Creating connectivity: trust, distrust and social microstructures at the core of the internet

Uta Meier-Hahn, meier-hahn@hiig.de
Alexander von Humboldt Institute for Internet and Society, Berlin

Prepared for TPRC – 43rd Research Conference on Communications, Information and Internet Policy | September 24-27, 2015 | Arlington, VA

Abstract: Since the commercialisation of the internet in the 1990s, many network operators world wide have been confronted with the paradox of internet interconnection: private network actors such as internet access providers, carriers and content-heavy companies compete in a market environment, but in order to have a product, they need to cooperate. This article illuminates practices of cooperation and coordination between networkers empirically from a micro-social perspective. The text focuses on the question of what role trust but also distrust play in mitigating legal, architectural and economic uncertainties in the field of internet interconnection. Preliminary findings from 38 qualitative interviews with network engineers, peering coordinators and internet exchange representatives across the globe are presented. Such networking professionals play a critical role in establishing, maintaining and dissolving connectivity globally. The article shows how trust and distrust work in tandem in this field. Distrust can cause critical moments that lead to reflection about existing modes of governance. On a theoretical level, the study proposes a conception of internet interconnection as a global microstructure that allows for coordination in the absence of multi-lateral regulation or overarching organisational structures.

Keywords: internet interconnection, uncertainty, trust, distrust, social microstructures, cooperation

1. Introduction

Since the commercialisation of the internet in the 1990s, many network operators world wide have been confronted with the paradox of internet interconnection: private network actors such as internet access providers, carriers and content-heavy companies compete in a market environment, but in order to have a product, they need to cooperate.

This article illuminates practices of cooperation and coordination between network engineers, peering coordinators and internet exchange representatives (subsequently called networkers) empirically from a micro-social perspective. The text focuses on the question of what role trust and distrust play in mitigating prevalent uncertainties in the field of internet interconnection.

The uncertainties in internet interconnection are manifold: In their day-to-day operations, networkers who arrange interconnection need to navigate through grey zones that are (1) legal, (2) architectural and (3) economic. – (1) From a legal perspective, internet interconnection is not regulated by multi-lateral, hierarchical rules like telephony. Formal regulation is emerging locally (e.g. in the USA, France), but it is still largely absent. (2) Architectural uncertainty primarily relates to the routing system and BGP, the border gateway protocol. The more than 50,000 autonomous systems of the internet use BGP to transmit routing information to each other. The difficulty is that BGP in its current form does not offer mechanisms to validate if the routing announcements are correct. (3) Economic uncertainties revolve around the valorisation of connectivity. Applying a market mode of economic exchange in internet interconnection is still a challenge, because the internet infrastructure does not register transactions. The internet protocol (IP) is a stateless packet-switching protocol. So unlike in telephony, mail or the interconnection of airlines, networkers have difficulty in conceptualise what exactly it is that they are exchanging, defining it as an entity and determining the qualities of this economic good (Meier-Hahn 2015).

Several disciplines have stressed positive associations with trust as a means of overcoming uncertainties. Economic sociology in particular has linked trust to cooperation (Beckert 2005; Granovetter 1985, 2001). For internet interconnection, both Sowell (Sowell 2012, 2013) and Mathew (Mathew 2014a) have framed trust among networkers as an enabling factor in internet operations. Mathew sees a combination of "interpersonal trust relationships and centralized organisations (or assurance structures)" as the "primary mechanism through which distributed governance operates" (Mathew 2014b).

Only recently has the positive concept of mis- or distrust been introduced to internet governance. Zuckerman has called this the "age of mistrust" ("Harnessing Mistrust for Civic Action," 2015). He sees mistrust as productive force in the critique of institutions. Hofmann goes even further. She warns of an "unqualified bias towards trust"

and suggests that we see trust and distrust as "inseparable companions" (Hofmann 2015a) in a relationship where distrust can also unfold in productive ways.

This article follows the latter notion and conceptualises trust and distrust in tandem. It uses the two-dimensional approach towards trust proposed by Lewicki et al. (1998a) (p. 6) as a backdrop against which the preliminary empirical findings (p. 8) about trust and distrust among networkers are brought to the fore.

With regard to the question "How does trust scale?", this text offers an alternative view to Mathew's reasoning. It explores the idea that internet interconnection entails a "global microstructure" (Cetina & Bruegger, 2002), which does not necessitate a backing by complex organisations (p. 28).

2. Dimensioning the field: How many networkers are we talking about?

When trying to assess the role of trust, distrust and how they are maintained, the potential number of people who are involved in internet interconnection becomes a relevant factor. According to Sowell, networkers have vaguely estimated "that there are between 1,000 to 1,500 people that 'keep the internet running'" (2012, p.22). I suggest a different approach for estimating how many networkers engage in internet interconnection globally. The underlying assumption is that networkers have different dispositions to interact with fellow interconnection professionals. These dispositions not only derive from personal attributes, cultural heritage or from business strategy; they are framed by a network's situatedness in the internet topology. Depending on the number and kind of linkages a network has with other networks, the potential need for and inclination to coordinate with other networkers varies.

With regard to the kind of linkages, networks such as internet service providers, internet access networks, content networks or hybrid networks roughly can be divided in four groups: 1. single-homed networks; 2. multi-homed networks; 3. networks connected to one internet exchange or co-location centre; 4. networks connected to multiple internet exchanges or co-location centres. The latter two groups comprise of the "active BGP speakers", i.e. networks which manage their connectivity independently.

In the following I briefly describe the groups in order to introduce some relevant terminology for the next section and in order to understand how the interconnection profile of a network frames the disposition for relationship-building.

2.1 Single-homed networks: fully dependent

Single-homed networks connect to just one internet service provider. That provider takes care of all connections to the internet for the network. The single-homed network

makes itself fully dependent on its one internet service provider. It pays its provider a so-called transit fee for connectivity with all internet destinations. Single-homed networks are informally referred to as "leaf ASes" because they hang like a leaf at the branch of a tree accessible only through the transit provider who exclusively serves them with data.

2.2 Multi-homed networks: partially dependent

Multi-homed networks connect to the global internet via several internet service providers. Networkers may choose a multi-homed architecture to increase resilience or to reduce their dependency from one transit provider. A network architecture of this kind may also result from historic circumstances such as a merger between two single-homed networks. Network engineers at multi-homed networks need to make interconnection arrangements with more than one transit provider. Thus, they are at the next level of interaction and relationship-building. However, at a multi-homed network, it is still the transit internet service providers who arrange internet connectivity. Multi-homed networks do not pursue an independent approach to internet interconnection.

2.3 Networks at one exchange facility: independent approach to interconnection

The third group comprises of networks that connect to *one internet exchange or a co-location facility* and from there interconnect with numerous networks. Internet exchanges typically offer (at least) two modes of interconnection, which demand different amounts of coordination from the networkers. The first mode is referred to as *multi-lateral peering agreements (MLPA)* with a so-called route server. The second mode of interconnection as a *direct, bilateral session* between two networks, which can be completed at internet exchanges or co-location facilities.

2.3.1 MLPA route server peerings: quick and impersonal

In the most simple MLPA arrangement, all networks that connect to a route server openly peer with each other. Every network announces to the route server the routes for which it is willing to receive and deliver IP packets from all other networks. More advanced setups may allow the participating networks to control their outgoing routing announcements in detail so that the connected networks receive tailored routing information. (A network that sells transit to other networks may want to prevent its customer network from receiving free peering at the route server. Thus, it may announce its routes to all but the customer's network.)

Through a route server, networks can get many peering connections at once quickly and thus easily achieve cost savings. The network engineers of the participating networks at the route server do not need to know each other in person, and they do not need to coordinate. Thus, route servers enable a very impersonal and transactional

kind of internet interconnection arrangements. Despite the simple setup and the economic promise, the use of route servers is all but homogenous, as a recent quantitative analysis by Richter et al. (2014) shows. My interviews affirm that some networkers deliberately do *not* peer at route servers because they distrust the mechanism whereby the internet exchange operates the route server as a third party between the peers (for details see 'Calculus-based distrust: "You should be defensive"', p. 21).

2.3.2 Bilateral interconnection sessions demand interpersonal coordination

Bilateral interconnection sessions can take two basic forms: "direct peering" and "private network interconnects" (PNI). Direct peerings are 1:1-connections established at the internet exchange. Internet exchanges often disapprove of or even prohibit transit or paid peering arrangements in such interconnections. Co-location facilities typically do not have guidelines about the commercial arrangements between the networks that interconnect at their facilities. At co-location centres, direct interconnection sessions take the form of dedicated point-to-point private links, which are commonly referred to as "private network interconnects" (PNI). PNIs use private fibre ("cross-connect" or "x-connect") between the two cages, in which the interconnecting parties, who are tenants at the co-location facility, store their own equipment. Networks are free to negotiate any kind of commercial interconnection agreement. Lengthy bilateral negotiations may precede direct interconnection sessions, both about the commercial conditions and about the operational arrangement of the prospective relationship. What traffic levels do the interconnecting parties expect to exchange? How many prefixes? If they peer at an exchange: what port size do they need? Who bears the costs for the cross-connect at a co-location centre? Will there be a trial period? How quickly will the networks respond when problems occur? Once an agreement is reached, networkers on both sides need to configure the interconnection session.

2.4 Networks at several exchange facilities: routine "BGP speakers"

The fourth group of networks is similar to the third group, except for the fact that networks in this group have a larger geographical footprint and typically carry higher volumes of traffic. Such networks interconnect at *numerous internet exchanges and/or co-location centres*, which are referred to as "points of presence" (POPs). Their interconnection portfolios are typically more complex, both because of the size and sometimes also because of the interconnection structure a network has developed over time. According to the interviewees, so-called de-peering happens less often than the public discourse might indicate. The networkers who are responsible for interconnection at networks in this group have the highest disposition to collaborate with other networkers in person.

Out of the more than 50,000 autonomous systems connected to the internet today, only an estimated maximum of 10,000 autonomous systems belong to groups 3 or

4[1]. It is these networks, which connect to one or more internet exchanges or co-locations, that are likely to actively manage their network's connectivity. These are the active "BGP speakers" of the internet. This reduces the over all maximum number of network engineers who coordinate with their interconnection counterparts in person significantly.

When reasoning about interpersonal trust and distrust among internet networkers, it might help to picture this professional group as a small town. The analogy obviously has its limits because networkers are spread all over the globe. But there are several mechanisms in place which allow for direct interpersonal and group interaction between these networkers as we will see in the following sections.

3. The two-dimensional approach towards trust

The two-dimensional approach to trust development by Lewicki et al. (1998a) serves as a backdrop against which the state and development of trust and distrust between internet networkers will be illuminated. This article assumes the following definition of interpersonal trust. Trust is understood as "confident positive expectations regarding another's conduct", while distrust is understood as "confident negative expectations regarding another's conduct" (Lewicki, McAllister, & Bies, 1998b).

The two-dimensional approach to trust views trust and distrust as independent dimensions. Conceptualised independently trust and distrust can co-occur. Low trust does not necessarily equal high distrust; high trust does not necessarily equal low distrust. Underlying this is the assumption that relationships may develop to have different degrees of complexity and social bandwidth. The same relationship can give rise to both trust and distrust. For instance, we might trust someone within a limited area of interaction (we trust the postman to deliver the mail) whereas we might not trust or even distrust the same person in other contexts (we might not trust the postman to separate his trash for the good of the environment). Acknowledging that trust and distrust can co-occur also enables us to capture how trust and distrust evolve, grow and decline. Thus it differs from often static, snapshot conceptions of trust.

The two-dimensional approach detaches the definitions of trust and distrust from the explicit risk of exploitation. The assumption that trust can only be meaningfully discussed if there is a risk of exploitation characterises rational-choice approaches in the behavioural research tradition. The behavioural approach brought forward i.e. by Williamson (1993) implies an either-or, binary understanding of trust and distrust as two poles of the same dimension. In this, trust is linked directly to cooperation. Distrust

---

1. For detailed BGP Statistics see http://bgp.potaroo.net/as6447/. This estimation roughly compares to 7839 entries in PeeringDB, a wiki-like database of networks that state to be interested in peering. (Accessed on August 27, 2015 - https://www.peeringdb.com)

is linked to non-cooperative behaviour, i.e. exploitation. For a review of the different research traditions see Lewicki et al. (2006a).

Both trust and distrust are further divided in two types: calculus-based and identification-based trust and distrust. *Calculus-based trust (CBT)* "is grounded in impersonal transactions" (Lewicki & Tomlinson, 2014). It follows from a positive calculation of "the outcomes resulting from creating and sustaining a relationship relative to the costs of maintaining or severing it" (Lewicki & Bunker as cited in Lewicki, Tomlinson, & Gillespie, 2006b). Both rewards for compliance and threats in cases of infringement ensure calculus-based trust. *Calculus-based distrust (CBD)* is also grounded in impersonal transactions. But "the overall anticipated costs to be derived from the relationship are assumed to outweigh the anticipated benefits" (Lewicki & Tomlinson, 2014).

Identification-based trust (IBT) on the other hand "is grounded in perceived compatibility of values, common goals, and positive emotional attachment to the other" (2014). The parties perceive each other as having common interests and they assume that their interests "will be protected or advocated by the other" (Lewicki, Tomlinson, & Gillespie, 2006c). They internalise each other's preferences to a certain degree. "IBT develops as the parties create joint products and goals, take on a common name, are colocated in close proximity, share common values, and can be further strengthened as these activities increase in frequency and intensity" (2006c). The level of trust increases over the course of repeated interactions that last in the long-term. The parties believe their counterparts to have good intentions. In contrast, *identification-based distrust (IBD)* is "grounded in perceived incompatibility of values, dissimilar goals, and negative emotional attachment to the other." (Lewicki & Tomlinson, 2014)

4. Preliminary findings

4.1 Methodology

I conducted 50 expert interviews between August 2014 and February 2015 in person at industry conferences as well as by phone or video call. A semi-structured questionnaire was used. Methodologically, this qualitative study relies on an interpretive research design (Schwartz-Shea & Yanow, 2012). Accordingly, the field of network actors was mapped in order to reveal the variety of perspectives and produce a rich understanding of internet interconnection practices, which tend to be hidden in computer science approaches. Interconnection experts from all five continents participated in this study, however, there was an emphasis on Europe and the USA. The participants represented so-called Tier 1s, carriers, transit providers, content-heavy networks, content distribution networks, local access providers and internet exchanges. Their professional experience in the field ranged from three to 25 years. A first set of 38 out of the 50 was used to analyse views about the role of trust in internet interconnection. Out of these, only two participants explicitly denied that trust played a role in internet inter-

connection at all. 36 people affirmed that they see trust at work in internet interconnection, and they elaborated on situations and experiences that involved distrust as well.

Throughout the analysis, evidence emerged suggesting that both trust and distrust are important concepts for explaining coordination, cooperation and collaboration among networkers. The wide array of answers leads me to draw an extra analytical framework, which specifically addresses the development of trust and distrust: the two-dimensional modelling of trust by Lewicki, McAllister & Bies (1998a). In this approach, trust and distrust are regarded not as poles of the same dimensions but as independent dimensions. Thus, trust and distrust can occur at the same time.

4.2 Cooperation and trust among internet networkers

Contrary to behavioural, rational choice reasoning about trust, in internet interconnection, trust is much more relationship based than transaction based. By creating interconnections, networkers create an ongoing interdependence. Peering relationships in particular usually have no termination date, which makes them differ from other kinds of market transactions. Internet interconnection relationships are made to last.

This section describes trust and distrust between networkers in a style leaning towards a "thick description" (Geertz 1973). It gives insight into the diversity of networker's rationales about trust and distrust and provides a context for understanding both cooperation and conflicts in the field of internet interconnection from a micro-social perspective.

4.2.1 Identification-based trust: "Agreements are made between people, not between companies"

Recalling the definition of identification-based trust as "a confident positive expectation regarding another's conduct" which is "grounded in perceived compatibility of values, common goals, and positive emotional attachment to the other" (Lewicki & Tomlinson, 2014) this section sets out to identify the interpretive frame in which networkers make identity-oriented trust assessments about each other. Strong reports of or agreement with such characteristics equates to a high level of identification-based trust, while a low occurrence equates to a low level of trust. Explicit rejection is filed under the category of identification-based *distrust*.

First, this section will identify the values that serve as cornerstones of what many perceive as a networker community. Then, I will present the modes of evaluation that networkers employ to make their trust assessments. A description of what the identification-based trust relationships at the core of the internet look like will follow and will offer a look into professional practices and cooperation. To conclude, I will discuss the ordering dynamic that identity-based trust entails in this realm.

Values. Identity-based trust among internet engineers is based on a common perception of the internet as "a people thing" (I-38). The internet is regarded as both an interpersonal network and a technical infrastructure. Statements like the following indicate this:

> "Contrary to popular belief **the internet is a bunch of people** who all trust each other. There are not a lot of systems in place to ensure that you do not do something wrong against me other than community backlash." (IX-78, emphasis added)

Some networkers further strongly hold on to the concept of a "technical legacy" (I-05). This refers to the origins of internet networking before commercialisation started in the 1990s, when getting networks interconnected and cooperating meant a proof of concept. Cooperation among internet engineers was mandatory to create the early internet. The technical legacy also implies an engineering ideal about the internet as a network of networks that gets more robust and better the more tightly it is meshed. Networkers who share a professional self-conception as care-takers of the internet continue to strive for this ideal: "We're making the internet work!" (I-38). European and US interviewees frequently referred to networkers as "we", albeit without delineating the border of this plurality. This points to two aspects of identity-based trust among networkers: 1) the idea that a community exists and 2) the slightly western-centric idea that this community of values is of global character, paralleling the internet infrastructure.[2]

Networkers gave examples of how they fall back on three modes of evaluation to assess trust towards fellow networkers: expertise, reputation and cultural codes.

Expertise among networkers is not assessed via traditional seals of quality such as university degrees. Where interviewees have university degrees they often only loosely relate to internet networking, if at all. Several dropped out of education in order to start working in the industry, while some changed career or entered their profession on a learning-by-doing basis. This comes as no surprise as in the early days, computer networking hardly existed in university's curricula, and even up till today, there is a lot of tacit knowledge that has not made its way into courses at all. So how do networkers demonstrate their expertise to each other? One possibility is to use remote forms such as email lists like the ones maintained by network operator groups, the Internet Engineering Task Force (IETF) or internet exchanges. These lists serve as platforms where networkers show off their technical skills and make themselves known by contributing to problem solving or the development of future internet technology. For ad-hoc co-

2. A deeper analysis of the perceived community/ies including the characteristics and mechanisms for inclusion and exclusion would go beyond the scope of this article. What should be noted, though, is that interviewees from outside of Europe or the US, e.g. Russia, African and Latin American countries observe European and US community activities, but they relate to them as outsiders. This indicates that the idea of a global *community* is somewhat idealised. It does not negate global coordination, though.

ordination, networkers use instant messaging technology. In a spot check, more than 400 networkers were present in each of the relevant channels, which signals a high responsiveness.[3] There are also in-person meetings: Networkers meet at events such as the Regional Internet Registry's meetings, the IETF meeting but also at so-called peering fora or at gatherings organised by internet exchanges. Networkers use such meetings to arrange interconnection, give technical presentations but also share problems and brainstorm to find solutions. There are regional differences, though. Examining these differences exhaustively would go beyond of the scope of this article, so I shall use just two examples to highlight this point: A Russian interviewee bemoaned how the term "community" historically has a negative connotation in Russia making it difficult for networkers to unite under that umbrella term in self-organisation. People would interpret everything with the tag "community" to be somehow state-driven, no matter how much neutrality is advertised. A Brazilian interviewee who had attended a North American Network Operator Group's (NANOG) meeting was amazed by how much the professional focus seemed to break down the competitive angle there:

> "Many participants in the event ... they do questions and they interact. And also, the presenters, they normally are not afraid to present about problems and to put their face to the others." (IX-99)

Active contributors who convince others of their technical insight and share their know-how on remote channels of communication or at the events are valued for high professional expertise.

The same channels of communication that allow for demonstrations of expertise also serve to build and share reputation. Reputation is an especially important factor of identity-based trust in internet interconnection. Because reputation allows for economic evaluation in market environments where the quality of the product is difficult to measure – as it is in internet interconnection – where pricing tends to be similar and where no previous interaction has taken place. This is typically the case when a network operator decides to move into a new region or market.

Cultural codes. The networker's world is full of symbolism and humour[4], which often is designed to be understood by other interconnection practitioners only. Such cultural codes delineate boundary zones of the community. Being acquainted with the codes helps build trust as well and may prompt people to cooperate as this vivid recollection by an internet exchange employee depicts:

---

3. This compares to roughly 4 percent of all the networks which are likely to manage their connectivity actively as described on pp. 3-6.

4. For a taste of networker's humour, listen to these songs which were performed at RIPE Meetings: "The day the routers died ..." (2007) - https://www.youtube.com/watch?v=_y36fG2Oba0 and "Imagine there's no transit" (2014) - https://vimeo.com/89387000.

> "I used to sell to enterprises. I dressed up looking a bit like a banker [laughs]. So I'd wear the pinstripe suit and I said: 'This is easy. It is a free product.' And I was in [employer's name, ed.] for about four months and I am thinking: 'No one is signing up for me. It's a free product. No one is connecting. I mean, how bad can I be? It's free! Why is nobody doing this?' And the smallest thing is: I changed my outfits to jeans and a casual top and yes, a smart jacket. **But just by changing interestingly enough to a pair of jeans, suddenly I started to see more people wanting to engage with me, talk to me.** Because now they felt that it's not something, that I meant to sell them something. Let's have a conversation around your strategy and network. Very, very small thing. But to this day, it still blows my mind. And ever since I did that, then I realised: 'Okay, there is a little bit more to it than just connect and get free capacity basically, or free peering.'" (IX-45, emphasis added)

This clothing example points to another commonly held opinion among network engineers: a negative attitude towards sales people. Asked whom they would not like to see in their community, the large majority of all interviewees answered "sales" or "commercial people". Upon request, interviewees specified what they mean by commercial: hardware vendors but also peering managers who seek paid instead of free peering relationships. This is interesting in itself. The fact that they declare others as commercial points to their self-perception as non-commercial. So, such interviewees see their own interconnection relationships and especially peering not directly as a commercial activity – which is slightly contradictory if both sides save money.

In practice. High levels of identification-based trust among networkers strengthen a social order that is characterised by an ability to break down the competitive angle in favour of being part of a support structure. Such networkers perceive of their interconnection counterparts as partners, which already indicates a mutual commitment. Before an interconnection relationship begins, they want to become acquainted with the person on the other side and get to know each other:

> "You need to be able to trust someone to peer with them. That's why we say we need to meet with someone, we need to talk to them, we certainly prefer meeting someone in person before we actually go and set up peering, right? (...) **I have flown to Australia just to meet a few people to set up peering because you need to be able to know them**, talk to them on the phone, you know. And when something breaks, talk to them directly to be able to fix it. So that is where the trust factor comes in." (I-92, emphasis added)

An around-the-clock personal availability to react when something breaks is a common expectation among trusted interconnection partners. The internet is live, it is always on and they feel responsible. It may not be visible to ordinary internet users, but the internet breaks all the time – networkers misconfigure protocols, routers stop working, construction works cut fibre cables, natural disasters affect networking infrastruc-

ture.[5] According to the principal engineer of a large content delivery network, he becomes involved in trouble shooting personally about every three weeks. In such situations, interpersonal relationships can let networkers cut the red tape and ignore standard procedures in favour of fast-track issue resolution, e.g. by overhauling equipment at a co-location to bring a competitor's circuit back up. Analogies used to describe trouble-shooting situations included "firefighter" (O-24) and "team sport" (I-38), which underline ad-hoc, issue-based, responsive collaboration towards a shared goal as well as knowledge of common rules.

> "Trusting the routing guys on the other side and them having an idea that you know what you're doing as well. Because there is nothing quite like interconnecting where there is perhaps technical mismatch (...) because **when troubles occur**, and they always do, **you will want both sides to be able to not waste time and firefight the bug -** whatever the problem happens to be." (O-24, emphasis added)

Where one networker has caused others trouble, e.g. by misconfiguring a protocol, fellow networkers expect the wrong-doer to "explain" and "apologise" (N-73). This can be seen as a demand for the counterpart to clarify his/her intentions, an important element of identification-based trust. The networker needs to convince the others "that he does not play fast and loose with [the] data, that the data is not manipulated or being abused" (I-52), that he/she "plays fairly" (I-13) so that both networks can still "work in good faith of each other" (I-61) and get rid of network abuse without degrading the quality of their competitor's internet access service.

Development. Identification-based trust does not come over night. It requires time to form – both in depth and social bandwidth. Networkers persistently present themselves to the community. As a less experienced networker sighed: "You've got to be in it for the long haul." (C-08) Social bandwidth refers to interaction in other contexts than just technical discussions. This is where the so-called socials and "beerings" or "Beer, Gear & Peer"[6] meetings come in. They broaden the range of experiences and topics networkers share with each other.

> "I've known [Networker X] for many years. **We were together at the beach in 2009.** Throughout the years, **we met over and over again** and talked. **So I just write an email: 'We need this** [enhancement] from you.' And [Networker X] goes: **'Sure!' Does not need to do much evaluation**." (I-60)

---

5. For a real-time view on detected BGP irregularities see https://bgpstream.com

6. Beering is a combination of "beer" and "peer". Beer, Gear & Peer alludes to BGP, the Border Gateway Protocol that is used to communicate between networks. Both refer to relaxed social gatherings outside of the regular programmes at NOG meetings or internet exchange meetings, often involving alcohol.

It is important to note that networkers are often highly specialised professionals within their companies. In small and even medium size ISPs there may be just one networker responsible for all internet interconnection and peering issues. Within the limits of their companies, these networkers have a lot of autonomy in decision-making processes.

> "Every networker or architect adds his personal touch to his network. He has to stay within certain borders. But **within the network, he is like ... the god**." (I-54, emphasis added)

The flip-side of this autonomy is that networkers often lack internal sparring partners. So they need to reach out to other professionals in order to discuss work-related issues and developments. Coming from such a position, networkers very much welcome the quality discussions they can have in this community of practice (Wenger 1998). It contributes to identity-based trust when people are in the same line of business. For networkers this means that they can talk about common issues, admit problems, share their "deep dark secrets" (N-98), experiences and ideas with colleagues rather than with customers (or members for IXPs). Sometimes these relationships serve as personal trust-shields both vis à vis other networkers in the industry and vis à vis the networker's own companies and their agendas. Identification-based trust can allow networkers collaborate in the face of competitive pressures and it can cross-cut company strategies:

> "It's very helpful to be able to have a conversation and say: 'Hey, **I have a problem** in this part of the world and it's affecting my performance where, **if that gets out to the press, that makes my company look really bad and it doesn't help me to solve the problem**.' Whereas if I trust another network engineer I can tell him exactly what's wrong and how it's impacting me and get him to help me to fix it. [...] **Trust is important so that we don't have to run around executing non-disclosure agreements constantly.**" (C-15, emphasis added)

Professional and private online social networks enforce identification-based trust. Networkers connect on sites like Facebook and LinkedIn, thereby producing tight, identified and semi-public social networks. Many networkers perceive their industry as a "small illustrious circle" (I-54) or a tight network, with a high fluctuation between the employers. An elite subgroup of networkers who represent global network actors meet frequently because they all travel to events around the globe, which has yielded the term "flying circus". One of these travellers reported being on the road two out of four weeks, e.g. at global conferences. Online status updates inspire gossip about individual career paths but also about how network operator's personnel policies indicate changes in interconnection strategies.[7]

---

7. For instance, since content-heavy network actors often seek free peering arrangements they are said to be especially interested in employing peering coordinators who have worked at internet service

Dynamic. Identification-based trust among networkers gives shape to an interaction order that is characterised by a solution-oriented, highly reactive capacity on the one hand ("firefighting"). On the other hand it enables coordinated planning activities (a "long-term understanding of each other"). Planning is a necessity that is rarely talked about in the public discussion about internet interconnection. But interconnection talks between networkers today often revolve around capacity upgrades and future developments – probably more often than around completely new relationships. In a typical scenario, one network may know that its traffic at a certain exchange facility will increase. In order to avoid congestion at that place, the networker in charge needs to prepare his/her interconnection partners and convince them to adjust their calculation, which is: they should discard their own forecasts, make an investment and upgrade their capacity as well – all in advance. For the partner such a request creates a situation that is difficult to judge, because it is possible that the requesting network is planning to "poach" customers: "Do we agree to this capacity or what do we do? Why is [he] asking for that? So it's tricky, we must have some feeling." (I-13)

In short: identification-based trust fosters future-oriented behaviour because where it exists, it provides continuity over time, which transaction-oriented thinking does not. Interpersonal relationships may even endure in times of structural or strategy changes, for example they may inhibit individuals to engage in fully competitive behaviour against acquaintances.

4.2.2 Calculus-based trust: "Self-interest polices trust"

Calculus-based trust results from decision-making processes in which networkers rationally weigh up the anticipated costs of engaging in an interconnection relationship and making themselves interdependent on other networks against the anticipated economic benefits.

Cooperation to have a product. Networkers who rely on calculus-based trust regard internet interconnection as a business relationship. All network operators are assumed to be driven by self-interest in the maximisation of their utility, which creates competition. But at the same time, all network operators' utility also depends on internet connectivity, and it is this resource that they can only produce together by interconnecting with other networks. In order to have connectivity-based products network operators need to cooperate. If they do not cooperate, none of them would have a product. So, trustees assume that it is a matter of common interest to look after internet connectivity as a shared resource. And they trust other network operators to do the same, because the network operator's self-interests are assumed to overlap. This type of trust nurtures a basic economic inclination towards cooperation among network operators, which also

---

providers previously. Ex-ISP peering coordinators are sought after for the personal network they have built while being responsible for peering at the ISP. They are also sought after because they know the ISP's margins and their tolerance, which are important indicators in negotiations.

expresses itself in the voluntary adoption of standards for interoperability. The simplified calculation goes like this: I foster global connectivity, because it is the basis for my product.

Generalised trust. Calculus-based trust in interconnection stems from the *generalised* assumption that all networks pursue their self-interest (in a similar way). So, while trust relationships remain interpersonal and are as such not transitive (Mathew 2014b), networkers' calculations include generalised assumptions which do span the industry. This also means that interconnection relationships which rest on this type of trust can be of impersonal character. In such relationships the contact between the networkers is functional, oriented towards effects ("getting things done") and displays a low social bandwidth. All that is necessary is that both networks produce the basic technical competency to set up a BGP session. This can be done by employees in the network operation centres (NOC).[8] If the over all evaluation, including trust, turns out positive, a clearly written email request with the technical information to the standard mailbox peering@network.tld may be enough to initiate a peering. Both the route server technology (p. 4) at internet exchanges and the rise of preconfigured plug'n'play routers have fostered these impersonal kinds of peering relationships and allowed them to spread rapidly.

Social maintenance. While calculus-based trust does not depend on pre-existing interpersonal relationships, such relationships may be incorporated into the calculation. In this scenario networkers perceive socialising as part of the business.

> "So it's really very much about the social element that once you cooperate, which is necessary to get the interconnection going, and there is **no contractual relationship** as such, then the best way of keeping that relationship is by having some kind of **social connection** which **acts as a currency** almost, you could say." (O-29, emphasis added)

The citation highlights an understanding of internet interconnection as a cooperative business relationship that does not have a preset termination date. In the absence of formal agreements, this business cooperation needs to draw on other resources to continue in the face of future competitive pressures. Interpersonal relationships are seen as a form of social maintenance, clearly in service of getting things done: "What they [the peering coordinators, ed.] should do does not change based on how many beers they have drunk together." (N-58) But social maintenance adds (value) to the positive expectations about an interconnection arrangement.

> "So, in order to establish who the correct people to work with are get the best internet conditions for your users, **it is very important to be sociable**

8. One interviewee lapidarily referred to such employees as "drones", highlighting that their job profile is limited to the execution of agreements that higher level peering managers or network engineers have arranged.

> **and come to events in your region and interact** with the people that you peer with and buy from and sell to, so that you can make sure that you're looking after everyone's interest. Because, you have to remember, that **the internet is 40,000 competitors** who are competing with each other. **But if they don't work together, then none of them have a product.**" (I-61, emphasis added)

Contracts. Calculus-based trust also leads networkers to be critical of peering contracts: Networkers who express high levels of calculus-based trust typically favour to arrange peering relationships on the basis of a handshake, avoiding technicalities such as contracts because they cause transaction costs. This preference of handshake agreements relates to the understanding of peering as a mutually beneficial relationship in which both parties save money as equal partners. The rationale behind this is that peering is actually tested by wether both parties are in a position to not peer. Because if one desperately needs to peer and the other one does not, then it is not an agreement between equals but an asymmetric relationship. Based on this definition, there is no need for a contract in peering. Further, trying to enforce a contract before a court in the event of conflict would only add costs for both parties or, as one networker says: "Peering contracts don't add value on it, right?" (C-92) In line with this, the interviewees perceived attempts to formalise an interconnection relationship by changing it from handshake agreement to contract as a signal of a lack of trust.

Route integrity. In the practice of peering[9], the assumption that all networks follow their self-interest also lets networkers put some calculus-based trust in the integrity of routes, which overall is still a contested issue that is fraught with uncertainties, because networks technically cannot assess the authenticity of a route. So interconnected networks run the risk of receiving spoofed, unreliable addresses and routes that do not have integrity from their counterparts. In a worst-case scenario, this can lead the affected network to forward traffic to wrong destinations, with the result that the content of this traffic may be compromised. Also, if the spoofed route announcements propagate into the global routing table to be used by networks around the globe, the correct recipients might become unreachable for anybody on the internet.[10] The underlying trust

---

9. In peering arrangements networks share routes and exchange traffic with each other directly at no charge. An economic reasoning behind peering is that both parties save money from interconnecting directly by cutting out third party transit networks in between them. So if the costs for arranging and operating the peering session are lower than the costs for transit, both parties have a classical economic interest in the relationship. Transit relationships induce uncertainties as well, but there is a clear classification who is the provider and who is the recipient of a service, which allows for the recipient to claim a better service or choose another provider.

10. In order to limit the need for trust, networks usually do so called prefix filtering, i.e. they estimate a maximum number (and types) of routes that an interconnected network will announce to them and limit what they accept to this setting. More sophisticated methods of prefix filtering include checking announced routes against the RIPE database. However, prefix filtering is a measure of defence that signals little trust or even distrust.

calculation that causes the positive expectation (to receive reviewed routes) despite such uncertainties again draws on to the maximisation hypothesis as a senior networker explains:

> "I give you my customer's routes and you give me your customer's routes, and that's all we give." And you go: "Well, isn't there some trust that you only give me your customer's routes?" Well, it's self-correcting. So in theory when you and I peer, I am careful to make sure that the routes I expose to you are routes where I obtain money. They're my customer's routes. If I expose peering or upstream routes to you, then I lose. Now, you're saying: "You trust me." I am saying: "**My self-interest polices that trust**. Because if I don't do precisely that, I'm a loser." (O-35, emphasis added)

So it is in the network's self-interest to announce just "healthy" routes – also, because if the network advertised bogus addresses, everyone else would have an interest in isolating the wrongdoer from the network. Widespread knowledge about such possible sanctions from other networks produces deterrence which, in turn, contributes towards honest behaviour.

> "If you don't play by the same rules, the wires get cut – is the theory. In practice, not quite so obvious." (O-35)

While uncertainties remain, such general calculus-based assumptions produce trust that helps the networkers to mitigate some uncertainties and engage in interconnection. Note though, how the interviewee above limits his statement to "theory". In practice, networks sometimes expose unexpected routes – be it intentionally or unintentionally – hence route integrity remains a critical issue. The technical community is trying to address this by way of authentication mechanisms.

Agreements are private. Calculus-based trust safeguards several informal rules in the realm of internet interconnection. One is to keep the content of interconnection agreements private. Preventing other market participants from having access to information prevents a fully competitive market. It ensures an asymmetry between competitors from which profit-margins and business-opportunities arise in markets (Beckert 2007). So both competitors know that transparency would hurt the interconnection counterpart's business and make future interaction more difficult. Several interviewees have stated how important it is for them to trust that both parties keep prices confidential and do not disclose how much volume of traffic two parties exchange in a given interconnection.

Dynamic. Repeated interaction sharpens the networker's judgment on whether to trust or not to trust. So through long-term experience with an interconnection counterpart, involving for instance well-managed traffic-levels and a reliable contact a networker will develop a high level of trust and confidence with regard to his/her counterpart's actions.

Summing up, calculus-based trust in internet interconnection to a large part derives from general considerations which are based on the assumption that every network pursues the maximisation of self-interest, largely in a similar way. Calculating trust signifies the commercial internet. Relationships between networkers are likely to be either impersonal or of limited bandwidth (such as impersonal email communication). They are driven by a getting-things-done attitude. Sometimes, socialising is fully incorporated into the calculation as "social maintenance". In recent years, advances in the route server technology have given rise to an increase in such impersonal peering relationships. High levels of calculus-based trust relate to little regulation by contract.

4.2.3 Identification-based distrust: "You can trust your own wife, not the peering partner"

In contrast to identification-based trust, identification-based distrust is "grounded in perceived incompatibility of values, dissimilar goals, and negative emotional attachment to the other." (Lewicki & Tomlinson, 2014) Both notions of identification-based trust and distrust have in common that networkers regard internet interconnection as an interpersonal relationship. However, in relationships where identification-based distrust prevails, networkers' interpretive frameworks diverge from the prevalent frame's characteristics of trust as described in the previous section.

There are infinite ways of disagreeing with something specific, such as the values and practices that have been subsumed under identification-based trust here. Distrust appears to be more difficult to describe comprehensively than trust. So this section limits itself to reporting where networkers have not only disagreed vaguely – such as in: "Knowing who you can trust and who you cannot trust is very important as well." (C-66) – but also pointed to alternative values, informal rules or practices. If we regard trust as the prevalent notion among networkers, then distrust highlights which aspects of the dominant frameworks of interpretation are contested.

Breaking with the technical legacy in favour of self-interest. Interconnection relationships are arm's length relationships in the sense that networks hand over their traffic to each other. They cannot control how their interconnection counterpart forwards that traffic. According to the technical legacy, it should be assumed that make their best effort (i.e. act in good faith) when transporting the traffic on the shortest path to the next hop towards its destination. So if networkers instead route their peering partner's traffic to the partner's disadvantage, this is at odds with the technical legacy. A network may for example re-route the traffic to a distant location in order to enforce a peering policy there, figuratively speaking taking their peering partner's traffic hostage. Where interconnection partners discover that "their" traffic is being abused in this way, which degrades their end-user's internet experience, identification-based distrust arises towards the deviant actors.

Lone warriors and egos. Networkers also have completely rejected the notion of trust in internet interconnection and with this also any identity of values or shared goals

among networkers. Where others perceive a coherent community, these networkers have a very particularised understanding of internet interconnection. One interviewee described this by way of an analogy with family relationships:

> "When you establish the peering session **you have to do a lot of checks. It's not like trust.** Trust, you can trust your neighbours but you cannot trust your peering partner. (...) They have to constantly monitor what's going on and re-route it if something is not correct. So, it's a lot of technician involvement after that. It's not like that you have to trust the peering. There is nothing about trust. **You can trust your own wife, not the peering partner.**" (I-02)

Note how the uncertainty here is compensated for by a strong emphasis on checks, monitoring and maximum control through technical means.

In relationships that are characterised by identification-based distrust, the dominant understanding of the internet as a common good may also clash with self-centred entrepreneurial attitudes. One networker offered a historical explanation for such an incompatibility of values. He described in detail how internet service providers failed to build an internet exchange point in a European country in the 1990s, according to him due to the lack of interpersonal trust. He ascribed this lack of trust to the networker's entrepreneurial self-perception as lone warriors. The managerial networking paradigm that was later described by Boltanski & Chiapello (2005) was not as dominant then as it is nowadays:

> "There were probably egos, you know, this was a time when internet service providers were run by high risk taking entrepreneurs. And technical people with strong risk-taking approach towards life. And there wasn't necessarily a good understanding of the benefits of long-term good relationships with your commercial rivals. So, yes, this caused a lot of trouble in the early days." (IX-65)

The "ego" aspect was mentioned again in the evaluation of expertism. Expertism does not necessarily lead to identification with another: Collaboration may run into a dead-end where networkers become so passionate about being right that they lose sight of supposedly common goals – such as building an internet exchange on neutral grounds. This allegedly hampered collaboration in France until a few years ago. Dissimilar goals characterise identification-based distrust.

Outsourcing responsibility to technology. Dishonesty, bad intentions and weak communication skills are further characteristics that cause distrust among networkers. This may appear to be a no-brainer. But it is worth mentioning, because in internet interconnection dishonest behaviour can be very difficult to detect in spite of all the monitoring systems that permeate the internet infrastructure and try to make things measurable and transparent. There may be various reasons for traffic flows to appear and disappear – from misconfigurations, to hardware issues to unexpected media events.

Individual networkers make use of this grey area. Two interviewees shared similar experiences: their monitoring systems had reported irregularities in a peering relationship. Upon inquiry, their peering counterparts rebuffed them and played along, declaring the irregularities to be temporal technical faults. Later on, both affected interviewees understood that they had been de-peered. Identification-based trust changed to suspicion and identification-based distrust because the interconnection counterparts had not taken responsibility for their actions:

> "After one week you are sure that you have been de-peered. And if the other person does not contact you, if he pretends to not be there, then the relationship with this person is probably over. That is less due to the de-peering. **It is more that this person lies. He is probably not trustworthy anymore – whatever he says.** And if he promises that the sessions will come back but nothing happens ... Whatever the internals of this company and the person's constraints may have been: this does not foster trust. **So you avoid both the person and the company that displays such a behaviour.** You do not want to have to do with them anymore and you do not want to buy anything from them anymore." (C-29)

Absence. As described above, community events may serve as places where identification-based trust can be built. In turn, absence from such events can solidify distrust towards those who stay away. The more interconnection relationships a network has, the greater the aggregated expectation that this network will also offer a personal "interface". Thus, constantly ignoring community events can be perceived as avoiding interpersonal relationships and discussions, which can increase negative expectations by those who are in demand of such relationships. Peering fora typically have socialising at the core of their agenda[11], so community building is intense, participants create personal relationships of greater bandwidth, and they also note well who does not engage.

> I won't name anybody, but I actually would say that people who are not fair actors in the transit world, they are not present in these peering forums. So we don't really meet them. (I-13)

Dynamics. Identification-based distrust can be triggered in many ways and via many channels of communication, obviously also relating to the personality of the networkers involved. However, some examples from the field for where identification-based trust has been declared broken are especially telling.

---

11. Peering fora are invite only events. The meeting places usually have a high recreational value, and so-called socials with drinks and entertainment are explicitly part of the agenda. The second unique item on the agenda is the "speed-dating": Half an hour long time slots for one-on-one meetings between peering coordinators. In advance of the forum, every participant gets access to an online booking tool through which one can request such a meeting with any other participant.

- When one networker attempted to change a handshake agreement that had existed for a long time into a formalised agreement, he was accused of breaking trust. (I-18)
- In another well-reported case in 2008, one networker misconfigured his network and affected many other networks. He was immediately perceived as a "bad actor" – and sanctioned with isolation.

> "If the trust is broken that is one of the very, very few things that will unite (...) you know, 99% of the internet. **If you are a bad actor** and betray the trust- (...) **if you lie** and say: 'Well, I am Youtube,' then **the rest of the internet is going to come down on you like a ton of bricks**." (IX-78, emphasis added)

The pride this interviewee takes with the fact that swift collaboration is possible is accompanied with critical thoughts about the legitimacy of self-policing: "the problem is that there is different definitions of breaking trust" (IX-78).

- Identification-based distrust also arises, where other modes of evaluation than the technical legacy enter networker's relationships:

> "Peering is at the boarder between engineers and finance (...) **as it starts moving towards finance**, which is what peering is, the peering relationships, negotiation, measurement, trust etc. … then: **suspicion, measurement, enforcement, lawyers - all business comes in**. It becomes business." (I-38)

4.2.4 Calculus-based distrust: "You should be defensive"

Calculus-based distrust is prevalent where "the overall anticipated costs to be derived from the relationship are assumed to outweigh the anticipated benefits." (Lewicki & Tomlinson, 2014) In this interpretive framework, internet interconnection again appears in a generalised economic context. Individual networkers and interpersonal relationships are hardly taken into account.

Examples from the field that fit in this category are manifold and often point to sore spots and zones of existing or potential conflict. Where calculus-based distrust rules, networkers suspect their counterparts may try to get some undue advantages in peering relationships, achieve a dominant position in a market or cause their interconnection partners harm by technical incompetence or an explicitly competitive strategy.

A basic level of calculus-based distrust is omnipresent in a competitive market. As described in the previous section, there may be commonalities in what network actors see as their self-interest. But a full match cannot be assumed. After all, today most network operators are for-profit driven private companies. And the interconnection industry seems to be getting ready for even more competition as developments towards comparison shopping in interconnection gain traction.

> "**So you should be defensive.** You shouldn't just trust that everyone's self-interest matches. You need to be aware that if you expose too much, other people have the opportunity to abuse you. And **in a world of opportunism, if you expose too much, it will get abused**." (O-35, emphasis added)

On a side note: Distrust also prevents so-called quality of service (QoS) in internet interconnection. The argument goes like this: since there are no contracts, the QoS mechanism is not enforceable. Monitoring would be demanded but it is difficult or impossible to do. So QoS would have to rely on trust. But the uncertainty is too high in comparison to the effort (C-29). Common interests or a common economic assessment cannot be assumed:

> "If someone else sets their priority for something and hands it to you, there's no reason why this should also be your priority." (N-58)

Negative expectations based on distrust lead to situations like this: internet service provider A might deny internet service provider B a mutually beneficial peering relationship because A fears that the new peer B will expand to a region where A is already active. The two networks will not establish a cooperation because A's fear of a subsequent competitive attack from B outweighs the anticipated benefit of the peering. In this vein, the representative of a global transit network complained about internet service providers who had denied him free peering:

> "We have this in writing from several incumbents, they wanna charge us because we compete too heavily with them for content delivery in their own country. And they think we charge prices that are too low. And they don't want us to be able to compete with them on price." (I-20)

In the development of trust and distrust among networkers, internet exchanges have played an ambiguous role. Today, they are often known for the integrative force they bring to the networker community. But this was not always the case and not everywhere.

As interviewees reported, numerous internet exchanges have failed in the past due to distrust because they were not perceived as neutral by the participants.[12] Not-for profit internet exchanges can signal their neutrality through several means, e.g. through an association-based governance model that allows for participatory decision-making.[13] But there are material aspects as well: hosting an internet exchange in one's own facility (and thus saving the money that competitors have to invest to reach that exchange) causes calculus-based distrust from the other networks. Such a setup would

---

12. The basic idea behind internet exchanges is to keep local traffic local by organising interconnection between local internet service providers and other network actors. By peering at no charge, all connected network could save bandwidth with their transit providers.

13. See Wagner & Mindus (2015) for three case studies of different IXP governance models.

also mean that the hosting network is in control of its competitor's equipment, which causes distrust as well. Such setups and the resulting distrust among network actors in a region have lead to internet exchanges failing in the past, even if networkers understood both the financial and technical requirements for interconnectivity between their networks.

One widely respected long-time representative of a large network did not express distrust towards other competitors at internet exchanges but towards internet exchanges as such. Despite all potential financial benefits of peering at an internet exchange, he was in complete dismay about the institution itself. He was concerned about possible third-party interference with the traffic.

> "We'd never push traffic across them. It was always private fibre. It had to be. You know (...) (sighs). It is just too risky for people you haven't got agreements and arrangements with to actively disrupt what you're doing. (...) **You never know who your neighbours are in an exchange.** Because when you go into an exchange, **they're busy selling more neighbour slots**. You have no idea who's on the same fabric and what their motives are!" (O-35)

So in this case, the calculus-based distrust also extends to internet exchanges. It underlines that internet exchanges in practice *are* perceived as intermediaries – even though most exchanges will reject that label. They become intermediaries precisely because they take on a label of neutrality. This neutrality, in the eyes of this networker, is characterised by an openness towards any network that pays. Therefore, an exchange's character as an intermediary lies in having made the decision to allow anybody in.

Calculus-based distrust is also grounded in *bad operational experiences* with a network or in doubts about technical competency. A senior networker from Asia illustrated the lack of competency or reliability with an example about the mismatch between a network's port size at an internet exchange and the backhaul capacity of that network:

> "**You need to know what they're saying is true** (...) It happens quite a lot in Asia, I mean, you know, people will buy a 2.5 Gigabit circuit but have a 10 Gigabit port [at the internet exchange, ed.]. And we have no way of knowing, because it's 10 Gigabit and we are sending 10 Gigabit of traffic, so we need to know from the other side to tell us (...) And, you know, the same thing is happening now in Europe. We see a lot of people coming in from, say, Russia or Eastern Europe in Frankfurt for peering and we have no idea what capacity they are bringing. They're coming even with a 10 Gig port – they'll be full before they know, right? **So, if they're sending, you know, a peering request for me, I'm pretty sure that their pipes are already full.**" (C-92, emphasis added)

4.2.5 Cooperation despite low levels of trust or existing distrust: monitoring and contracts

Network operators who depend on the internet to generate their services do not have an exit choice. So what coping strategies do they use to overcome the uncertain-

ties and interconnect despite low levels of trust or distrust? The main strategies identified in the field are as follows.

Monitoring and technical limitations

Where calculus-based distrust is of a general character, it also expresses itself through the technical measures networkers take in order to mitigate the existing uncertainties. The coping strategy is to seek control through technology. "Trust is good; control is better." (I-18). Such distrust encourages networkers to become active and constantly monitor what is going on in their network so they can reroute traffic if something is not correct. They seek to automise as much as possible and technically limit their connection in such a way that if the counterparts did something bad – deliberate or not deliberate – they would have technical limitations in place. "So you don't **have** to trust your peer." (I-05) For instance, these networkers will set up strict policies as to which prefixes they accept from other networks or check them against the RIPE database.

However, networks also struggle with monitoring. It can be difficult to invent a smart system that alarms networkers in severe situations only. It is also a question of resources (I-02). Smaller and medium sized networks often can only rely on basic software, so they have just little insight into the infrastructure around them. Big networks on the other hand have implemented mechanisms of control with a lot of technician involvement, often in-house as this experienced interviewee from a fast-growing network explains:

> "Everywhere I've worked there has been a fairly homegrown toolset at the start. And at this stage at [company name] it is a homegrown toolset. We are certainly talking to a variety of vendors. But their handl[ing of] the information on the other side is, ahm, challenging. Data storage, of relationships. We do not really outsource that at this time." (C-79)

Apart from individual monitoring efforts, distrust also has a productive side in terms of community efforts in monitoring. Global alliances such as the "RIPE Atlas"[14] or "The RING"[15] draw on distrust as a resource for collaboration. In these alliances networks contribute probes or measurement resources so that every participating network can access an aggregate view on the internet or an outside view on its network.

Contracts

Contracts are a means to create bounded transactions despite of distrust. In transit interconnections where there is a clear provider-customer relationship, service level

14. https://atlas.ripe.net

15. https://ring.nlnog.net

agreements (SLAs) are the norm. Most peering relationships however work on an informal basis. A 2012 OECD report found that 99.51% of all reported peerings were based on handshake agreements (Weller & Woodcock, 2012). As impressive as this number is, the calculation takes the number of peerings as a basis, not the amount of traffic that is being exchanged in global peering relationships. So it says little about how much of the aggregate global traffic exchange is in fact governed by contract.

In fact, the interviews reveal that for larger networks, it is common practice to convert peerings at internet exchanges into private network interconnects once the exchange involves significant amounts of traffic. Then, the business rationale becomes dominant. Formal peering agreements have become more common in private network interconnects, also because both parties make an actual commitment in terms of capital and operational cost (see p. 5).Thus, it can be assumed that significant parts of the overall internet traffic are being exchanged in arrangements that do involve the use of contracts. Usually, it is the larger party in terms of market dominance that gets to write that contract.

Contracts can mitigate calculus-based distrust, because they contribute towards stabilising a relationship:

> "Where we need a contract is where it's A, very important that we have this connection for our business and B, we do not trust 100 percent that the other party will not change their decision in a way that will hurt our business. And then that's the cases where you need a contract. A contract is basically where you say: We know that for as long as this contract runs, you are not going to change anything beyond what we agree in this contract is going to happen." (C-66)

This being said, in practice the power of peering contracts is unclear. Since in free peering no one is paying the other side, there is no way to uphold what is in the contract in a court of law.

> "So the agreements are generally these neutral, quasi unenforceable statements of clarity with no cause termination." (C-10)

So how do "quasi unenforceable" contracts mitigate uncertainty? A Tier 1 representative argues: from a company perspective, contracts are good and important, because of the high fluctuation in the industry. Through formalised documents new employees will know what was previously agreed upon. In other words: Through contracts personal relationships and therefore identification-based trust aspects are pushed out of the interconnection relationship. Contracts objectify internet interconnection. Or, as an interviewee put it:

> "I think, the contract is of course for regulating the interconnection if you completely remove the sense of trust." (I-05)

5. Discussion

Trust and distrust can co-occur. The preliminary findings above certainly affirm that this is the case in the field of internet interconnection. The attitude "Trust and measure it!" (I-38) underlines the ambivalence. Trust and distrust are not exclusive. But beyond this, what can we infer from the findings and the description of internet interconnection in practice above?

I conclude by offering interpretations along two lines: the first reflects upon the productive interplay between trust and distrust in terms of governance; the second puts a spotlight on the global interaction order that has been depicted alongside the empirical findings.

5.1 A generative interpretation of the interplay between trust and distrust

Trust and distrust serve as resources for ordering processes. They work in tandem and contribute to a dynamic of ordering. Drawing on Sztompka's paradox of democracy (Sztompka 1997), Hofmann (2015) has introduced to the discourse about internet governance a generative interpretation of distrust as a source of institution building. Sztompka argues that democracy fosters a "culture of trust" by institutionalising distrust. He gives the example of constitutions, which are defensive laws against the state. In the democratic order, distrust of the abuse of power has been institutionalised in the form of constitutions. Constitutions can be regarded as "trust-generating expressions of distrust". They serve as trust anchors. Hofmann further provides a warning: expressions of distrust should not be interpreted as "erosions of trust" per se (2015, p.3). Instead, distrust can point to both developments towards crisis and towards progress.

When we consider the findings about trust and distrust among networkers for the ordering processes to which they contribute, the interplay between trust and distrust becomes apparent: On the one hand, there are the two types of trust. Identification-based trust produces coherence in the professional community, propagates the technical legacy and long-term relationships. This type of trust forms the basis for a distributed, informal help structure and it moderates competition. Identity-based trust also enables future-oriented coordination among competitors. At the same time, it entails an issue-based, distributed, highly reactive operational capacity. The preference for informal coordination, symbolised by the famous handshake agreements, connects identification-based trust and calculus-based trust. The latter type of trust stands for little regulation by contract. Calculus-based trust can be seen as a trust carpet that fosters cooperation. It infers cooperation from the existing interdependence and the necessity to create connectivity together. Due to its grounding in the *general* notion of maximisation of self-interest, calculus-based trust propels impersonal, objectified modes of coordination in internet interconnection.

On the other hand, there are the two types of distrust. Distrust can create a moment of reflection about underlying rules or conventions. Where parties openly articulate their distrust, they challenge aspects of the prevalent order. It becomes evident that something is not working from the point of view of the distrusting party. Thus, distrust can lead to "critical moments" (Boltanski & Thévenot, 1991/2006), in which the status quo of coordination and its legitimacy become debatable. If the other party takes the openly articulated doubt on board, this gives momentum to "reflexive coordination"; it sparks governance processes (Hofmann, Katzenbach, & Gollatz, 2014; Straßheim 2009). In this respect, distrust can become a productive source of change. For instance, it may well be argued that it was calculus-based distrust with regard to the abuse of market power that drove network operators in the US to demand that internet interconnection be included in the FCC Ruling about "Protecting and Promoting the Open Internet" (Wheeler, Clyburn, Rosenworcel, Pai, & O'Rielly, 2015) and therefore that the regulator be granted a role in the resolution of disputes.

With regard to internet exchanges, experiences of distrust have made it necessary for the community to find ways to increase the exchanges' legitimacy. Internet exchanges have started to reflect on their governance models and seek to increase their trustworthiness for members. Associations like EuroIX or the recently founded OpenIX have evolved. They respond to distrust by promoting standardisation of internet exchanges, fostering best-practice documentation, creating opportunities for knowledge-sharing and generally facilitating more transparency around internet exchanges. For instance, the umbrella organisation Euro IX is developing a platform that integrates internet service provider data from the wiki-like PeeringDB with real-time data from all participating internet exchanges so that all exchanges can benefit from this aggregated information. Also, organisations like PCH or ISOC have been quite active in propagating internet exchanges and offering further codyfied knowledge in the form of best-practice write-ups for internet exchanges that are in the course of formation around the globe. Remaining distrust against the current routing systems drives networkers to continuously improve their internal monitoring systems. It lets them support community initiatives brought forward by the Regional Internet Registries for collaborative measurement such as the RIPE Atlas and engage in the development of a validation mechanism for routing (ideas revolve around using a resource public key infrastructure, see also Hall, Clayton, Anderson, & Ouzounis, 2011). And finally, identification-based distrust of "bad actors" who damage the global routing system strengthens mechanisms for rapid informal coordination among networkers worldwide – from informal trust groups, to well-maintained, semi-public channels for real-time communication between networkers around the globe, to alert systems like the recently announced alert service BGPStream[16].

16. https://bgpstream.com/

These examples show that the absence of overarching formal regulation of internet interconnection does not mean that there are no rules. In fact, in internet interconnection institutionalisation is happening in a bottom-up way, catering in its forms to the decentralised character of the internet. Informal rules and conventions among networkers counter uncertainty and transform distrust into spheres of trust so that uncertainty is mitigated and cooperation prevails more often than it fails. That said, uncertainties and distrust in internet interconnection remain, sometimes leading to outages or disputes between interconnection counterparts. These conflicts should not be downplayed. But regulatory initiatives are well-advised to take a close look at the practices of interconnection and at the global, informal structures and conventions that exist before taking action.

5.2 Global micro-structures at the core of the internet

This study has taken a micro-social perspective. It takes the practices of networkers as a starting point to develop an understanding of coordination in internet interconnection. So it is reasonable to ask to what extent interpersonal relationships between networkers and their interaction can be related to a global order. How does the above analysis of interpersonal trust and distrust allow us to infer insights about a social order that directly relates to the large-scale distributed systems of the internet?

Cetina & Bruegger's concept of *global microstructures* (2002) offers a theoretical vantage point that allows us to put the empirical results in a global perspective. Cetina & Bruegger analysed global financial exchange markets from a micro-social research perspective. They found evidence for a distinct type of social interaction order, which is represented by brokers world wide. This order is "global in scope but microsocial in character" (2002, p. 905). Several micro-structural patterns characterise it. Among these are most importantly "reciprocal interlocking of time dimensions among actors" (2002, p. 944) and the fact that actors are constituted through their role as observers of a common object. The patterns lead Cetina & Bruegger to affirm that brokers experience shared situations and act intersubjectively – although they are distributed across the globe. In the concept of global microstructures technology plays a pivotal role. The network creates both the common object that is being watched and it is the channel of communication that enables coordination.

Parallels to internet interconnection are easy to see: The previously mentioned chat channels (p. 8) show how a significant number of networkers from all time zones sign on in the mornings and off in the evenings, handing over the watch like in a change of guards. They constitute their agency by observing the internet through their monitoring systems, by trading knowledge and acting upon the very infrastructure by way of controlling traffic flows.

Cetina & Bruegger emphasise that a global interaction order of this kind can be limited in social bandwidth. It can work in the absence of sophisticated regimes and or-

ganisational structures. Internet interconnection certainly qualifies as such a field; it is only under patchwork control.

> "(...) global social forms – by which we mean fields of interaction that stretch across all time zones (or have the potential to do so) – need not imply further expansions of social complexity along the lines of highly differentiated organizations or complex social control and authority structures. Rather, the installation of global social forms that are not nationally bound would seem to be largely dependent on individuals and social microstructures. Perhaps it only becomes feasible at all in relation to such structures." (2002, p. 5)

What Cetina & Bruegger insinuate, has potential implications for internet governance. If internet interconnection is supported by social microstructures; and if it can be assumed that the absence of national regulation or overarching organisational structures characterises an enabling environment for global social forms, then the formalisation and institutionalisation of internet interconnection are likely to put pressure on such informal structures. This points to a legitimate question: do the informal rules and sanctioning mechanisms in internet interconnection ensure a good trajectory for the future development of internet connectivity? To answer this question, more empirical research about informal rules and decision-making processes in this field is needed.

6. Bibliography

Beckert, J. (2005). Trust and the performative construction of markets. *MPIfG Discussion Paper 05/8, SSRN 2465811.*

Beckert, J. (2007). Die soziale Ordnung von Märkten. In *Märkte als soziale Strukturen* (pp. 43-62). Frankfurt/Main: Campus Verlag.

Boltanski, L., & Thévenot. (2006). *Princeton Studies in Cultural Sociology: On Justification. Economies of Worth.* Princeton And Oxford: Princeton University Press. (Original work published 1991)

Boltanski, L., Chiapello, E., & Elliott, G. (2005). *The new spirit of capitalism.* London; New York: Verso. Retrieved from WorldCat.

Cetina, K. K., & Bruegger, U. (2002). Global Microstructures: The Virtual Societies of Financial Markets. *American Journal of Sociology*, *107*(4), 905-950. Retrieved from Google Scholar.

Geertz, C. (1973). Thick description: Toward an interpretive theory of culture. In *The interpretation of cultures: Selected Essays* (pp. 537-56). Basic Books.

Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *The America Journal of Sociology*, *91*(3), 481-510. Retrieved from http://www.jstor.org/stable/2780199

Granovetter, M. (2001). A Theoretical Agenda for Economic Sociology. In *Economic Sociology at the Millenium.* New York: Russel Sage Foundation.

Hall, C., Clayton, R., Anderson, R., & Ouzounis, E. (2011). Inter-X: Resilience of the Internet Interconnection Ecosystem-Full Report. *Inter-X: Resilience of the Internet Interconnection Ecosystem* (Vol. 239) [Full Report] (Full Report). Brussels, Belgium: European Network and Information Security Agency (ENISA).

Hofmann, J. (2015). Constellations of Trust and Distrust in Internet Governance. In *Report of the Expert Group 'Risks of Eroding Trust - Foresight on the Medium-Term Implications for European Research and Innovation Policies (TRUSTFORESIGHT)'.* Brussels: European Commission.

Hofmann, J., Katzenbach C., Gollatz K. (2014). Between Coordination and Regulation: Conceptualizing Governance in Internet Governance. Presented at "2014 GigaNet Symposium, Istanbul". Retrieved from: forthcoming

Lewicki, R. J., & Tomlinson, E. L. (2014). Trust, Trust Development, And Trust Repair. In P. T. Coleman, M. Deutsch, & E. C. Marcus (Eds.), *The handbook of conflict resolution : theory and practice* (3rd ed., pp. 104-136).

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998a). Trust And Distrust: New Relationships And Realities. *Academiy of Management. The Academiy of Management Review*, 483-458.

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998b). Trust And Distrust: New Relationships And Realities. *Academiy of Management. The Academiy of Management Review*, 483-458.

Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006a). Models of Interpersonal Trust Development: Theoretical Approaches, Empirical Evidence, and Future Directions. *Journal of Management*, *32*(6), 991-1022. doi:10.1177/0149206306294405

Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006b). Models of Interpersonal Trust Development: Theoretical Approaches, Empirical Evidence, and Future Directions. *Journal of Management*, *32*(6), 991-1022. doi:10.1177/0149206306294405

Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006c). Models of Interpersonal Trust Development: Theoretical Approaches, Empirical Evidence, and Future Directions. *Journal of Management*, *32*(6), 991-1022. doi:10.1177/0149206306294405

Mathew, A. J. (2014a). *Where in the World is the Internet? Locating Political Power in Internet Infrastructure.* Doctoral dissertation. Retrieved from http://www.ischool.berkeley.edu/files/ashwin-dissertation.pdf

Mathew, A. J. (2014b). *Where in the World is the Internet? Locating Political Power in Internet Infrastructure.* Doctoral dissertation. Retrieved from http://www.ischool.berkeley.edu/files/ashwin-dissertation.pdf

Meier-Hahn, U. (2015, Februar 5). Internet Interconnection: Networking in Uncertain Terrain [Web log post]. Retrieved from https://labs.ripe.net/Members/uta_meier_hahn/internet-interconnection-networking-in-uncertain-terrain

Richter, P., Smaragdakis G., et al. (2014). Peering at peerings: On the role of IXP route servers.

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive research design concepts and processes.* New York: Routledge. Retrieved from http://site.ebrary.com/id/10545530

Sowell, J. H. (2012). Empirical studies of bottom-up Internet governance. TPRC The Research Conference on Communication, Information and Internet Policy.

Sowell, J. (2013). Framing the Value of Internet Exchange Participation. Presented at "TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy". Retrieved from: http://ssrn.com/abstract=2241841

Straßheim, H. (2009). Governance als reflexive Koordination. In S. Botzem, J. Hofmann, S. Quack, G. F. Schuppert, & H. Straßheim (Eds.), *Governance als Prozess* (Schriften zur Governance-Forschung ed., Vol. 1). Retrieved from 10.5771/9783845215723

Sztompka, P. (1997). *Trust, distrust and the paradox of Democracy*. Wissenschaftszentrum Berlin für Sozialforschung (WZB). WZB Discussion Paper.

Wagner, B., & Mindus, P. (2015). *NoC Internet Governance Case Studies Series: Multistakeholder Governance and Nodal Authority - Understanding Internet Exchange Points*. Retrieved from https://cihr.eu/wp-content/uploads/2015/01/Wagner_Mindus_IXPs_NoC1.pdf

Weller, D., & Woodcock, B. (2012). Internet Traffic Exchange: Market Developments and Policy Challenges. *OECD Digital Economy Papers*, *No. 207.* doi:10.1787/5k918gpt130q-en

Wenger, E. (1998). *Communities of practice : learning, meaning, and identity.* Cambridge, U.K. ; New York, N.Y.: Cambridge University Press. Retrieved from Library of Congress or OCLC Worldcat.

Wheeler, Clyburn, Rosenworcel, Pai, & O'Rielly. (2015). Protecting and Promoting the Open Internet. *Protecting and Promoting the Open Internet* [Report And Order On Remand, Declaratory Ruling, And Order] (Report And Order On Remand, Declaratory Ruling, And Order). Washington, D.C.. Retrieved from http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf

Williamson, O. E. (1993). Calculativeness, Trust, and Economic Organization. *Journal of Law and Economics*, *36*, 453-486.

Zuckerman, E. (2015).*The system is broken – and that's the good news* [Keynote at re:publica Conference]. from https://www.youtube.com/watch?v=CJAJ8CNAT3A