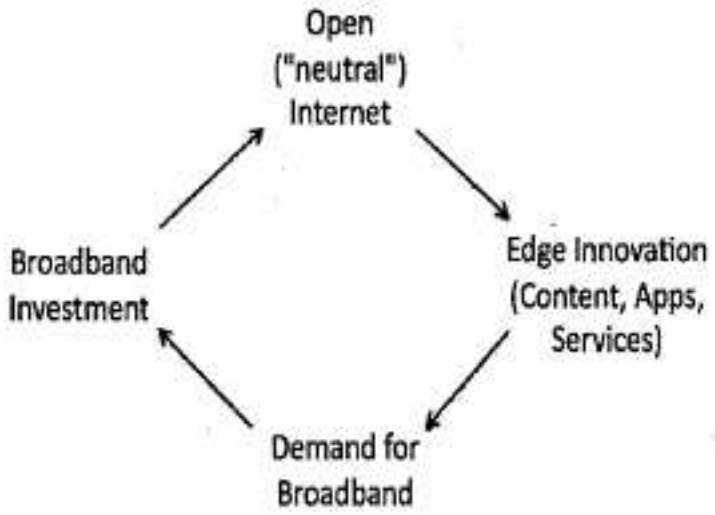
European Parliament, proposed regulation, 26 March 2014

Net Neutrality: value

[The FCC's] justification for the specific rules at issue here –that they will preserve and facilitate the "virtuous circle" of innovation that has driven the explosive growth of the Internet– is reasonable and supported by substantial evidence. *United States Court of Appeals for the District of Columbia, January 14, 2014*



Virtuous circle – Asia Pacific?



Net Neutrality – non neutral behavior

- Examples of non-neutral behavior:
- Blocking and throttling. Deep Packet inspection to see content type and source (what and from where).
- Prioritization (fast and slow lanes), favoring own content or that of a partner over other's.
- Examples from Asia Pacific: Japan, Korea, Vietnam.

Net Neutrality – Japan

General authority: Telecommunications Business Act prohibits any telecom carrier from unfair discrimination when providing services. Japanese Constitution maintains that the secrecy of any means of communication shall not be violated.

Recommendations strongly supporting net neutrality developed by industry (communications ministry as observer). Industry developed and adopted guidelines on packet shaping, managing traffic.

These recommendations apply to both fixed and mobile.

Non-Neutral: NTT public wifi access from a convenience store, found to be blocking access to websites of rival stores. Ministry rules against NTT based on violation of secrecy of communications, not the telecom business law.

Korea: protecting the ecosystem

Government has been interventionist in Internet/broadband sector: supporting and maintaining its development.

Concept of "Common Carrier" in the Telecommunications Business Act, prohibits discrimination by both fixed and mobile operators.

Net neutrality principles based on the FCC's 2005 Internet statement are included in the US/Korea FTA (2012).

Korea Communications Commission (KCC) has seemed reluctant to enforce these non-discrimination/fairness principles where disruption might affect the "health" of the broader ecosystem.

Korea: protecting the ecosystem

2011, mobile VoIP OTT (Kakao Talk, LINE, etc) start service. Mobile operators SK Telecom and Korea Telecom complain to KCC, began degrading service for lower price user plans.

KCC ruling allows operators to charge their subscribers for the access to these services.

2012, Korea Telecom cut off Samsung's smart TVs over complaints about the amount of data users were consuming: KT insisted Samsung should pay for the cost of the necessary bandwidth. Lasted 5 days, before KCC protested against the shut-down, a later investigation gave a mild punishment to KT.

KCC organized processes to develop net neutrality principles, and principles on traffic management, but hasn't yet implemented them as regulation or mandated guidelines.

Vietnam – response to OTT services

August 2013: government considers managing OTT messaging and voices services: cites lost revenue for communications operators from voice calls and SMS.

OTT today: Viber est. 13million users, Zalo (Vietnamese company) catching up with 12million.

February 2014: Viettel in talks to buy Kakao Talk. Mobifone, applies for license to operate own OTT service. The Vinaphone (and others) negotiating with OTT companies.

2013, Govt draft decrees on Information Technology Services, Internet Services and Online Information and Content my affect discrimination in the market.

Workshop on Network Neutrality in Asia Pacific

TIME	PROGRAMME
1330-1340	Welcome and Introductions **Ms. Lim May-Ann, Executive Director, Asia Cloud Computing Association, and Adam Peake, Executive Research Fellow, GLOCOM, International University of Japan**
1340-1350	**Network Neutrality in Asia** **Mr. Adam Peake, Executive Research Fellow, GLOCOM, International University of Japan** Net neutrality debates have been dominated by the US and EU. Wither Asia's opinion on this controversial issue? This session will review some observations on network neutrality regulations which have emerged from the Asia Pacific region.
1350-1400	**Business perspectives of network neutrality** **Mr. Subramanian Chandrasekhar, Director Government Affairs, Microsoft India** The recent NETmundial Stakeholder Statement is one of the first global statements around net neutrality which has been released. What are the factors impacting business investment choices, and where do they stand in terms of an equitable Internet for all?
1400-1410	**A Telco Perspective on Net Neutrality** **Mr. Vikram Tiwathia, Associate Director General, Cellular Operators Association of India** What constitutes "reasonable" traffic management for telcos and cloud providers? What other considerations around prioritised Internet access do data providers face today?
1410-1420	**User/Civil Society/NGO perspective on Net Neutrality** **Mr. Nikhil Pahwa, Editor & Publisher, MediaNama** What are consumer expectations around net neutrality? Beyond privacy issues, is there a fear that reasonable Internet access may soon be beyond the average consumer?
1420-1450	**Open discussion** Moderated by: Ms. Lim May-Ann, Executive Director, Asia Cloud Computing Association
1450-1500	Wrap-up – discussion highlights review, and closing

asia cloud computing association

@accacloud

is.gd/accacloud

About the Asia Cloud Computing Association

We are a leading influential industry voice on cloud computing – we involve business, government and people in Asia – the public, private and people sectors

Mission: to accelerate cloud computing adoption across Asia Pacific

Engaging stakeholders, providing tools to educate, and advocate to remove barriers to using cloud computing and other technology tools

http://www.asiacloudcomputing.org
(new!)

Contact the Secretariat at info@asiacloudcomputing.org

Working Groups and Thought Leadership

Cloud Readiness Index 2011, 2012, 2014; regular touchpoint meetings with policymakers

Impact of Data Sovereignty on Cloud Computing; Financial Services Industry and Cloud

Small and Medium Enterprises and the Cloud Computing Market

NEW! Collection, Storage, Use and Query of Data

Cloud Assessment Tool; looking into awarding APAC Cloud Service of the Quarter