**Internet Politics and Politics in the Internet 26.8.2013**

The Internet is moving to a centre stage in terms of future media and even international politics. The development of the Internet itself is mired in politics. Let's take a look at the most notable recent developments in the scope, technology and politics on the Internet.

Over the past 2 years, the number of mobile broadband subscriptions has grown from about 1B to 2 billion. The number of individuals using the Internet is now estimated by ITU-T to be 2.75 billion. A great majority are using wireless access while the growth of fixed broadband is saturating at about 700M. The growth of mobile is significant because the Internet was really designed for mains powered desktops and fixed access connections. Now most hosts are battery powered and mobile. This calls for a re-evaluation of many requirements and design choices of the technology.

Related to the growth of the number of users, the unallocated address space in IPv4 has been exhausted in Asia-Pacific and the developed world. IPv6, designed by the Internet Engineering Task Force, is promoted as the successor to IPv4. In 2011-12, we have seen the IPv6 day and the IPv6 launch. IPv6 deployment requires that every router, every server and every client computer will be upgraded to support Ipv4 and Ipv6 in parallel. However, still today, incentives to deployment are missing and therefore little is happening. Users and corporations that need the Internet already have IPv4 addresses and see little point in investing for the sake of new users who they do not expect to communicate with anyway. A critical point is that although we have working methods for deploying IPv6 in client machines, all servers still need IPv4 to be reachable from legacy IPv4 client machines. Therefore, there are no economic reasons for deploying IPv6 in servers that should be reachable to all Internet users. Consequently, why deploy IPv6 clients, if all servers run IPv4 anyway? Moreover, if IPv4 addresses are not available for client machines, they can use private IPv4 addresses that are not unique over the Internet and send their traffic through a Network Address Translator (NAT). If a new company needs servers and cannot obtain globally unique IPv4 addresses for them, it can host its services in a cloud provided by a cloud service provider and let the provider worry about the addressing. Actually, this gives a hint that the shortage of IPv4 addresses boosts the business of the cloud providers while it is difficult to see how any of the big players would profit from IPv6. For mobile battery powered users IPv6 promises a longer packet header and a globally unique address leading to more packet overhead on the air interface and increased vulnerability to attacks. Deployment of IPv6 is an example of Internet politics.

Over the past months lots of the news has been Internet related. Bradley Manning was sentenced to 35 years in prison for leaking US government secrets to WikiLeaks – an example of a conflict between the Internet mentality of "information wants to be free" and the Internet generation against traditions. Edward Snowden got a temporary asylum from the authoritarian Russian government that seems to provide more freedom than the traditional bastion of freedom and democracy: the US. In Helsingin Sanomat (18.7.2013) leader of the Transcend Peace University, Johan Galtung introduces the term *new fascism* that justifies total surveillance of the Internet in the name on anti-terrorism and national security. Personally, I feel that the term is a bit confusing. To me, the term, *fascism* combines totalitarianism with racism and genocide.

Wikipedia defines totalitarianism as "a political system in which the state holds total authority over the society and seeks to control all aspects of public and private life whenever necessary." Totalitarian systems are different from authoritarian regimes that actually may support rather extended freedom provided that the main authority is not questioned. The definition implies that a totalitarian regime needs an ideology that justifies the control and it does not accept nor protect the privacy of its citizens. Organisations like, National Security Agency (NSA) in the US, the Swedish Defence Radio Authority (FRA) and Government Communications Headquarters (GCHQ) in the UK are authorized to monitor all Internet data that crosses a national border. Many times it is far from easy to differentiate the traffic of own nationals from non-nationals. Therefore, we can see that people's privacy is being violated and this is justified by the political ideology of anti-terrorism and national security. Unfortunately, the situation with people's privacy in the Internet is worse than that: major Internet service providers such as Google and Facebook base their business models on mining private information about people and leveraging this information for profit. Most Internet

users care little about this because this mining comes with lofty promises of ”free services” and assurances that indeed the magic of Internet offers everybody “a free lunch”!

The worries of loss of privacy are countered by many Internet applications turning to use encrypted connections between clients and servers with the https protocol. This indeed limits the role of pure network based monitoring: in the middle of the network, a monitoring point can only see the source and destination addresses in packets. Agencies like NSA, FRA and GCHQ send orders to the service providers to release the content from points where https is terminated, i.e. the cloud of the service provider. This order comes with a non-discloser demand saying that the very existence of the order can not be mentioned by the service provider forcing e.g. the CEOs and PR –officers of these companies to lie in public. To me all this means that many governments that, traditionally, are seen as bastions of freedom and democracy have indeed given the tools of a modern totalitarian system to the hands of a small secret sect of people. The next step on this path would be a will to systematically misuse those tools. The opportunity is there.

Players that have widely differing and even conflicting interests use the Internet to communicate and run their lives and businesses. The current Internet makes it possible to misuse people’s trust and take advantage of and cheat the careless and the gullible. In the long term it is paramount that non-aggressive and cooperative strategies of interaction between the players will prevail. After all, the most successful societies are those with higher levels of mutual trust and the most developed forms of cooperation among the people. To help such development, multi-disciplinary Internet research combining technology with economics, law and social sciences, is needed. We, as Internet users, should also become more aware of the privacy issues related to all Internet and smartphone use.