NASIG 2017: Daily Wrap Up

Day 2 March 8, 2018

http://nasig2018.northamericansig.org/

twitter.com/nasig2018
#NASIG2018PR

Cybersecurity and Internet Governance

During the first session of the day, we were privileged to have Dr. Milton Mueller present on Cyber Security and Internet Governance. Drawing from his new book *Will the Internet Fragment?* the presentation focused on the discursive dominance of the searches related to cyber security compared to searches for Internet Governance. Currently, the conversation about Internet Governance has been taken over by concerns of the cybersecurity community. Dr. Mueller, argued that this is possibly because since one can take down a country by bringing down cybersecurity systems therefore it becomes much more important.

Dr. Mueller argued that the world of cybersecurity stems from different roots than the world of Internet governance. First, cybersecurity is the security of cyber space. The definition of cyberspace from the US joint chiefs of staff is that cybersecurity is “the collection of all kinds of electronic devices and networked and embedded devices” but this makes cybersecurity sound like a collection of digital communication devices. Dr. Mueller instead argues that it is *connectivity* that transforms these devices into a space- this connectivity is TCP/IP.

The concerns about cybersecurity began to intersect with Internet Governance about 10 years ago. This was described as a two frames problem: an *Internet governance problem* and a *cybersecurity governance problem*.

The Internet governance problem is characterized as coming from a non-state actor-dominated community. It is an environment where state actors and non-state actors are equal and is predominantly concerned with minimizing blockages based on jurisdiction.

The cybersecurity governance problem is characterized as coming from a military governance background. Members of this area see security as a national issue, not as a cyber one. The primary actor was the national government, not the global multistakeholder community.

The distinguishing characteristics of cybersecurity can be categorized as national and social. Cyberspace is divided up into national territories and defended as such. This is true in places like Russia and China, but also in the United States. The unit of security is the nation to the individual user, organization, or collective entity. Since the responsibility lies with the state, a military model is the ideal model for the state, the main threats to security come from other states. Regarding the societal level, security has to be as global as possible, the location of the computer doesn't matter, the emphasis needs to be on the global nature of cybersecurity. The aim is to secure the individual user of the organizations that are a part of cyberspace. Most of the responsibility lies on private actors and the role of the state become one of law enforcement through the prosecuting and deterring bad actors.

What is Internet territory? Dr. Mueller asserts that he has been thinking about autonomous systems, but we are still thinking about Internet territories in 2D ways (think about a map), instead, we need to think about the Internet territory as networked. This territory is comprised of the connections between a variety of nodes which clash with territorial ideology of states.

Fragmentation, or as Dr. Mueller prefers, *alignment*, is when actors are trying to force cyberspace into the boundaries of the territories of the nation-state- “the subjugation of the cyber domain to political jurisdiction.”

There are several methods of alignment that Dr. Muller located within his concept of *alignment*: national securitization, territorialization of information flows, and alignment of critical resources. Finally, he cited some examples of securitization and alignment: Huawei and the US market, Kaspersky and the US market, and the Chinese ban on foreign ownership of cloud services.

In sum, Dr. Mueller argues that information security experts should aim to use the CIA principles - Confidentiality, Integrity, and availability to understand adversaries, vulnerabilities, exploits and threats.

Rapporteur: Anna Loup

Does Internet Governance impact everybody?

Marilyn Cade talked about how Internet Governance impacts everyone. Internet Governance is not an amalgamation of everything coming together in a single place: there is no single path to Internet Governance. She talked about the definition of Internet Governance. The father of the Internet in Africa,, Nii Quaynor was Koffi Annan assistant and so was a great help. It took 1+ years for private sector, civil society, and others to be allowed in the room to discuss internet issues. Only in WSIS were there groups other than governments allowed to play on the same table.

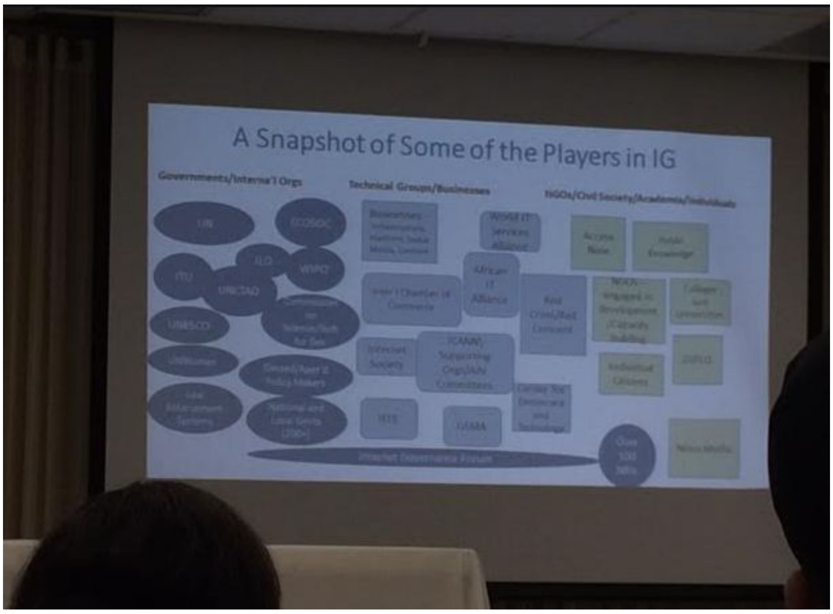
What are the rules affecting

access to information and content and how ICT is impacted.

Internet Governance is an ICT tool to use. Typically business delegates its policy work to trade associations; only large organizations have their own policy departments. Business around the world come to various meetings but what you do not see are the Small and Medium businesses since they are busy running their own companies.

When the IGF was launched, the US government only focused on five to six issues. But now there are many more issues.

Today 300 million women in the world are illiterate. We need to start thinking about what the policies are and why we are not doing things in terms of investment.


A Snapshot of Some of the Players in IG
Governments/Interna'l Orgs
Technical Groups/Businesses
NGOs/Civil Society/Academia/Individuals
UN
ECOSOC
ILO
ITU
WIPO
UNCTAD
UNESCO
Commission on Science/Tech for Dev
African IT Alliance
Access Now
Public Knowledge
Red Cross/Red Crescent
Internet Society
ICANN Supporting Orgs/Adv Committees
NGOs engaged in Development /Capacity building
Colleges and Universities
DIPLO
Individual Citizens
National and Local Govts (200+)
IETF
GSMA
Center for Democracy and Technology
Internet Governance Forum
Over 100 NRIs
News Media

Hardened infrastructure is incredibly important everywhere in the world. Internet Governance is an umbrella term that everyone can work on.

The engagement in expert agencies of the UN, UNESCO, ITU, WIPO. No single space is truly multistakeholder like the IGF The IGF is a model of multi stakeholder engagement.

At ICANN we create binding policies and we also provide a shelter to the interacted parties having to get authorization and approval from government, since if registries and registrars had to get authority in every country ICANN would look totally different . ICANN allows these companies not to have to do this.

Mobile to mobile traffic is growing rapidly. The underlying connectivity that the Internet brings is what brings people together.

NRIs have the ability to actually change policy by inviting and working with government officials and having them come to these national IGF and learn about it and potentially change the government policy.

Using the IGF as an access point to engage with give officials is a very effective tool.

Rapporteur: Judith Hellerstein

Role of US government in the past, present and future governance of the Internet

Ambassador David Gross talked about the birth and the growth of the Internet. US government was involved in almost every piece of it. Originally the Internet was designed to have university and schools and labs connected to it.

1983 IANA was set up by Jon postel. Former VP Gore recognized the internet as something that can change the world.

First generation internet was based on you having a wired internet but in 2000 it was recognized that mobile data and the ability to get on it can change the world. Key to economic prosperity and peace is access to knowledge and by empowering people to gain this access can help them gain this knowledge.

Change and innovations have led to greater growth and stability. US government recognized this early on. US Government tried to explain and explore the opportunities that people can have when they gain access to the net. In other countries they thought this was a danger and fought against it since then they would lose control over their own people as they will gain knowledge

The is a need for ongoing copy creation and local content. Local content is still a great need to us today and having content in local languages. Also ensuring security of the internet. This was a major priority in the US, which was security in terms of privacy and security was what concerned the US government,, however, all the rest of world cared about was ICANN.

Major idea is how to promote national security. Rest of the world wanted to take ICANN out of the US's control and US just fighting to prevent this. In 2005, it seemed that nothing had changed in terms of representation from 2003 WSIS. There was still a limit on number of civil society reps allowed to join the conference.

On the eve of the summit in 2005, the US Government found itself at loggerheads. People were pressing the US Government to agree to giving into the other counties. There was a real push for the US Government to say yes or their was a fear that this head off state event would fail.

Ambassador Gross did not have this fear of failure since his boss, the Secretary of State, was not there. Ambassador Gross said his fear was that he could not go back to the US with a bad deal. As such, he would sooner have a failed summit than go home with a bad deal. So at the last minute some Europeans came up with a solution and discussed it with Ambassador Gross and he signed off on it. This led to the European and others to support the US and at the same time to create the igf. The reason the US government supported this, the creation of the IGF was that the US government had always would be able to do the igf was that they had been on the record stating that we would talk to anyone about the internet.

Originally private sector was upset with Ambassador Gross's decision as they had thought or feared that he had given away control over the Internet. They had not realized that he was just creating a place for everyone to share ideas. They also thought it would be another ITU-like event that would have as its result a negotiated outcome. However, this changed very quickly as people saw the value of the IGF. Ambassador Gross noted that the groups who were the most anti-Internet people are now the greatest supporters of the IGF

Rapporteur: Judith Hellerstein

Content Regulation and Freedom of Expression

In his second session of the day, Dr Milton Mueller started off by examining the historical roots of Freedom of Expression (FoE), which has its origins from the religious conflict of the 17th century that culminated in the separation of Church and State. The concepts of tolerance, natural rights and free will also contributed to the emergence of FoE. The modern concept of FoE is based on the rights of individuals. FoE is believed to be a means of discovering truth, and consequently, also as a necessary condition for fostering democracy.

FoE may be regulated or restricted on the basis of several considerations such as obscenity/indecency, national security, defamation/libel/slander, fraud, intellectual property violation, insider information about the market, hate speech and incitement to conflict are some of these. There is often a continuing tension between Intellectual Property and FoE.

The Internet radically transforms the traditional concept of FoE, as on it, information is available without gatekeepers, transcends jurisdiction, provides anonymity, and erases the boundary lines between multiple media that were traditionally regulated differently, such as newspapers, broadcasts, motion pictures and websites.

There have been efforts, particularly by Governments, to impose jurisdictional controls over the Internet by superimposition of traditional territorial laws on virtual space through blocking, filtering or censorship. This causes fragmentation of the Internet. The alleged reasons for such regulation include child pornography, copyrights, fake news, privacy considerations or subversion. Much of these happen on private platforms such as social media. The degree to which States resort to blocking and filtering varies widely around the world.

There exist technologies that help in circumventing censorship, including VPNs, Tor, Alternative/Dynamic DNS, and initiatives such as Internet Freedom Initiative of the US Govt. Lately, States have been cracking down on the use of these technologies as well.

The degree of responsibility of the technology intermediary vs States has historically varied significantly. Private actors were initially allowed to discriminate based on their own policies on FoE, but this has resulted in a significant amount of regulation. Early solutions to this problem involved rating and labelling (eg., ICRA,V-CHIP) easily identifiable domain names (such as .xxx). However, most of these had issues such as scalability or categorization challenges. Some private content control technologies were partially successful, for instance automatic content classification. However, most of these would not work on a fine-grained level or with rule-based legal frameworks.

Today, content regulation is mostly algorithm-based and run by large social media service providers based on the platform's perceptions of their own liability and existing immunity provisions for publishing third party content. There has been recent concern about the abuse of the immunity provisions (Section 230) for activities such as prostitution and child trafficking. Platform responsibility, whereby the responsibility shifts to private actors for regulation of content, is increasingly becoming an area of debate. The occasional abuse of immunity provisions should not be taken as argument for a more controlled and regulated Internet.

Rapporteur: Satish Babu

Policy Development in ICANN

The second session of the afternoon saw Jonathan Zuck talking to the students about policy development in ICANN. He noted that while there are various policy making bodies, such as government and standards bodies, ICANN's Domain Name System (DNS) DNS policy development processes are unusual because of the large number of people from different industries, backgrounds and regions who are involved.

He gave an overview of the Supporting Organizations (SO) within ICANN, which are charged with developing policy:

- Generic Names Supporting Organization (GNSO)
- Country Code Names Supporting Organisation (ccNSO)
- Address Supporting Organization (ASO)

And he also talked about the Advisory Committees (ACs) that *advise* the ICANN Board on policy matters:

- At-Large Advisory Committee (ALAC)
- Security and Stability Advisory Committee (SSAC)
- Government Advisory Committee (GAC)

GNSO Policy Development
Jonathan participates in the GNSO, and outlined the process that this group uses to formulate policy. Processes in the other SOs may differ:

- The GNSO identifies a problem.
- The Board asks staff to document the problem and conduct some initial research to justify the creation of a Working Group (WG) within the community.
- Once the WG is sanctioned, a call for volunteers is made: anyone may participate.
- A charter is developed. Sometimes, Jonathan noted, the discussion on how to define the problem and its parameters is more difficult than solving the actual problem.
- Then the WG commences its work and reaches out to the rest of the ICANN community as well as industries outside of the community, for feedback on the issue

it is trying to solve.

- The WG issues a policy proposal, which is published for public comment: anyone may give input.
- The WG then takes the feedback into account and develops a final proposal.
- The final proposal is sent to the ICANN Board for review. Sometimes, the Board issues another call for comment.
- Once the Board believes that the policy proposal is final, it will ask the ICANN staff to implement it.

He noted that there are many requests for feedback and plenty of opportunity for input along the way so that everyone has the opportunity to have their voice heard.

There were several questions from the students, including on the issue of conflicts of interest when setting policy, how ICANN is dealing with the UN General Data Protection Ruling (GDPR) and bias within the community.

Jonathan also touched upon ICANN's accountability mechanisms and the Empowered Community, initiatives to make policy development easier for newcomers and periodic participants, the Internet Society's Collaborative Governance Project and data driven policy development: defining metrics for success, how to measure them and making the data more available.

Rapporteur: Susannah Gray

Internet Trust From Students' Perspectives

In the final session of the day, Siranush Vardanyan started off with an exposition of ICANN's Fellowship and NextGen Programmes through a presentation entitled "ICANN and You: The Stakeholder Journey". ICANN, as a multistakeholder entity, provides a platform to project the voices of all stakeholders as inputs to the policy development processes.

The 4-step stakeholder journey in ICANN starts off as a Newcomer, who has multiple resources (such as ICANN Learn) at her disposal. From Newcomer, the stakeholder becomes a Learner, who now has regional resources at her disposal. Next, she becomes a Collaborator wherein programmes such as NextGen and Fellowship are available. Collaborators are able to plan their own events in Internet Governance. Finally, the person graduates as a Leader, occupying leadership positions in different structures within ICANN.

The main programmes available to support ICANN volunteers are Fellowship, NextGen and Newcomer programmes. These are respectively directed at professionals, students and newcomers in general. Fellowship is open to global applicants and typically opens 6 months prior to the ICANN meeting. The NextGen programme is targeted at the particular region where the ICANN meeting will take place. The Newcomer programme is open to all who participate in ICANN meetings (which are themselves open to everyone). All three programmes explain, at different degrees of details, the structure and functions of ICANN and its constituent parts. Fellowship allows participation for three times and have coaches who are experienced Fellows who mentor up to 3 mentees who are first-time Fellows.

ICANN Learn is a learning platform that has numerous online resources (available in 6 languages) that are required for anyone who want to learn about ICANN.

Internet Trust from Students' Perspectives
Three local students participated in the discussion on Internet Trust. Internet resources may be treated by different end-users based on their subjective perceptions. The participants defined trust as the degree of confidence that they could place on a resource based on direct knowledge of the source and their credibility and background. Today, the Internet has substituted print sources and libraries as information sources. It is often difficult to trust sources that are not well-known. Younger generation may have more confidence on Internet resources whereas older generation may blindly accept information.

A survey done in 2013 revealed that some of the issues with Internet sources included spam, abusive email, computer virus, scams such as 'Nigerian fraud', generic emails, excessive bills for Internet. Roughly half of the users did not perceive any difficulty or risk.

A basic precaution that could be taken would be to confirm the source to avoid phishing and identity theft. Many users do not trust payments made on the Internet as they are afraid of losing money. Many users are afraid to trust e-Commerce. The younger generation is generally more confident while using these services. Several risks can be mitigated by taking elementary precautions and building awareness on the risks.

While buying online, quality, reliability and specifications (such as size of clothes) are some of the issues that users face. Reputation of the seller is one way to assess the risk. Users have to exercise significant caution while using resources online (particularly search engines), especially while using unknown services.

Students learn from the classroom & teachers, from colleagues, and from media about trustworthy practices and resources while using online sources. Students also teach other students as well as parents and family members.

NASIG participants thanked the students for their presence as well as for their comments.

Rapporteur: Satish Babu

International Womens Day @ NASIG 2018

BIBLIOTECA
UNIVERSIDAD POLITÉCNICA PUERTO RICO
Profesionales en Práctica.
NASIG
North American School of Internet Governance
.pr
PUERTO RICO
TOP LEVEL DOMAIN
www.domains.pr
EN INTERNET
@DOMAINSPR
@PUNTOPR
@PUNTOPR

Group NASIG 2018 picture