Global Commission
on Internet Governance

ourinternet.org

Meeting of the Research Advisory Network

June 27, 2014

A meeting of the Research Advisory Network convened on June 27, 2014 in Paris, France at the Organisation for Economic Co-operation and Development. The event was held under the Chatham House Rule, which precludes attribution of any specific points to any specific person. The following summarizes the main topics that were discussed at meeting.

Session 1: Scenarios for Internet Fragmentation and Session 2: Building a Research Agenda Examining Internet Fragmentation

- Conceptually, we need to come to a clearer understanding of what fragmentation means.
- By extension, we also need to better understand precisely what non-fragmentation looks like, be it at the infrastructure, logical, content, or policy/legal layer. The technical and legal dimensions are often conflated.
- There is a need to distinguish between a fragmented Internet and one that contains a healthy level of diversity, particularly at the content level.
- Another way of conceptualizing or categorizing the issue is by asking whether a "fragmentation decision" has an impact elsewhere. For example, are there cross-border implications?
- Terminology also matters. The term fragmentation might have an overly negative connotation. Degrees of interoperability or universality might be more analytically precise.
- For the most part, we have a technically interoperable system, but there is Internet fragmentation due to different legal systems, linguistic barriers, systems of content filtering, preferential market access, a lack of system transparency, and the effects of surveillance, which are resulting in moves towards higher levels of data localization and other ad hoc measures.
- The research should be on the trends towards fragmentation, rather than static scenarios.
- In approaching the problem, we should also use threat scenarios that detail particular threats to the Internet and ask: what causes these threats, what is the predicted likelihood of these scenarios, what effects various threats might have, and how to counter these threats.
- More generally, we should adopt a five category analytical model to analyze the issue of fragmentation. The categories include: 1) specifying what fragmentation is as well as what characteristics make for a universal Internet; 2) assessing where we currently have higher levels of universality and higher levels of fragmentation online; 3) specifying at what layer (content, logical, legal, infrastructure) fragmentation is likely to occur within a given scenario;

4) examining both the positives and the negatives of a given fragmentation scenario for various interests; and 5) predicting the causes and effects of fragmentation for each scenario.

- Some recommended scenarios for fragmentation include: 1) regulatory divergence/convergence; 2) the growth or decline of cross-border restrictions on content; 3) changes to institutional systems of Internet governance, including administration of critical Internet resources; 4) the transition to IPv6; 5) interconnection pricing models and potential regulatory changes; 6) net neutrality; 7) and the possibility of alternative domain name systems.
- More generally, the costs of fragmentation could be estimated through a scenario that looks at the expenses associated with re-connecting (regaining interoperability) after having "unplugged" or opted out of universal norms / standards.
- It is also important to distinguish between two notions of time scale. There is the possibility of fragmentation emerging either incrementally over a longer period of time or rapidly through sudden disruptive events.
- More operational definitions of fragmentation could include: 1) reference to antecedents (e.g. the Minitel, AoL) of a pre-Internet interoperability period; 2) fragmentation could be defined as actions that inhibit competition or the openness of the Internet to new players, or actions that limit in an unreasonable way the efficiency of communication; and 3) fragmentation could be any adverse action or deviation from accepted governance principles [OECD's IPPs or the Net Mundial Principles].

Session 3: International Cybersecurity Cooperation and Infrastructure Stability

- Cybersecurity is marked by three main problems: offence dominance, low barriers to entry, and an attribution problem.
- There is a need for greater conceptual clarity about what constitutes an actual cyberattack or criminal activity versus other forms of social action. The Tallinn Manual provides some clarity.
- It is not always apparent who should respond to the need for higher levels of cybersecurity: individuals, companies, states, or some hybrid response. Responses will vary across countries. What are opportunities for international cooperation on cybersecurity?
- When we talk about cybersecurity we should ask who or what we are trying to make secure. Is it security of the content, networks, companies, states, or individuals that is most important? What do we do when there are trade-offs between security for different actors?
- Some of the statistics that form the basis of current understandings of the problem are potentially misleading. It would be helpful to normalize the growth in cyberattacks against the growth in overall Internet traffic.

- To some extent, the decentralized structure of the Internet promotes resilience and improves the security of the system.
- Because cyberattacks are so easy to launch and usually lack a clear kinetic outcome, they can give rise to escalation and retaliation, with uncooperative behaviour generating more uncooperative behaviour.
- Some sort of adjudication mechanism could be used to stop short spirals of escalation.
- Heightening security measures to prevent cyberattacks could also fragment the Internet by breaking it into trusted and untrusted blocks. How can this tension be addressed?
- There are also questions about infrastructure security. How secure are networks, Internet exchange points, and undersea cables?
- There are sometimes security advantages for an institution to operate its own Top Level Domain (TLD).
- There are currently more than 500 Certificate Authorities (CAs), not all of them trustworthy.
- Under DNS-Based Authentication of Named Entities (DANE), only the website and the Domain Name System (DNS) can issue a certificate and it has to be public, which makes it more secure than the current certificate authority system.
- Cyberwarfare tends to undermine the level of trust people have in the system. However, it is not clear whether people lose trust in other people, the Internet as a system, states, or companies.
- There is an incentive problem in the market for zero day vulnerabilities in regard to identification and patching of network weaknesses. When compared to other actors with an interest in mitigating network problems, certain state agencies (like national intelligence services) will pay for knowledge about a vulnerability that they can then potentially exploit. At the same time, other state agencies (like industry ministries) having an interest in correcting vulnerabilities.
- Cyberthreats have ramifications for the global economy, such as creating disincentives for consumers to transact online commerce. Separately, cybersecurity-related issues can affect markets for network equipment manufacturers such as Huawei or Cisco Systems.
- In the area of cybersecurity, the Commission should aim for research on topics requiring higher levels of political attention and that are not already well researched.
- A study of country best practices on cybersecurity could be useful.

Session 4: Building Consensus about Individual Rights

- There is an opportunity to build consensus on how to balance, interpret and apply different rights online.

- More discussion is needed of emergent rights, like the right to be forgotten, and the effects that these newly framed rights will have on the governance of the Internet, access to knowledge, free speech, and media freedom.
- At one level, the right to be forgotten can actually be understood as a new frame for an old contest between the right to privacy and the right to freedom of expression.
- There also needs to be consideration of the rights of minority groups, disenfranchised peoples and children.
- Government, the private sector and civil society each have a role to play in ensuring human rights online.
- It is also not clear to what extent states should be the main guarantors of individual rights and to what extent companies should be allowed to self-police and rely on socially enforced norms of corporate social responsibility in order to protect individual rights. The approaches are largely complementary, but too much of either might generate negative externalities in other sectors.
- One limitation on the protection of rights online is the large number of jurisdictional boundaries across which rights cannot always be enforced.
- Redressing this problem could begin by establishing clubs of cooperation, maybe starting with the "Five Eyes," before moving to all Western democracies, for example.
- Perhaps we need a new, global "Magna Carta" for the Internet.
- One major issue with the protection of rights online involves cases in which they conflict. Freedom of expression rights often conflict with other rights and each state has specific legal provisions in place to indicate what sort of speech is covered by free expression legislation.
- Given the jurisdictional fragmentation that currently exists, there are few effective arbitration mechanisms that can allow individuals to redress rights violations with significant transnational dimensions.
- Technological change can both enhance and undermine rights online. We need to find a way to manage changes to the technology so that rights remain protected.

Session 5: Next Steps for the RAN and Upcoming Schedule

- The next meeting of the GCIG will be held in Seoul, South Korea in October of 2014.
- The RAN will meet during the Internet Governance Forum in Istanbul, but there will also be other meetings, virtual or otherwise.
- An immediate next step will be a paper laying out various modalities of fragmentation, while also unpacking the term, thinking about when fragmentation has salutary or unsalutary effects, and comparatively assessing the universality of the current Internet ecosystem.

- The RAN should contribute a threat analysis paper on potential changes to the Internet governance ecosystem.
- CIGI will commission a poll on levels of trust in the Internet. RAN members who wish to contribute to the development of the survey questions will be invited and encouraged to do so.
- There will be a formal process for commissioning papers. Potential authors will be asked to submit a one-page proposal outlining research questions, methods, the structure and length of the proposed paper, and a brief abstract. Payment will be made upon delivery.
- RAN members will be encouraged to provide informal peer review of submitted papers.
- The papers will be published on the GCIG website.
- The papers will inform the work of the Commissioners.

NOTE: SUBSEQUENT TO THE MEETING

Based on discussions at the RAN meeting the following papers have been commissioned to support the plans for fragmentation research.

- *A Model for Understanding and Assessing Types of Internet Fragmentation*
- *Implications of the Resurgence of Proprietary Technical Protocols*
- *The Economic Costs of Data Localization Policies: A Case Study of the Financial Sector*
- *The Economic Costs of Global Internet Fragmentation*
- *Legal Interoperability as a Fragmentation Combating Tool*