The Continuing Struggle for Control of Cyberspace—And The Deterioration of Western Influence

By Paul Rosenzweig Monday, January 13, 2014 at 7:00 AM

Who will run cyberspace? It's one of the most important questions in the world today. Yet few outside a narrow group of policy wonks, lawyers, technologists, and international bureaucrats are paying attention to the question—much less the answer.

This post is intended to explain the issue in a bit of detail. I've come, lately, to the conclusion that this is one of the most significant questions facing the development of cyberspace in the coming few years. The answer we choose to the question of governance will, in the end, affect the whole world. Today, the globe-spanning reach of cyberspace touches the lives of more than 2.5 billion people. The so-called "Internet of Things" controls more than 1 trillion devices—everything ranging from cars and houses to industrial plants, elevators and even medical devices. Every day (in 2012) we created roughly 2.5 quintillion bytes of data (that's a 1 followed by 18 zeros). Put another way, 90% of the data created since the dawn of human history was created (and passed through cyberspace) in the last two years. As a world community our dependence upon and interdependence with the cyber domain is growing so fast that our conception of its size can't keep up with the reality of it. How we govern this distributed and dynamic space is profoundly important to the future prosperity of humankind.

And that's why it is so troubling that some, in a rush to "internationalize" the governance of the internet, are rushing to change the current structure. The system we have in place, imperfect as it is, has been, by any measure, successful in creating the opportunity for economic growth and intellectual freedom. Yet some are not content to leave well-enough alone. In my judgment the changes proposed would be mistakes of grave consequence.

What I hope to do in this post is three interrelated things: 1) Explain in summary fashion what the current internet governance structure is; 2) Describe the proposed changes, broadly speaking and why they matter; and 3) Outline some of the developments that we can anticipate in the next 12-24 months. In the end, the most disturbing part of the analysis is that US leadership is lacking – partially as a result of Snowdenitis, but also because of a lack of attention.

Where We Are Today — The current governance structure of cyberspace grew up over time – almost accidentally. The operation of the network has been defined by two organizations – the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN). Taken together the two organizations both set the technical protocols and standards for operation of the network and manage the assignment of names in the cyberspace addressing directory – known as the domain name system. Over the years they have proven to be relatively (though not, of course, completely) non-partisan and professional, typically operating by consensus. But some around the world think that their policy making is highly influenced by the nations that are most technologically reliant on the internet and have contributed the most to its development and growth – nations like the United States and other Western democracies. Others have the opposite concern – that their own governments don't have a veto power over ICANN decisions.

One consequence of that influence is that the decisions of the IETF and ICAAN lean, somewhat, in the direction of libertarian freedom – there is a strong predilection to reduce interference in the operation of the network to the minimum necessary for ordered liberty. There is, for example, a great reluctance to use internet protocols as a way of monitoring or managing content because doing so smacks of an infringement on civil liberties.

One particularly good example of this mindset is the changing view of encryption in the IETF. Several years ago many countries asked the IETF to incorporate an encryption standard in the Internet Protocols. The IETF declined since, inevitably, encryption makes the entire network marginally less efficient. Today, however, in the wake of the NSA/Snowden disclosures, the IETF has begun to reconsider that view point – not because of a change in the engineering but rather as a modest pro-freedom evolution of network protocols. The effort is just beginning, and only time will tell if it comes to fruition, but it is emblematic of the nature of the "multi-stakeholder model" (MSM) for management of the network.

Complaints and Criticisms — Some non-Western international participants characterize this structure and Western-oriented influence as a form of American cultural imperialism. And to be fair, they do have a point. From the perspective of an authoritarian country "internet freedom" is just code for "disruption of the status quo." And we, in the West, likewise tend to be what Evgeny Morozov calls "cyber-utopians." We really do believe in the power of free expression to change political and economic environments and our not-so-covert objective in supporting internet freedom is to spread Western memes of democracy and capitalism.

As a result the non-Western countries want a different entity to manage the domain – and the one they've chosen is the

International Telecommunications Union (the ITU dates back to 1865 but is now a part of the UN). They argue that transferring authority to govern cyberspace to the ITU (or a similar international treaty organization) is a means of converting the "control" of the Internet into a conventional international process that dismantles the current position of global dominance of U.S. and Western national interests. [As an aside, the concern rests on a false conception of "control" – there really is no central authority controlling the network – but that, too, is what some want to change.] In the ITU, like most UN institutions, a "one nation/one vote" rule applies – a prospect that would certainly change the MSM of cyberspace governance, with results that are unpredictable, but inevitably will have influence on the current model of internet business processes, which rely on a universal, global, united market, using invariant standards, protocols and parameters.

Supporters argue that giving the ITU a role in Internet governance is no different from the role that the World Customs Organization has in setting shipping standards, or the International Civil Aviation Organization has in setting aviation traffic rules. Others are less concerned with the regulatory function than the fiscal one – the shift away from traditional telephony has impacted the revenue stream of many nations and an exercise of ITU jurisdiction is thought to be likely to restore some of the lost resources for many nations.

Events in Dubai – Against that backdrop, the ITU sponsored a meeting – the World Conference on International Telecommunications (WCIT) – in Dubai in December 2012. The meeting was, in many ways, a confused harbinger of things to come. Western nations tried to protect the status quo of a multi-stakeholder approach to internet governance, while more authoritarian countries, led by Russia, China, Saudi Arabia, and Iran sought to amend the International Telecommunications

Regulations (ITRs) and make them a legal ground for control over internet content. [The ITRs have, for some time, been the principally technical standards that are the main product of the ITU – addressing things like frequency assignment and the like.]

In the end, the US won some points at the Dubai meeting. At its insistence, the revised ITRs contained no mention of the word "Internet" and the Preamble was amended to require nations adopting the ITRs to do so in a manner "that respects and upholds their human rights obligations."

Two results point however, to some greater conflict over internet management and, in my judgment, bode ill for the future of internet governance. First, there was inclusion in the ITRs of a draft regulation directed at spam. It is, I think, emblematic why authoritarian countries want to regulate political expression are so enamored of ITU governance — they seek an international standard that allows each nation to manage its domestic internet however it pleases (in effect, giving international law approval to domestic internet content limitation).

Now, nobody likes spam (except, obviously, the spammers). But it ought to go without saying that a mandate to end spam can only be implemented by reviewing the *content* of all email messages. After all, spam is in the eye of the receiver and that perspective requires knowing what the message says. So, though the eventual course of development for this particular regulation is uncertain, it seems likely that it will be taken as a license to monitor content by national governments.

The second anti-freedom result was an odd and procedurally suspect resolution proposed by Iran. It read that "To foster an enabling environment for the greater growth of the Internet, . . . "all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability,

security and continuity of the existing Internet and its future development and of the future Internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized." This was, in effect, an effort to reassert the role of sovereigns in making internet policy.

For both these reasons, the ITRs proved not to be the product of a unanimous consensus. The vote was 89 in favor and 55 against. Those objecting to the ITRs included many of the Western nations — the US, the EU, Australia, Canada, Japan, and others. As with most international agreements, the ITRs must be ratified by individual nations; can be subject to reservations; and then must be implemented by domestic law. The ITRs will take effect on January 1, 2015 – and they will only bind nations that ratified them.

Does It Matter? – So does it matter at all? Some think that advisory international regulations that are non-binding should be of little moment or concern to the objecting nations. On reflection, however, I think that doesn't give the ITR's due credit for importance.

Indeed, with all due respect, those who want to transfer regulatory authority over the cyber domain to the ITU or who are unconcerned about that possibility are making a mistake of significant proportions. At best, such a transfer would diminish internet freedom. At worst, it might fracture the network altogether, breaking the universality of the interconnected cyber domain.

First, and most narrowly, the analogy to commercial international organizations is a false one. Aviation communications frequency requirements and standard shipping container sizes are not fraught with political significance in the same way that the regulation of cyberspace has become. International institutions like ICAO and

the WCO succeed precisely because they manage the mundane, technical aspects of a highly specialized industry. And when they do face more substantive concerns, their culture of consensus and cooperation suffices to smooth over most disputes. By contrast, regulation of the network brings with it a host of highly contextual, political questions – perhaps no questions are more fundamental and more controversial that those which challenge basic state authority. Many, therefore, fear that sovereigns seek international control of the network precisely because they want to stifle dissent and choke off the new medium of communication that has made maintaining the status quo hard.

Second, those who are not concerned underestimate, I think, the norm-setting value of international law. To be sure, the ITRs don't take effect of their own accord – they require ratification and implementation. And if we dissent from their content they won't bind America. But it is a very different world where authoritarian countries can ground their repressive actions in an appeal to international law – one where Western interests in freedom of politics and economy will hold less sway. Put bluntly, it matters in the court of public opinion if China can say "we are just implementing international law."

And so some countries, concerned with outside influences, build firewalls to filter content. Middle Eastern countries have proposed the construction of a separate Halal network intended to keep out non-Muslim influences. And, in Belarus, "all visitors of Internet cafes and other public places of Internet access have been obliged to provide passports or other documents identifying [the] person in order to use the Internet." Indeed, the instinct to filter content is not limited to authoritarian régimes — even liberal Western countries like Australia have proposed restrictions on Internet traffic, albeit for facially more legitimate reasons, such as limiting the spread of child pornography. While these efforts proceed apace even in the absence of international authority, imagine how much more robust

these efforts might be if they had the imprimatur of UN approval.

Third, and even more fundamentally, we should systematically prefer governance by ICANN and the IETF over that of the ITU for reasons beyond questions of national interest. We should do so because it makes good economic sense. The world economy and humanity's overall general welfare would be better served by ICANN's adherence (albeit imperfect) to a deregulated, market-driven approach to the development of cyberspace. This approach compares favorably to the turgid, ineffective process of the international public regulatory sector. If you consider that American or European processes are slow, you must realize that the problem will only be magnified in the international sphere.

Recall, again, the size and scope of the network. Given the scale of the enterprise, the mechanisms for multinational cooperation are too cumbersome, hierarchical and slow to be of much use in the development of international standards. Acceptable behavior in cyberspace mutates across multiple dimensions at a pace that far outstrips the speed of the policy making apparatus in the public international system (which, to cite just one example, has yet to conclude an updated trade treaty despite nearly two decades of effort). We should all be concerned that there is no surer way to kill the economic value of the cyber domain than to let the public international community run it.

And, finally, the efforts at WCIT are I think a harbinger of things to come. It is difficult to make predictions, but (as I'll discuss in more detail in the next section) the morphing of the ITU is an ongoing process. The next major meeting is in Busan, South Korea in 2014 and there we might see an even greater push for more direct control of network protocols (or perhaps not). In my view, the only thing about the proposed transition of governance to the ITU that is certain is that it increases the risk of polarizing an already contentious domain even further. We have seen the

rumblings of what state-control of the network look like already, and the vision is not a pretty one.

What Lies Ahead – So, what's next in this domain? As I just noted, the ITU's next plenipotentiary meeting will be in South Korea from late October to early November 2014. Two events are on the horizon for that meeting.

First, some are talking about amending the Constitution of the ITU. Doing so requires a two-thirds majority. The current proposals range from an ITU "oversight" council to replacement of ICANN with ITU governing structures. The later prospect, in particular, would be chilling and could result, in the end, on the amendment of technical Internet Protocols and naming rules to foster sovereign control of the network. No drafts have yet been produced – and the Constitution requires that they be published by April. At that point we may see exactly what steps might be proposed.

Bottom line: The decision of some countries to not accede to the Dubai ITRs has already raised the possibility of degrading the interoperability of the network globally. Revisions to the IP creation process or the DNS naming system might accelerate that degradation (since Western nations are also unlikely to follow authoritarian IPs) and accelerate the move toward the possibility of a "splinternet."

Still, amending the Constitution would be hard. If we take the 89-55 vote in Dubai as a baseline then those who would change the ITU's Constitution to mandate internet governance were short of the necessary majority in 2012 – but perhaps not any longer. For one thing, there were many members who did not cast a ballot in Dubai – total ITU membership is 193 countries, so 55 is already fewer than the 1/3 blocking minority necessary. More to the point, however, those 55 votes have likely eroded since Dubai – thanks to

Edward Snowden.

The Snowden revelations of NSA activity are troubling on a number of levels. But the most disturbing aspect is that he has revealed that some parts of the US government are insufficiently cognizant of their broader responsibility to network governance. Any fair assessment suggests that the US government has been a reasonable custodian of cyberspace freedom and governance, fostering the conditions that have fueled the domain's explosive growth. Yet Snowden's disclosures make clear that some in American have sought to take advantage of that custodial position, thereby strengthening the argument of those who would seek to change the structure of Internet governance.

In other words it is by no means clear that those 55 votes are still in the US camp. Many, including some of our closer EU allies, may be ready for a radical change in internet governance. And as I've noted already, I think that sort of change would be a significant error – and the irony of Snowden's actions is that they may have the unintended consequence of hastening the diminution of Internet freedom rather than arresting its erosion.

The second development is even more of a sleeper. At the Busan meeting, the ITU will elect a new Secretary-General. The incumbent, Dr. Hamdan Toure of Mali, is term-limited. As of today, there is only one announced candidate for the position. He brings to his candidacy a great deal of experience, including, most recently as Deputy to Dr. Toure in the ITU. While such internal promotion is laudable, I will be forgiven if I express a small amount of concern – the candidate is Dr. Houlin Zhao of China. Thus, one plausible scenario would be for 2015 to see a newly empowered ITU dealing with international internet public policy issues, and perhaps even asserting authority to create internet technical standards, under the direction of Dr. Zhao.

One final note: The US is not really paying attention. Again, as of today we have yet to name an ambassadorial rank leader for the US delegation. And, frankly, I don't think that the Executive Branch has as great a concern about these events as I do. There is a crying need, however, for greater US engagement – notwithstanding the Snowden fall out. More importantly, the US private sector needs to recognize that the lack of a strong US governmental presence is doing them harm – they need to quickly and decisively collectivize their efforts if they are going to avert potentially adverse results.

* * * * *

There is a real intellectual appeal to the idea of an international governance system to manage an international entity like cyberspace. But, upon closer examination the idea is fraught with peril. What is needed now is a reinvigoration of the existing multi-stakeholder structure combined with bilateral and multilateral agreements on narrow issues of general applicability. Those who support the MSM and ICAAN/IETF structure must acknowledge the dislocation that diminished revenue is having on some nations that are dependent on telecommunications taxes for a portion of their budget and, where possible, propose mechanisms to ameliorate the adverse effects.

More importantly, we should strive to instill confidence in ICAAN and the IETF as stewards of cyberspace. It may, for example, be necessary to further decouple those institutions from Western influence. But even after the Snowden disclosures we must also recognize that the non-State structure currently in place is *less* subject to political manipulation than the alternatives. These international institutions are multi-stakeholder groups where individuals, technologists, political organizations, innovators and commercial entities all have a voice. The product of their consensus is more representative and more moderated than any system respondent to only sovereign interests can hope to be.

The way forward for the United States and other Western nations is to make common cause with allies and friends around the globe to establish cooperative mechanisms that yield strong standards of conduct while assuring the continuity of critical cyber freedoms against the challenge of authoritarian sovereigns.