Panel 2: Alternative Modes and Challenges Posed by States to Western Governance

Nigel Inkster, chair and rapporteur; Pano Yannakogeorgos, co-chair
Chris Bronk, Tim Maurer, James Mulvenon, Rafal Rohozinski

The current model of multi-stakeholder Internet governance is coming under challenge from many directions. The aim of this panel is to examine the attitudes of key stakeholders to the status quo; analyse the motives of those seeking change; consider the implications of alternative governance proposals; and examine whether a more appealing narrative can be developed to support the status quo or something close to it.

Below are the framing questions for the panel:

1. What are the key elements of Russian and Chinese policies on Internet governance and what are the drivers for these policies? How congruent are they?

2. Assuming there is broad congruence on a common set of objectives, how will these states pursue their aims? What are the strengths and weaknesses of their position(s)?

3. How would an Internet governed under this model operate and what would be the strategic implications for the West if such a model were to prevail?

4. Can we talk of a common "G77" position on Internet governance and if so what are its main constituents?

5. Are the drivers for G77 approaches political, economic or a combination of both? Can the status quo be modified to address their concerns and if so, how?

6. Can the USA and the "like-minded" construct a positive narrative for the multi-stakeholder governance model - or is it condemned to fight a war of attrition?

7. To what extent can the norms of a decentralised multi-stakeholder model of Internet governance be extended to the emerging Internet of IPv6 and the Internet of things?

Summary

The impending World Conference on International Telecommunications (WCIT) is emblematic of an ideological divide between - predominantly western - nations espousing the current multi-stakeholder model of Internet governance and those favouring a government-led governance structure under the United Nations. Chief amongst the latter are Russia and China both of which have a particular interest in securing international validation of their aspirations to control Internet content. Many so-called G77 states remain uncommitted but are to varying degrees suspicious of a governance model perceived as benefitting and entrenching the interests of the US and its allies and attracted by the prospect of exercising greater control over a phenomenon hitherto seen as disempowering. The ideological dividing lines are however blurred by the interests of a range of actors including national telecommunications companies seeking to restore revenue streams lost as a result of the move from circuit to packet switching.

Russia has taken a prominent position in arguing the case for Information Security through the promotion of a Code of Conduct and proposals for cyber warfare to be made subject to an arms control treaty. Russia's position is rooted in its immediate post-Soviet experience when Russian telecommunications were effectively colonised by foreign interests. In the mid-1990s Russia's security services launched a fight-back and the same cadres in Russia's security apparatus – FAPSI/FSB, Interior Ministry, Defence Ministry, National Security Council and think-tanks close to Russia's security constituency– have had the lead role in efforts to re-territorialise Russia's telecommunications and Internet services ever since, with the MFA as a relatively recent addition. Russia's overwhelming objective is to recover control of its own "information space" and to exercise effective control in a sphere of influence encompassing the former Soviet states. Its aspirations are to have an internationally acknowledged right to filter content; to establish jurisdictional boundaries within cyberspace; to have predictability in managing international security issues within the cyber domain; and to develop sufficient capacities to be able to constrain key competitors within that domain. It is the ends that matter: Russia will pursue these by whatever means can help it gain traction on the issue and hence will not be wedded to any one approach.

China has exploited its relatively late entry into the cyber domain to leapfrog the West and avoid repeating many of the latter's mistakes. Singapore in particular has served as a source of advice for the Chinese leadership on how to combine economic modernisation with political control. China's rapid adoption of the Internet has been accompanied by a sophisticated suite of techniques for monitoring and controlling Internet activities and Internet content while creating the impression of a lively and unconstrained cyber environment and ensuring that China remains connected to global cyberspace to facilitate continued economic development. China makes much play with the term "informatisation" – 信息化- the significance of which is not well understood in the West. "Informatisation" needs to be seen as the use of ICT to act as a force-multiplier across the full spectrum of state activities and hence has a much wider strategic significance than is generally appreciated; it is emblematic of a whole-of-state approach. China shares Russian thinking on information sovereignty – exercising control of information within its own borders. But China's thinking goes further, to include the right to attack hostile information outside its own borders that has the capacity to jeopardise internal stability. Organisationally China wishes to see Internet governance move from ICANN, which it sees as a vehicle for US Internet hegemony, to the ITU. Its long-term strategy is to shape the international information environment by increasing dominance of various Internet standards bodies such as the IETF and W3C and the exploitation of its dominant position in global mobile telephony manufacture.

The G77 grouping is far from homogenous and comprises a wide range of outlooks, priorities and levels of technical and political sophistication. Key swing states are likely to be India, Brazil and Iran, the latter in its capacity as animateur for the recent NAM revival. It should not be forgotten than for these states WCIT represents just the latest battle in a war that has been waged since the late 1990s over Internet governance. Since then there have been significant developments in the fields of politics, security and economics which will affect the debate. Politically the aspirations of the developing world to have greater participation in the debate have been frustrated due to the logistical and financial difficulties of participating in the meetings of bodies such as the Internet Engineering Task Force (IETF) though such concerns are now starting to be addressed. Cyber security and the militarisation of the Internet are also contentious areas not least due to developments like Stuxnet and are a factor for politicisation within the ITU as evidenced by the latter's engagement with Kaspersky Labs.

But it is the economic dimension that may most affect the attitudes of G77 states – and for proponents of the multi-stakeholder model, Internet prosperity may prove a more effective rallying-cry than the current emphasis on Internet freedom. Such an approach would need to be more mindful of the economic losses suffered by many states as a result of a move from circuit switching to VOIP. Arguments that the loss of direct revenues to governments can be more than compensated for by the longer-term benefits to be expected from an expansion of Web-based services may be valid but are unlikely to resonate with corrupt officials. And the economic case needs to be considered within the context of calls, including from European network operators, for a redistribution of revenue from content service providers to carriers based on the principle that the "sending network pays" to reflect the fact that a few services such as video streaming take up disproportionate amounts of bandwidth. In effect the debate turns on whether ISPs should be seen as the providers of public goods available to all or whether some form of toll system reflecting actual levels of usage is more appropriate.

ICANN may be facing a crisis of legitimacy. The memorandum of understanding between ICANN and the Department of Commerce elicits widespread distrust, though there is little that countries can currently do to wrest control of ICANN from the US without disrupting the entire functioning of the Internet. A possible option for ICANN to bolster its legitimacy might be via a unilateral Declaration of Independence from any government.

Further considerations affecting the debate over Internet governance are the roll-out of IPv6 as IPv4 addresses are running out, a phenomenon energetically promoted by states such as Russia and China and attractive to any state wishing to register domain names in non-Roman scripts. Over time the roll-out of IPv6 could result in the Regional Internet Registries (RIRs) maintained by the IANA (Internet Assigned Numbers Authority), via agreement with ICANN/IANA, becoming progressively side-lined, while an alternative de facto model of domain name governance takes hold. A suggested course of action to preserve the current multi-stakeholder arrangements of Internet governance in the face of this challenge is that IANA allocate IPv6 blocks to the ITU, which could then serve as an RIR itself and allocate new address space to Country Internet Registries (CIR). This procedure would enable market forces to determine whether the ITU is capable of serving as an RIR.

Developments within the domain name system comprise another relevant factor for governance. These developments include multilingual domain names, generic top-level domain names, and alternate Domain Name Systems at the country level. They could catalyze the so-called "balkanization" of the Internet as they introduce more localized functionality. Similarly the emergence of the Internet of Things (IoT) –machines communicating directly without human intervention – is empowering for those seeking alternative modes of governance. It has already stirred debates on privacy and other issues related to object naming: which authorities will be responsible for assigning the identifier; ways to find information about the object; how information security is ensured; ethical and legal framework of IoT control mechanisms. Although these issues have not received great exposure within the USA, they are already subjects of working groups in the EU and China – a development which runs counter to the bottom-up model characterizing Internet governance to date.   Thus, the USA and its allies should be wary of winning the battle over IPv4 and ICANN whilst losing the actual war.

Conclusions

The global landscape for ICT seems to be undergoing a process of fragmentation. Call it balkanisation, border controls or walled gardens, the Internet is becoming subject to greater levels of territorialisation. Increasingly states are allowing local carriers to provide content free of charge, and since most users' interests are local, they have little incentive to stray outside the walled garden especially if doing so incurs financial costs. And whatever their positions of principle, all states are practising some degree of content control. Moreover wider changes in the landscape – demography, domain-name governance and increasing automation –are accelerating the shift in the nature of the Internet we have come to know.

The debate over Internet governance is a function of different perceptions of global governance more generally. States such as Russia and China, with fundamentally different world views and imbued with the conviction that the tide of global affairs is moving in their direction, are unlikely to be persuaded away from the stances outlined in the preceding text. At the same time, there is not a total identity of view between Russia and China and efforts should be made to explore and exploit such divergences of positions as can be identified. The key focus however has to be on what for want of a better term have been called the G77 states. If the exponents of the multi-stakeholder model want to carry this constituency - or rather win over constituencies within it that share common interests - they will have to be more ready to acknowledge and address the shortcomings of the current model and in particular take active steps to ensure that its inherent economic and political inequalities are redressed; develop a more nuanced narrative which does not just focus on Internet freedom as an unchallenged good; and address honestly and be willing to take steps to mitigate threats arising out of the militarisation of the Internet. Above all, exponents of the multi-stakeholder model have to look beyond single events such as WCIT and single organisations such as ITU and recognise that this is a campaign needing to be pursued on all fronts at all times.

For citation: N. Inkster, rapporteur, Summary for Panel 2: Alternative Modes and Challenges Posed by States to Western Governance. Cyber Norms Workshop 2.0, Sept., 2012. http://citizenlab.org/cybernorms2012/