ICANN Studienkreis Budapest, Hungary 28-29 April 2011 Peter H. Hellmonds

Thank you, Yrjö.

Ladies and Gentlemen, dear friends.

It is a pleasure for me to be here today in this great and wonderful city of Budapest and to be speaking to you and discussing with you the various visions for the future that are looming on the horizon as quite concrete manifestations of current trends, extrapolated into the future up to 2020.

When I asked you, Yrjö, about how you wanted to run this session, you answered that this session today "is going to be a general 'crystal ball' session." You continued to outline that you wanted to discuss the dimensions of technology, governance, applications and content. When we discussed the session then yesterday on the boat, you clarified this and you said you wanted to move from the technology by way of looking at the alternative scenarios to the governance issues deriving from them, and then look at the real life implications, such as the chance to help creating and sustaining democracy movements in the world by ways of ICTs.

Now, since my company, Nokia Siemens Networks, is paying me to be here, I should be permitted to use the industry knowledge and vision that was developed in my company for the development of the technology in communication networks and the commercial dynamics going on there. I will use that as a starting point for the technology section of this session.

Technology

From a technology perspective, my view is that we see three basic trends that have started already today and will continue to shape the technology landscape of the future:

a) the proliferation of smart devices will continue

b) the access networks and their usage will be a lot more mobile

c) access, backhaul and aggregation as well as core network components will all be based on the Internet Protocol

d) the applications and real-time content are going to be hosted more and more in the cloud

e) the network experience will become ever more personal to the individual user, who will carry his Internet device in his pocket and access and upload in real time via social networks

f) communications will become even more ubiquitous with the integration of communications into the fabric of other industries, thus forcing the switch-over to IPv6 as IPv4 number space has run out

g) bandwidth demand is continuing to increase, especially with the growing demand for video, which is expected to represent more than half of all traffic by 2020, up from one quarter today

h) and we will continue to see ever more convergence of phone, data, media and other uses of the network around the concept of a unified network, which we call the Network of One

i) finally, I predict that telephony will become a mere app on the new smart devices and our today's Telcos are in dire need to transform if they do not want to go down history alley.

For us as a technology company supplying the networks to the myriad of operators around the world, the challenge is of course to provide our corporate operator customers with the tools to manage this kind of network so that the end user experience can be enhanced. So, the things our technology experts are doing are centered around simplifying the network with network optimization, new fixed and mobile access technologies and converged and simplified network architectures. They are also optimizing the service delivery, focussing on a converged, IP-based service infrastructure for voice and data services. And finally we are transforming the operational and management capabilities of our customers.

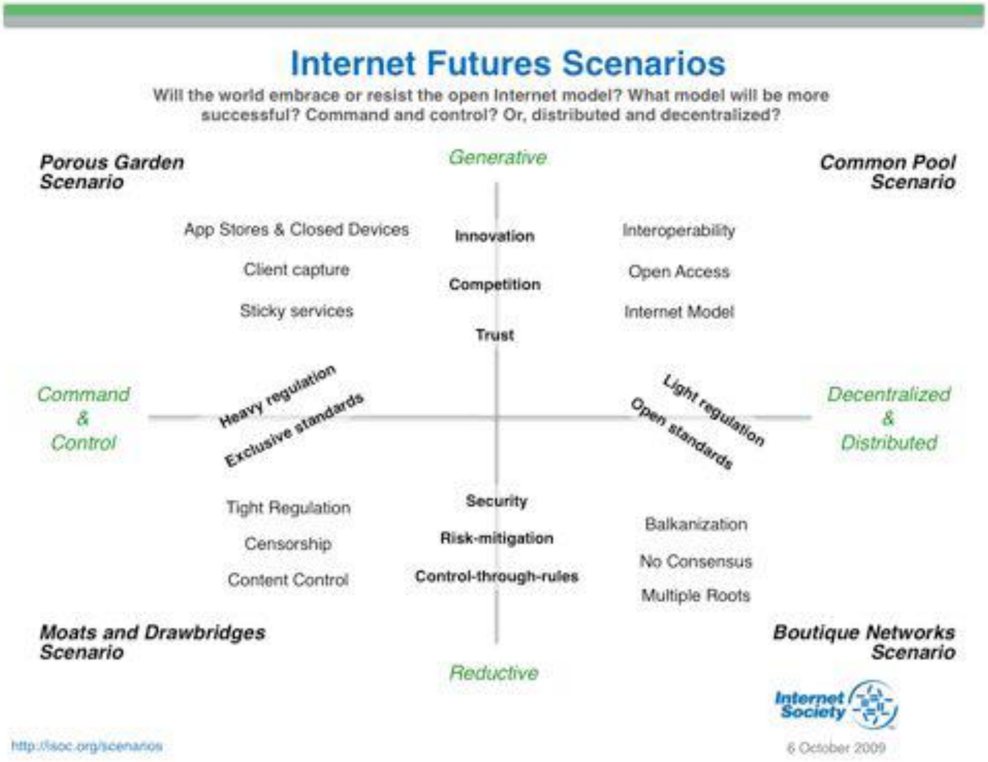
Now, I could go into the details of these, but for the sake of time, I would rather like to concentrate on more are the scenarios for a possible future that derive from underlying currents and streams of actions and activities of players in this technology landscape. Because I am at heart not a technology expert, but someone interested in the social and political dimension of the net.

Alternative Scenarios

A good starting point for this discussion could be the report published by ISOC in 2009, where they presented the outcome of a scenario planning exercise, looking at possible futures of the Internet on two axes:

- first, will the world embrace or resists the open Internet model?
- second, will there be a command and control model or a distributed and decentralized model as we know it today?

The result was something depicted in four quadrants divided by these axes, resulting in four distinct scenario models, i.e.



I will not comment too much on this graph, other than saying that I do not see these models as mutually exclusive. What I see is that a number of these models are already co-existing at the current time. We know that in certain countries, under certain regimes, there is already a heavily regulated and censored Internet, as described in the lower left quadrant. Some companies try to tie their customers closely to their own branded app stores etc, so that would be the top left quadrant. There are also already some people running separate root server systems, which would be a sign of the bottom right quadrant, whereas the Internet that most of us here have come to appreciate is the common pool Internet we can see in the top right quadrant.

What I want to say is that we may need to look at multiple scenarios taking place at the same time, using the same underlying Internet infrastructure, coexisting, but not necessarily completely interlinked without disruptions. For me, the most likely scenarios that are looming on the horizon are the following:

a) a Cyber Mafia network, operating in the underground, coexisting and interacting at certain points with the existing Internet, but also keeping certain aspects secret and hidden. This vision of a scenario, I must admit, is being influenced by one of my favorite novels, the 1984 Neuromancer novel by William Gibson, where he popularized the term Cyberspace (coined by him in Burning Chrome two years earlier), and where he outlined a vision of organized crime, operating in the Matrix, hiring Cyberpunks to do their hacking work for them.
While we know already of Botnets that can be purchased for various nefarious ends such as DDOS attacks or mass spam mailings, I can easily envision that organized crime will use or is using sophisticated technology means to operate their global network, and to attack corporations for either stripping them of their assets or user data or for simple blackmail.

b) a Cyber Warfare scenario is also highly likely. If you look up the term Cyber Warfare at Wikipedia, you see a number of issues mentioned there such as cyber espionage and sabotage against civil, commercial and also against government and military targets, including electric power grids, banking networks, communication infrastructures, etc.
Next to the Cyber Mafia mentioned above, there are a number of states who are actively developing either defensive or offensive cyber warfare capabilities, and there is already a history of several cyber warfare activities against other states, such as the Estonian DDOS attacks of 2007, the 2008 South Ossetian war, where Russian, South Ossetian, Georgian and Azerbaijani sites were attacked. In 2009 there were attacks against South Korean sites and in 2010 the Stuxnet worm targeted Iranian capabilities, to name just a few well-known ones. As a response, the US is introducing the Kill Switch Bill, and in Europe there are activities to create Cyber Defense Systems.

c) Another possibility is that around the Internet of Things there could develop a number of proprietary networks for logistics handling, and for a myriad of other applications. When every item produced could potentially receive its own IPv6 address, there is no indication that not certain industries would prefer to keep their corporate data protected from the rest of the Internet. Similarly, it is quite conceivable that banking networks such as SWIFT or similar could opt out of connecting to the general Internet, yet still be using the Internet Protocol suites. These could be run either as Intranets, with some interconnection points to the Internet, or it is conceivable that certain sectors chose to keep a strict separation, for example the electrical grid companies may opt to protect their critical infrastructure by not connecting to the Internet, but to keep the electrical grid in a separate logical loop.

d) So, what I can envision is a multitude of Internet networks, coexisting, either interconnecting or not, but still using the IP-based protocols. If we would see a lot more Cyber Crime and Cyber Warfare, I could envision that the command and control scenario outlined by ISOC could become a much more logical option. However, if such a controlled network would become the norm, I can easily envision a counter culture developing a free and open network initiative, creating in effect a separate network that tries to evade the government-ordered controls. If the root is controlled by governments, cyber activists would simply install a separate, alternative root, circumventing the controls and creating a global, free Internet.

Governance Issues

In my scenario, I have outlined that I can easily envision a number of parallel Internets, even with multiple roots, coexisting next to each other.

What are the governance issues here? Each network would likely run its own governance. The Cyber Mafia bosses will determine the rules to govern their networks. The Cyber Czars in the various defense ministries of states will try to install their command and control structures and Cyber Activists around the world will try to find ways and means to establish bottoms up rules to make sure the Open and Free Internet will continue to function. So, for me, the most likely scenario is that of a balkanized Internet.

We will probably all look back at the current time and wonder why we all got so hooked up about the triviality of DNS lookups and ICANN’s interrelationships between Board, GAC and GNSO.

(let’s discuss)

Real Life Implications

Democratic uprisings and revolutions in Tunisia, Egypt, Libya, Bahrain, Yemen, and Syria show the power of communication technologies to help shape events. Autocratic rulers have attempted – mostly in vain – to shut down those communication means, only to find that the cyber-activist community has been fast in innovation, helping to circumvent restrictions by alternative means, such as the voice-to-text transcription service etc.

(let’s discuss)