Before the sky falls down: a 'constitutional dialogue' over the depletion of Internet addresses (draft)

(will be published in: Bridget Hutter (2010). Anticipating Risk)

Introduction: the definition of risks as contested terrain

Although it has not yet attracted much public attention, the Internet is at risk of running out of addresses. The depletion of the Internet's address space may seriously hamper the future growth and innovativeness of the Internet (OECD 2008). The potential effects of the upcoming scarcity have been likened to those of "the gasoline shortages of the 1970s to the industrial economy" (Mueller 2008). According to current calculations, the pool of unallocated Internet addresses could dry out as soon as in spring 2012.[1] Anticipating the imminent shortage, the first signs of private trading activities have already been observed. In June 2008, for example, a block of 256 Internet addresses was offered for sale on Ebay, an electronic trading platform. This episode was presented a few months later at a meeting of Internet address experts as evidence of the suspected emergence of a black market for Internet addresses. The concern over a black market is part of a broader crisis scenario, which links the upcoming depletion of Internet addresses to the uncertain future of industry self-regulation in this area. As some experts fear, the authority to manage this common pool resource on behalf of all Internet users may vanish as well once the reservoir of unallocated addresses is dried out. The attempt to auction off an address block, a clear breach of current rules which preclude the selling of address space, could indeed indicate the dwindling authority of consensual address management on the Internet.

There is widespread consensus among the experts that a black market for Internet addresses would pose serious risks not only to the governance structure of the address space but also to the integrity of the Internet at large. "Chaos in addresses is chaos in the network", as one observer summarized the fundamental role of Internet addresses to the functioning of the data network. But does a black market for Internet addresses really exist or is likely to develop in the near future? Perhaps not surprisingly, the answers to these questions turn out to be controversial. In the context of Internet address space management, the anticipation and prevention of risks have become a terrain of passionate conflicts. Experts kept arguing on the Internet even throughout the night of New Year's Eve over the implications and consequences of various policy options. It is well known that the definition of risks "often takes the form of intense struggles" (Hilgartner 1992: 47). Beck (2008: 140) even argues that "conflicts of perspectives" constitute the "essence of risk". Given such fundamental relevance, one may wonder what these struggles are about. There are various approaches to explain the controversies surrounding risks and this article aims to contribute to this line of research by addressing this question in a specific way: In light of the pervasive uncertainty over future risks, how do risks become selected for attention and what makes them such a bone of contention, in other words, how can conflicting perspectives on risks be explained? As I want to show for the area of

[1] A real time calculation of the projected date of address space depletion can be found here: [http://www.potaroo.net/tools/ipv4/].

Internet address management, risks do not emerge arbitrarily, they reflect competing notions of the public good and related governance structures.

The anticipation of risks is not a straightforward process but full of ironies. As Beck (2006: 332) notes, risks are real only to the extent that they are anticipated and once they are anticipated, they "produce a compulsion to act" due to the obligation to "have to control something even if one does not know whether it exists!" (ibid: 335). This process of looking into the future, of making sense of unclear data and predicting threats has recently been described as creating "representations of the future" (Brown & Michael 2003) or "anticipatory frames" (Vogel 2008). Such concepts share the idea that the anticipation of hazards is performative in the sense that it highlights certain threats, privileges specific causal explanations and corresponding courses of action at the expense of others. Anticipatory knowledge in the form of scenarios or narratives (Deuten & Rip 2000) can provide meaning and direction to specific policies (Jasanoff 1999). Accordingly, struggles over anticipatory frames may indicate competing aspirations to control the future (Giddens 1999: 3).

Hilgartner (1992: 40) suggests that we conceptualize risks as a composition of various elements: an object assumed to pose the risk, a putative harm and a causal linkage between the object and the harm. He further argues that linking objects to harm is a contentious process because harm can be ascribed to many objects (ibid: 42). Since risks are embedded in networks of control and responsibility, changes in the definition of risk objects "can redistribute responsibility for risks, change the locus of decision making, and determine who has the right-- and who has the obligation-- to do 'something about hazards" (ibid: 47). Struggles over the anticipation of risks pertain to the future shape of such "socio-technical networks" (ibid: 50). Hilgartner's approach emphasizes the epistemological dimension of struggles over risks by coupling risk objects with the structure of rights and responsibilities that reflect their composition. Changing linkages between risk objects and putative harm may thus question the rationality of regulatory arrangements.

The anticipation of risks may mobilize what Douglas (1992a: 7) has aptly called a "constitutional dialogue", that is debates on future damage that might concern "life and limb" of a community. According to cultural theory, controversies over risk aim at a "bridge between the known facts of existence and the construction of a moral community" (Douglas 1992b: 29). They link "some real danger and some disapproved behaviour, coding danger in terms of a threat to valued institutions" (ibid: 26). The important contribution of cultural theory lies in the embedding of controversies over future hazards in a political and normative context. As Rayner (1992: 92) puts it, social groups tend to emphasize those risks that are "connected with legitimating moral principles". Controversies over risks thus "signpost major moments of choice" (Douglas 1992b: 27) for a community.

Bearing in mind the virtual nature and the performative effects of risks, this article sets out to explore the controversy over risks related to Internet address policy as a "constitutional dialogue". The goal is to relate the debate among experts over relevant risks, potential harms and respective remedies to various notions of the social order and the common good held by that group. With a view to presenting the ongoing controversy in a symmetrical way, the various perspectives will be structured along three popular perceptions of danger in Internet

address space management: the risk of doing nothing, the risk of changing something and the risk of doing the wrong thing.

Managing scarcity: the Internet address space and its regulatory framework

Communication services such as telephony or postal mail require a universal addressing system in order to work. Addressing systems are sets of standardized attributes like area codes or house numbers which allows messages to reach their destination. Usually, each communication service comes with its own addressing convention. The address system or "address space" of the Internet has been likened to a language that enables interaction between heterogeneous machines or servers. Internet addresses provide each item connected to the network with a unique number (naming function), and they determine its topological position (localizing function). Without such a uniform language, the Internet couldn't exist.

The address space of the Internet differs from that of telephone networks in several ways. First, users hardly ever notice the addresses because they are hidden. Internet users do not type numbers to access a webpage, they type names which resolve into addresses.[2] Second, the address space of the Internet is finite. While the numbering plan of telephone networks can be expanded when it reaches its limits, the address space of the Internet cannot but needs to be replaced by a larger version instead. Because the intended transition from the present address space to a larger one has not quite worked out, the Internet now risks running out of addresses. A third relevant difference concerns the ownership and governance of the address space. While the telephone numbering system is subject to national sovereignty and typically managed by national regulators, the Internet address space constitutes a global common pool resource which doesn't belong to anyone. Since the early 1990s, a system of Regional Internet Registries (RIR) evolved, which is responsible for the policies that govern the allocation of addresses.[3] The RIRs are nonprofit organizations whose membership and policy makers consist primarily of the main users of addresses, Internet Service Providers and organizations with large networks including universities. The global address space is thus managed by self-regulation and the authority of the RIRs depends on the consent of their memberships. The RIRs take care of three tasks: the distribution of address space, the setting of allocation rules and last but not least the maintenance of the so-called Whois database which records the allocations[4].

Internet addresses are defined by a technical standard which is called "Internet Protocol version 4" (IPv4). In retrospect, the introduction of IPv4 in 1983 came to be seen as the date of birth of

---

[2] For example, "www.lse.ac.uk" may resolve into "158.143.29.38". This is just one number of a larger address block held by the LSE.

[3] The global address space is managed by five RIRs, which were created between 1989 and 2005, each covering one continent: RIPE NCC (Réseaux IP Européens Network Coordination Centre) in 1989, APNIC (Asia Pacific Netowork Information Centre) in 1993, ARIN (American Registry for Internet Numbers) in 1997, LACNIC (Latin American and Caribbean Internet Addresses Registry) in 2002 and AfriNIC (African Network Information Centre) in 2005. Their membership varies between several hundred and several thousand organizations (see Karrenberg at al. 2001).

[4] The "Whois database" contains information on the holder of Internet addresses. As Wikipedia notes: "The WHOIS system originated as a method that system administrators could use to look up information to contact other IP address or domain name administrators (almost like a "white pages")" [http://en.wikipedia.org/wiki/WHOIS].

the Internet. Theoretically, IPv4 can create more than 4 billion unique addresses. Yet, the address space was already a scarce resource less than 10 years after its introduction.[5] In the second half of the 1990s, a new and much larger address space was therefore developed: Internet Protocol version 6 (IPv6). Unfortunately, the old and the new address space are incompatible; they speak different languages. Because of their incompatibility, it was expected – a formal transition plan does not exist – that organizations would use IPv4 and IPv6 addresses in parallel until all devices connected to the Internet would have migrated to the new standard. Given the global architecture and the poly-central governing structure of the Internet, nobody was put in charge to organize, let alone to enforce, the necessary transition process. In the absence of a global regulatory framework, the actors involved hoped that the invisible hand of the market would gradually take care of it. As a long-term observer declared, "you guys were all meant to figure this was in your own best interests and your local decisions would, say, become global" (Huston 23.10.2007, RIPE 55).

However, the market driven coordination across the Internet has so far failed and as a result, "we are really in a very bad place" (ibid). Roughly ten years after the completion of IPv6, most Internet service and content providers still rely on IPv4. Due to the ongoing growth of the Internet, the global demand for IPv4 addresses is accelerating and the depletion of unallocated IPv4 addresses is now in close reach. According to recent calculations, the last IPv4 address blocks will be handed out in spring 2012. Even if the transition to IPv6 got started in the current year, there would still be a significant lack of IPv4 address space to accommodate the future growth of the Internet. Since any new application or service will depend on both "address families", the demand for IPv4 addresses will soon exceed the remaining supply, a serious problem that is expected to persist for at least a decade (Elmore, Camp & Stevens 2008).

Not surprisingly, experts have begun thinking about what could be done to mitigate the upcoming crisis (for a detailed report, see OECD 2008). The proposal discussed in this article aims at creating a market for allocated but unused address blocks. Among other things, a market for IPv4 addresses is believed to provide an incentive to free up unused address space and make it available for organizations willing to pay for it. Yet, while a recent "Internet census" found that "only 3.6% of allocated addresses" are actually visible (Heidemann et al 2008)[6], it remains unclear how much of the allocated address space is currently in use. Other estimates suggest that between 10 and 15% of the allocated address space is in use. In any case, if a significant share of the idle part could be reclaimed the exhaustion of IPv4 addresses could be deferred by up to seven years (Huston quoted by OECD 2008: 27). Yet, the permission to *transfer* (the policy terminology for 'sell') address blocks between holders would imply a major modification of the existing allocation policies. At present, Internet addresses are defined as a common pool resource that cannot be owned. They are regarded as "loans" and its holders as

[5] Throughout the 1980s and early 1990s, when nobody foresaw the Internet's future as a mass media, addresses were handed out rather generously in large blocks of up to 16 Mio addresses. Organizations with early access to the Internet still hold such large allocations of address space. For the list of allocations, see: [http://www.iana.org/assignments/ipv4-address-space/].

[6] As the authors themselves note, such figures are very problematic due to firewalls and other security mechanisms that prevent a proper census. Still, the large amount of allocated but unused address space is reflected in the language used to discuss address policy. Experts don't refer to the exhaustion of the IPv4 address space, they talk about the exhaustion of the "free pool" or the "unallocated pool" of addresses.

"custodians". Reflecting the long-standing scarcity of Internet addresses, the basic allocation rules stipulate that recipients must provide "documented justification" to prove their need for address space and return allocations no longer required to the registry (Hubbard et al 1996). A trading of address space is obviously not permitted under such circumstances.[7]

Between July 2007 and February 2008, policy proposals were tabled in three of the five regions that detailed various ways of relaxing the strict rules governing the addresses space in order to allow for a trading of address blocks. The original proposals[8], which varied from an almost completely liberalized market to rather minor adjustments of the current policies, have sparked a heated and persistent debate among the members of the Regional Internet Registries and beyond. These debates take place on public mailing lists and at policy meetings.[9] As the next section will show, the anticipation of risks plays a crucial role in the discussion of the pros and cons of the various policy proposals. All perspectives presented in the following part conceptualize the risks involved in specific ways and ascribe these risks to certain forms of disapproved behavior: the risk of doing nothing, the risk of changing something and the risk of doing the wrong thing.

Framing risks and mobilizing action: black versus open markets
The risk of doing nothing

> "Human nature is that we consider inaction to have less impact than action. I think in this case it's actually the opposite" (Leibrand 7.4.2008, ARIN 21).

In July 2007, a policy proposal was presented in the Asia and Pacific region, which advocated a removal of the constraints that prohibit the trading of Internet addresses. Huston (2007) predicts that the "demand of for IPv4 addresses will continue beyond the time of unallocated address pool exhaustion" and that this continuous demand will lead to "a period of movement of IPv4 address blocks between address holders" to meet this demand (ibid). According to the policy proposal, the registry should accept such movements of address space for the sake of the registry's database: "This proposal, by acknowledging the existence of address transfers and registering the outcomes would ensure that the APNIC address registry continues to maintain accurate data about resources and resource holders" (ibid). In other words, if the RIR accepts and records the movement of address blocks among its members, it mitigates "the risks to the integrity of

[7] Mergers and acquisitions are among the few exceptions of this rule. However, even in those cases do the registries reserve the right to evaluate and approve the organization's need for the combined address space.
[8] In the course of the discussion, all of the original policy proposals were modified. This article doesn't cover these changes but they can be traced here: [http://www.ripe.net/ripe/policies/proposals/archive/; https://www.arin.net/policy/proposals/policy_archive.html; http://www.apnic.net/services/services-apnic-provides/policy/policy-proposals].
[9] The following section relies on RIR members' and other experts' contributions to public mailing lists and face-to-face meetings, which are recorded and transcribed. All citations used in the following sections are taken from publicly archived sources, which are generally considered to be in the public domain. Quotes from meetings are indicated by the name of the RIR and the meeting number; quotes from mailing lists mention the name of the mailing list (PPML, NANOG, IETF). Names of individuals who didn't give permission to be quoted are changed.

the network (…) associated with the unregistered transfers of IPv4 addresses" (Huston 2007). "Unregistered transfers" is the official terminology for a private trading of address blocks behind the registry's back. The author of the policy proposal regards such unauthorized movement of Internet addresses as the real risk that needs to be addressed by the RIR.

The assumption that address blocks will start moving when the pool of unallocated addresses is exhausted is widely shared among the experts of Internet address management. In fact, a relevant number of RIR members across the five regions are convinced that a market for IPv4 addresses is already evolving right now, before the address space is fully depleted:

> "There is a market in v4 addresses. Whether it's legal or not, whether we like it or not. Legacy blocks[10] are being transferred out from underneath our feet and we need policy that reflects what's going on right now. We are not talking about the future any more. Money is (…) changing hands…." (van Mook 28.10.2008, RIPE 57).

> "A market already exists (…) As the IPv4 free pool exhausts, that market is going to get much bigger, much faster. It would be nice if this market were somehow self-regulated by the industry players involved since failing that implies something I suspect none of us want. (…) Perhaps we could agree that not doing something until it is too late would be bad?" (David Conrad 19.02. 2008, NANOG).

For the advocates of a policy change, the trade of Internet addresses is an inevitable development and they make this point with a sense of urgency. In their view, the regional registries have no choice but to accept the

> "simple reality […] that businesses who require IPv4 addresses to continue operations will do what is necessary to obtain them" (Conrad 19.2.2008, NANOG).

In their view, the issue is not longer whether or not companies will trade address blocks but if they do this on a "black market or an open market" (Bush 7.5.2008, RIPE 56) and

> "how (or even if) the existing policy bodies can impose some form of self-regulation to keep the inevitable market behavior from completely running amok" (Conrad 19.2. 2008, NANOG).

The market is perceived as an occurrence beyond the control of industry self-regulation, and it is suspected that the pending depletion of IPv4 addresses will weaken the RIR's regulatory authority even more. As one RIR member put it, "it's not that we can send the Internet police after them" (Delong 15.12.2008, ARIN 22). The movement of addresses might not longer be governed by the existing allocation framework but by a logic of economic scarcity which infuses its own rules and values into address management. In light of such powerlessness, the RIRs may as well

> "stop all discussions of whether we allow or disallow or regulate or not regulate a market because we don't have any tools" to create or prohibit a market (Blokzijl 28.10.2008, RIPE 57).

---

[10] The term "legacy blocks" refers to Internet addresses that were allocated before a formal regulatory framework operated by the RIRs was in place. Legacy addresses show a low usage rate and have an unclear ownership status (OECD 2008: 26).

The black market constitutes a proper "risk object", which is believed to create serious harm. One form of harm consists in the movement of address space without being reflected in the registries' Whois databases. As a result, the information on actual holders of individual address blocks could become less and less reliable. If the registry ceases to provide accurate information, however, the function and value of Internet addresses themselves are put at risk. Internet addresses are an odd object that can be easily copied and stolen, as one of the policy authors warns:

> "Don't forget addresses are numbers. In a true black market, if I'm a bad player, I can sell *you* number 10, *you* number 10, *you* number 10, and *you* number 10 and none of you will know that you've been fooled. Black markets allow for incredibly bad distortion. What happens is chaos in the address space. We'd like to mitigate that risk" (Huston 06.09.2007, APCNIC 24).

Without a reliable registry, Internet addresses could lose their uniqueness and thus turn into mere strings of numbers. No doubt, such a development would undermine the Internet infrastructure. An unreliable database implies risks also for the prospective buyers of address space. How could they be sure that the purchased address block is indeed unique and not "hijacked" or copied? A RIR member in favor of an open market compares the uncertainty of buying used addresses to that of buying a used car:

> "I am in favor of having a transfer policy that legitimate organizations […] will elect to do the transfers under as a method of keeping their risks lower – the same reason that you might buy a used car at CarMax rather than from somebody with an advertisement in the paper" (Stormeas 07.04.2008, ARIN 21).

Yet, a corrupted, unreliable Whois database is not the only risk that the Regional Internet Registries face. According to another worst case scenario, the RIRs could be put out of business by competitors with a more liberal approach to address markets as a new business model. After the pool of IPv4 addresses is exhausted, the Regional Internet Registries lose the specific allocation function that sets them apart from other potential registry operators. Since the Whois database is public, it can be as easily copied as any other digital information available on the Internet. Should the RIRs decide to hold fast to the existing policies, they could find themselves in competition with other registries, as the director of APNIC reminds the members:

> "I would suggest, if the RIRs do decide not to do anything, then for anyone in this room who would like to think about starting up a transfer registry […] there is potentially a business opportunity there. […] I think there comes a time potentially where, if the RIRs aren't covering this particular area, then someone else might, and it could be a private enterprise or a government entity" (Wilson 06.09.2007, APNIC 24).

Any change of ownership the registries refuse to record in the Whois database could thus become a business opportunity or even the starting point for a public service. By refusing to accept – and register – the reality of address trading, the registries may put at risk their future authority if not the governance model.

The distinction made between an open and a black market plays a crucial role in the risk scenario of the market advocates. The latter is associated with damage to nearly every aspect of the Internet's addressing system: the authority of the registry, the integrity of the registry's

database, the identifier function of the address space and ultimately the value of the Internet at large:

> "If we do nothing about this area of transfers, the industry will continue. It will hobble along somehow. But the integrity of addressing and the understanding that when someone places an address in the routing system, you clearly understand who it is, and it isn't a hijack, it will become harder and harder and harder, and when you eventually get to the point of losing coherency in the address system, you no longer have a network worth while" (Huston, APNIC 24, 06.09.2007).

By contrast, the open market to be created by the registries is expected to move address blocks in a favorable way, for example by increasing the efficiency of address utilization. The authors of the European policy proposal for an address market advertise their transfer model as a means to "enable usage of the probably significant pool of 'allocated but unused' IPv4 addresses" (Titley & van Mook 2007). Hence, trading address space per se doesn't appear to be a threatening activity. On the contrary, provided the transactions between buyers and sellers are reflected in the database, it is believed to mitigate the risks ascribed to the black market.

The prediction of the profound harm caused by a black market comes across as moral pressure for changing current address policies. Yet, the anticipation of a black market will only induce support for a policy change, if the underlying assumptions are broadly accepted as a representation of the future. The majority of RIR members must share the beliefs that a black market is evolving, that it poses risks to the Internet as well as its governing structures and, furthermore, that an open market for Internet addresses presents an effective remedy against these ills. However, as long as IPv4 addresses are still available, the potential size and harm of a black market are even for experts difficult to assess. What is more, open markets for Internet addresses may involve new risks. As the next section will show, the emergence of a black market is just one of many risks that observers are anticipating.

The risk of changing something

> "Essentially the only thing we can do now is stand back and get ready to roast marshmallows on the fire of the media driven panic when the pool runs dry" (Tony Hain 14.07.07, IETF).

As even the advocates of a market for Internet addresses concede, the introduction of a trading system would present "a big departure from currently set policy" (Titley & van Mook 2007) if not a "revolution in how we do things" (Murphy & Wilson 2009: 2). A market would imply a "fundamental change [in, J.H.] the way we have been imagining address space" (Inatuko 28.08. 2008, APNIC 26) as it would suspend basic principles of the existing allocation rules. At present, the registries hand out address space on a license basis, according to proven need. Address holders are expected to return address space when the need no longer exists. Without saying so, the introduction of a trading system is aimed at holders of address blocks who, despite having excess address space, are not returning it to the registry. As a RIR member observes,

> "if the transferor has IPv4 to give they likely are already in violation of their RSA[11] in any case" (Mittelstaedt 13.02.2008, PPML).

Sceptics point out that, in light of the present allocation rules, a market would provide a "financial incentive for those who don't adhere to the community spirit" (Curran 19.02.2008, NANOG). It

> "would introduce ridiculous unfairness, and result only in rewarding those who could be argued have been dishonest (apologies for the moral tone, but fairness requires some moral perspective)" (Wilder 01.10.2008, PPML).

What seems to be at stake here is nothing less than the moral foundation of industry self-regulation. It is suspected that an address market, even the mere discussion of it, may be performative in the sense that it creates monetary value for the common pool resource and undermines the "community spirit" on which self-regulation is based. As a RIR member argues,

> "…the transfer policy talk is preventing people from returning unused space. Why would anyone surrender unneeded IP space if there were a likelihood or even a possibility that that space will hold monetary value?" (Kargel 30.09.2008, PPML).

Money is believed to not only corrode the morals of the community but also to create opportunities for abuse and manipulation. Big companies with large resources may hoard address blocks for speculation or to form monopolies and "over time the deep-pockets own everything (…)" (Mittelstaedt 14.02.2008, PPML). From the perspective of the market opponents, trading of address space thus presents a "harmful and/or exploitive activity" (Kargel 01.10.08, PPML) associated with greed, fraudulence, and abuse of financial power.

Sceptical observers also suspect that, as a consequence of a monetarization, the status of Internet addresses and that of the registries as their "stewards" could irreversibly change:

> "One way a transfer market might pose such a threat is if it moved us from regarding IPv4 addresses as a common pool resource to a private property regime with its attendant regulatory constructs (rights, obligations, and enforcement mechanisms)" (Lehr, Vest, Lear 2008: 25).

A trading of address space could create private assets that would no longer be governed by industry consensus but by property rights, tax and antitrust law. Although the policy proposals under discussion include various precautions to prevent the market from overruling RIR address policies, it is uncertain if address traders would accept those rules. While the advocates of an address market stress the fact that the RIRs lack the authority to prevent a black market from emerging, the skeptics insist that

> "…none of the RIRs as currently constituted possesses clear authority or adequate means to enforce any proposed rules and restrictions on transfer markets (…) the current regime has been sustained by the community of shared interests and by the need to return to the RIRs for subsequent allocations of IPv4 addresses. Introduction of a transfer market opens the door to the opportunity to bypass the RIR process, thereby potentially disrupting important components of the self-enforcement mechanism" (Lehr, Vest, Lear 2008: 31).

Opponents of a market for Internet addresses fear that a significant change of well established policies could mean "men in suits come in and take over" (Claffy17.04.2008, PPML) and, hence, the end of self-regulation. They stress risks such as lawsuits over access or ownership to

[11] Registration Service Agreement between RIR and address holder.

address space, taxation of as yet common property and not least public regulation of the scarce resource. As a British Telecom representative put it,

> "what RIPE should do is not encourage the appearance of a market place, because the appearance of a market place, in the end, is going to attract regulatory attention (…) In the end, there are going to be competition issues, there are going to be antitrust issues and all the things that regulators like to look at in terms of the fairness of the market itself. Once again, if we see that kind of global address shopping, we are going to see governmental agencies interested in intervening here to protect their national or sovereign interests" (McFadden 23.10.2007, RIPE 55).

Public intervention in address space management could mean that the RIRs lose their autonomy and the industry ends up as mere participants in an intergovernmental policy process.

Another common concern among RIR members is that a trade of Internet addresses could generate so much additional supply that the lifetime of IPv4 addresses would be significantly extended and the introduction of the new address space indefinitely delayed if not altogether derailed. While the upcoming exhaustion of IPv4 affects everyone and may well encourage the transition to the new address space IPv6, an aftermarket is suspected to have the opposite effect and increase the uncertainty about the future deployment of IPv6. Yet,

> "the ISP and carrier community needs one thing very importantly in this process of transition and that is predictability" (McFadden 23.10.2007, RIPE 55).

A market for IPv4 could

> "take focus away from IPv6 deployment" and "draw real resources in the terms of engineer money and time" (Bicknell 7.4.2008, ARIN 21). Thus, "making v4 hang around" may actually be to the detriment of the Internet and "one could argue that the proper stewardship is, pour gasoline on v4 and make it exhaust next week (…) rather than trying to -- you know, tweeze it out as long as we can" (Rafmer 07.04.2008, ARIN 21).

The dangers ascribed to a market for Internet addresses make it clear that, in addition to the "risks of doing nothing", there are considerable risks related to doing something, namely, to change established principles and practices. Risk prevention in the form of establishing an open market for Internet addresses may have unknown side-effects and create numerous kinds of new risks. From the skeptics' point of view, not enough is known about the implications of a market to justify a policy proposal that would turn the "economic architecture of the Internet addressing (…) system upside down." Without solid research of the potential side-effects,

> "this exercise looks like promoting blatant cyberlandgrab, which i don't believe is what any of the registries intend" (Claffy 16.04.2008, PPML).

Critics are also questioning the assumption that a black market is already emerging. As an apparently exasperated RIR member emphasizes after months of debates,

> "this policy is basically ASSUMING that unauthorized transfers are going to happen and we need to regulate them now. While we can suspect that they will happen, and have a very STRONG guess that they will happen, suspicions and strong guesses are NOT GROUNDS for policy (…) What PROOF is there that money for IPv4 transfers at this time will help anything?" (Mittelstaedt 29.09.2008, PPML).

After all, the "black market may not become a gigantic monster" (Zainger 07.04.2008, ARIN 21).

In light of the lack of knowledge about potential side-effects, critics warn against the risk of opening this "pandora's box" prematurely. They liken the market for Internet addresses to a "genie" that cannot be "put back into the bottle". As a fierce opponent warns,

> "please consider that the address transfer policy will be irreversible in a way that nothing has been since the RIR system has been established" (Vest 28.08.2008, APNIC 26).

Once a market governs the movement of address blocks, the RIRs may find themselves without the power to set or revise its rules and even to maintain their consensus model. As Murphy & Wilson (2009: 3) note laconically,

> "although a market cannot be said to rule out the consensus model that has turned out well for the Internet community, it also cannot be said to fully support it. This change may be a cultural one we find difficult to reverse, and it might undermine any future attempt by the community to try to differentiate itself on governance model".

In sum, the skeptics are questioning whether the risks associated with a black market are indeed greater than those of an open market. The transformation of a shared public resource into a tradable good is deemed dangerous, so dangerous in fact that the risks of a black market appear almost secondary in comparison. In other words, the very distinction between the black market and the open market, which forms the conceptual foundation of the policy proposals for address trading, does not have much credibility among the opposing members:

> "I don't buy into the premise that not changing policy is necessarily the most harmful thing we can do. There are many, many unknowns either way we go in this scenario. And I don't think that there is any way to develop enough data to really know which direction is more harmful. And I will point out that we have a great deal more operational experience with current policy than we do with what would be done by adopting such a radical policy" (DeLong 07.04.2008, ARIN 21).

In times of heightened uncertainty, adhering to well established policies looks like a safer choice while "any new policy like the one proposed, simply muddies the waters and creates confusion" (Dillon 12.2.2008, PPML).

The anticipation of risks to the Internet and its governing structure play an important role in the arguments on both sides, the proponents as well as the opponents of a market for Internet addresses. At the heart of the debate are profoundly different perceptions of the future, the time after the exhaustion of the IPv4 address space. While the proponents of an address market believe that it would merely bring into the open a black market that is already evolving, the opponents express doubts about its existence, significance and, above all, the inevitability of such a market. The authority and efficacy of industry self-regulation forms a related point of contention. Will the Regional Internet Registries be still powerful enough to regulate the movement of addresses after the pool of unallocated addresses runs dry or should they admit defeat and simply abandon their regulatory role? These questions are subject of a third line of argument, which revolves around the risk of doing the wrong thing.

The risk of "doing it badly": the design of an address market

> "Although we are reminded of Woody Allen's quote wherein he 'hope[s] mankind has the wisdom to choose correctly... between utter hopelessness and total

> extinction," there are (…) measures we can take to survive the coming storm." (Murphy & Wilson 2008: 10)

The members of the RIRs who are principally in favor address markets nonetheless hold diverging views about the best way forward, and a comparison of the original policy proposals tabled in the RIR regions show varying "rules of the game" (OECD 2008: 26; Mueller 2008; Huston 2008). The differences revolve around liberal versus restrictive approaches to the design of an address market. Some advocates of address trading believe that the RIRs should continue to regulate the movement of IPv4 addresses while others are convinced that regulatory constraints will drive traders into a black market. A somewhat symbolic bone of contention concerns the principle of needs-based allocations. Again, the reference to future risks underpins the reasoning on all sides.

Under the current policies across all regions, organizations must document a need in order to get address space, and it is the task of the registry to check that the applicant fulfils the requirements.[12] The liberal policy proposals for an address market suggest the removal of most of these constraints and reducing the role of the registry to that of a "title office", which would more or less content itself with registering the changes of ownership of address space. By contrast, ARIN's policy proposal recommends making purchases of address space contingent "upon pre-qualification from ARIN to confirm its eligibility" (ARIN Advisory Council 2008) on the grounds that "ARIN's control systems" and "audit trails" provide a safeguard against the fundamental risks inherent to markets such as speculation, hoarding and the potential for fraud (ibid.). By acting as the "monkey in the middle", which is supposed to check the legitimacy of both the seller and the buyer of address space, the registry "takes significant risk off the recipients" (Bicknell 23.11.2008, PPML). As an observer from another RIR notes in defense of these constraints,

> "… one might look at this and say, 'hey, it's ARIN again in their tradition [of, J. H.] over-specifying everything and being amateur regulators' as some people have said before in this meeting, but what they are really trying to do to my mind is to maintain the address space as a public resource, and quite forcefully say, 'you cannot transfer it unless the need has been demonstrated beforehand'" (Garbenker 07.05.2008, RIPE 56).

The evaluation of a member's need for address space is regarded as a panacea against the dangerous side-effects of a trading system and it is believed to prevent the common pool resource from privatization. By adhering to established control practices, the registry hopes to keep the market forces in check and its own authority intact.

Unlike ARIN's approach to an address market, the policy proposals tabled in the European and the Asia-Pacific region depart from the current regulatory framework. More importantly, neither of them stipulates a needs-based justification for acquiring Internet addresses. Instead, both proposals suggest limiting the future role of the Regional Internet Registries to that of a "title office", which acknowledges and records the movements of address space among their

[12] Additional allocations are only granted when the applicant's record is up-to-date and demonstrates that 80% of the obtained address space is in use. The "needs-based" policy does not only help to conserve scarce address space, it also codifies regulatory authority in address space management.

members, provided that a minimum set of requirements is met.[13] The reasoning behind this somewhat self-emasculating approach reflects concerns with the authority of the registry after the depletion of address space: Without the pool of unallocated address space as an authority source, will the rule-setting mandate of the RIRs still be respected by their members or will the registries lose the legitimacy to regulate the movement of address blocks? As one RIR member remarks,

> "to regulate other people's use of resources is fundamentally different from the task of coordinating handouts from a resource-pool" (Heldal 12.02.2008, PPML).

Some experts see the RIRs at risk and predict that only a hands-off approach to the emerging address market will ensure future acceptance among the members:

> "…while the address allocation function was a de facto monopoly function, the same cannot be said for the registry function, and the general compliance with registry policies, particularly with potentially onerous registry policies, is not necessarily a certain outcome. The reason behind this lies in the observation that the selection of a registry, and the derivation of authority of the registry operator, is more based on common convention than by external imposition (…) The registry is public (…) this implies that cloning the registry in some form or fashion is potentially possible at any time" (Huston 2008).

The experts who principally support the idea of a trading of address space nonetheless vehemently disagree on the rules for such a market. Not surprisingly, their disagreement corresponds to differing perceptions of the risks involved. While the emergence of a black market constitutes the common concern of both parties, they not only ascribe different risks to it, they also link these risks to different regulatory philosophies. The proponents of retaining the present allocation rules, including the verification of need, privilege the badness of markets, namely their potential for speculation and fraud, as the main risk. The registry as an intermediary between the trading partners is expected to reduce the risks brought about by markets. Aside from that, the approval of address transfers under familiar terms would also keep the ensuing changes to a minimum so that

> "it also feels a lot like the current process. If you need space you keep submitting forms to ARIN, like always. Almost nothing changes. There's nothing to explain. There should be no bumpy transition to some other scheme" (Bicknell 23.11.08, PPML).

For the advocates of a liberal market model, the adherence to established policies such as the evaluation of needs does not mitigate risks but rather creates them by putting the registry system itself at risk. In their view, dangers to the integrity of the registries' database deserve prioritization. As one expert drastically expresses this position,

> "I see the notion that 'we should change as little as possible and we should cling desperately to our cherished allocation policies even when there is nothing left to allocate' as not being a conservative notion, nor even a quaint and amusing notion, but an astonishingly radical and extremely risky notion (…) that imperils the coherence of the address system for the entire Internet" (Huston, RIPE, 25.10.2008).

From this latter perspective, the Whois database which records the allocation of address space is the key element of the Regional Internet Registry that needs to be protected in the upcoming

[13] For example, both sellers and buyers have to be members of the RIR; the traded address blocks need to be allocated to the seller, belong to the region of the RIR and have a minimum size (see Huston 2007; Titley & van Mook 2007).

crisis while adhering to present forms of address space regulation appears to be mere "window dressing" which "brings the RIR into an untenable position" (Garbenker 07.05.2008, RIPE 56).

Whereas one group of market proponents focuses on risks to the address space as common pool resource and its specific regulatory regime, the other group centers on the coherence of the address space, manifested in the integrity of the Whois database. Both types of risks are in turn attributed to specific courses of action deemed dangerous: overregulation, which may result in the emergence of a black market or competing registries, versus under-regulation, which in turn may cause speculation, fraud and, ultimately, the end of the Internet address space as a self-regulated common pool resource.

Anticipating risks in light of competing definitions of the public good

Facing the close exhaustion of the pool of unallocated IPv4 addresses, the Regional Internet Registries have reached a crossroads. The upcoming crisis calls into question nearly every aspect of the regulatory arrangement that has evolved over the past decade around the allocation of global Internet addresses. Important principles such as the common pool resource-character of Internet addresses or self-regulation outside the purview of states that used to be taken for granted are now appearing fragile. Yet at present, the actual consequences of the address space depletion are still a matter of speculation. In fact, it is even uncertain if IPv6, the new address space, will ever replace IPv4 or end up as a failed innovation. The lack of any formal coordination leaves the deployment of IPv6 to the discretion of individual organizations. In view of this volatile environment, the RIR members are debating their options for mitigating the looming dangers.

The frequent reference to risk in the debate about address policies indicates that the exhaustion of the address space affects the future role of the RIRs in an essential way. The pool of unallocated addresses has been a reliable source of authority for the regulatory regime since compliance with the RIRs' rules and regulations has been a requirement for address assignments. While it is undisputed among the RIR members that the demand for IPv4 addresses will persist for many years after the exhaustion of the address space, it is uncertain how Internet Service Providers, the main customers of the RIRs, are going to go about it, particularly if they will accept or subvert regulatory constraints placed on the future movement of addresses. In light of such uncertainty, the continuation of the present regulatory principles and procedures is no longer self-evident and a revised understanding of the RIRs' role may be required.

As the debate on the pros and cons of markets for Internet addresses shows, the collective effort of anticipating risks does not center on one specific danger or harm but rather disperses into bundles of conflicting expectations, forebodings and conclusions all of which are competing for hegemony. Risk, as Hilgartner (1992: 32) suggests, "is not something that gets attached to technology after the engineers go home"; risks are continuously constructed through processes that are both problematic and contentious. The controversies over risks illustrate that potential harms – the emergence of a black market or the privatization of the address space – can be attributed to many regulatory actions or inactions. In fact, the address policy experts vehemently disagree over the causal relations between potential risks and regulations. For

some, the black market already exists, for others the emergence of a black market depends on the future course of regulation. A third group of experts doubts that there is sufficient address "liquidity" for a black market to evolve, and yet another influential group ascribes harm to both black and open markets. Obviously, all experts involved are selective in their perception of risks. The opponents of an address market by and large ignore the potential harm of an inaccurate database. The advocates of a market, in turn, play down the risks a market might pose for the tradition of self-governance in this field.

Hence, risks associated with the depletion of Internet addresses are not simply out there waiting to be addressed, neither are they arbitrarily chosen; their anticipation entails sense-making and framing activities reflecting a given social context (Tansey 2004). Controversies over risks shed light on the various options considered for the assembling of objects, harms and causal linkages involved in such framing processes. Moreover, they provide clues to the sources of the passion that fuels the process of generating and selecting risks for attention.

The potential harm mobilized in support of or opposition to specific courses of action are by no means trivial. They concern core institutions, values and procedures of the RIR communities. As (Murphy & Wilson 2009: 4) point out "without exaggerating, it is likely that what we do in response to this crisis will determine the architecture of the Internet for a long while to come". The moral commitment to the Internet and its governance structure play a central role in the debate over risks as common values "work on the estimates of probabilities as well as on the perceived magnitudes of loss" (Douglas and Wildavsky (1982: 85). The anticipated magnitude of loss appears as the source of the controversy's passion and it helps to understand which of the risks have a chance to become performative by shaping the future course of Internet address management. The members of the RIRs focus on those risks that potentially affect what they regard as the institutional core or the public good in Internet address management. Their conflicts articulate the various ways this public good can be defined and maintained. They moralize their respective choices by linking potential hazards to disapproved courses of collective action: the risk of doing nothing, the risk of changing something and the risk of doing the wrong thing. The anticipation of risk thus implies a "constitutional dialogue" over the common good and related values of a community.

5. References

ARIN Advisory Council (2008). IPv4 Transfer Policy Proposal (2008-2) [https://www.arin.net/policy/proposals/2008_2.html].

Beck, Ulrich (2006). "Living in the world risk society." Economy and Society 35(3): 329 — 345.

Beck, Ulrich (2009). World at Risk. Cambridge, Polity Press.

Brown, Nik and Mike Michael (2003). "A Sociology of Expectations: Retrospecting Prospects and Prospecting Retrospects." Technology Analysis & Strategic Management 15(1): 3-18.

Deuten, J. Jasper and Arie Rip (2000). The Narrative Shaping of a Product Creation Process. Contested Futures. A sociology of prospective techno-science. N. Brown, B. Rappert and A. Webster. Alershot, Ashgate**:** 65-86.

Douglas, M. and A. Wildavsky (1982). Risk and Culture. Berkeley, University of California Press.
Douglas, M. (1992a). "Risk and Blame." Risk and Blame. Essays in Cultural Theory. M. Douglas. London, New York, Routledge**:** 3-22.
Douglas, M. (1992b). Risk and Justice. Risk and Blame. Essays in Cultural Theory. M. Douglas. London, New York, Routledge**:** 22-37.
Elmore, H., L. J. Camp, et al. (2008). "Diffusion and Adoption of IPv6 in the ARIN Region." from http://weis2008.econinfosec.org/papers/Elmore.pdf.
Giddens, Anthony (1999). "Risk and Responsibility." The Modern Law Review 62(1): 1-10.
Heidemann, John, Yuri Pradkin, et al. (2008). Census and Survey of the Visible Internet (extended). USC/ISI Technical Report**:** 19.
Hilgartner, S. (1992). The social construction of risk objects: or, how to pry open networks of risk Organizations, uncertainties and risk. J. F. Short and L. Clarke. Boulder, Westview Press**:** 39-53.
Hubbard, K., M. Kosters, D. Conrad, et al. (1996). RFC2050 - Internet Registry IP Allocation Guidelines, IETF.
Huston, G. (2007). IPv4 address transfers. prop-050-v001: 4 [http://archive.apnic.net/policy/discussions/prop-050-v001.txt].
Huston, G. (2008). "The Changing Foundation of the Internet: Address Transfers and Markets." The ISP Column. A monthly column on things Internet(November): 1-9.
Jasanoff, Sheila (1999). "The Songlines of Risk." Environmental Values 8: 135-152.
Karrenberg, Daniel, Gerard Ross, Paul Wilson, et al. (2001). "Development of the Regional Internet Registry System." The Internet Protocol Journal 4(4): 17-29.
Lehr, William, Tom Vest, et al. (2008). Running on Empty: the challenge of managing Internet addresses. TPRC.
Mueller, M. (2008). Scarcity in IP addresses: IPv4 Address Transfer Markets and the Regional Internet Address Registries. IGP Paper.
Murphy, Niall and David Wilson (2009). "The End of Eternity." The Internet Protocol Journal 11(4): 18-28.
OECD (2008). Internet Address Space: Economic Considerations in the Transition from IPv4 to IPv6. DSTI/ICCP(2007)20Rev2. Paris, OECD.
Rayner, Steve (1992). Cultural Theory and Risk Analysis. Social Theories of Risk. S. Krimsky and D. Golding. Westport, London, Praeger**:** 83-115.
Tansey, James (2004). "Risk as politics, culture as power." Journal of Risk Research **7**(1): 17–32.
Titley, N. and R. van Mook (2007). Enabling Methods for Reallocation of IPv4 Resources. 2007-08: 2.
Vogel, Kathleen M. (2008). "'Iraqi Winnebagos™ of death': imagined and realized futures of US bioweapons threat assessments." Science and Public Policy **35**(8): 561–573.