How is trust defined in Internet governance organisations?

(Applied Ethics in not-for-profit Internet organisations, managing critical Internet resources – a case study on Trust)

Desiree Zeljka Miloshevic Evans

Contemporary Diplomacy

A dissertation presented to the Faculty of Arts in the University of Malta

for the degree of

Master in Contemporary Diplomacy with specialization in Internet Governance

2015

L-UNIVERSITÀ TA' MALTA

UNIVERSITY OF MALTA

DECLARATION

I hereby declare that this dissertation is my own original work and I have acknowledged any use of published or unpublished works of other people.

Desiree Zeljka Miloshevic Evans

5th May 2015

Belgrade, Serbia

ACKNOWLEDGMENT

I would like to thank my family and my supervisor, Dr Jovan Kurbalija for his support and guidance. In addition I would like to thank Dr Alison Powell, Dr John Earls, Dr Stefaan Verhlust, and Dr Jesse Sowell for their continued interest in the topic of my research, Dr Goran Milovanovic for discussing aspects of data analysis, all members of the Regional Internet Registries (RIR) community that completed the survey as well as to management of five RIRs for their cooperation and interview time.

DEDICATION

To all my patient friends.

ABSTRACT

Trust has emerged as a central issue in Internet governance (IG). It impacts the activity and setup of organisations, dictates user attitudes to institutions and technology and, in the era following the Snowden revelations is a key topic of discussion in many international forums. In this dissertation a specific group of important global IG organisations with distributed governance systems called Regional Internet Registries (RIRs), that manage allocation of global Internet resources namely the IP addresses and AS numbers are studied to discover the answer to our question: How the concept of trust is operationalised in their activities? The investigation is built from a comprehensive appreciation of how trust has traditionally been analysed in social science literature combined with research into the history and evolution of IG itself. The concepts developed were then applied to the RIRs through surveys and discussion with active members and stakeholders, and the results enabled the development of a concise framework of trust indicators that the author believes can contribute to the current worldwide debate on trust in IG, and form the basis of further investigations into this important and fascinating field. The framework tests showed that the concept of how trust is acted upon within the RIRs has similarities to many membership-based not-for-profit organisations, but it pointed to much specificity too. Members of studied IG organisations perceive the role of the board and relationship of their organisation with the wider Internet community as critical for continuing to have trust in the organisation, a non-transparent act of an organisation as potentially most damaging to trust, followed by external regulatory threats and deviation from policies while at the same time, in general, arguing for transparency and a slightly more conservative business predictability value over organisational core mission.

TABLE OF CONTENTS

DECLARATION

ACKNOWLEDGMENT

DEDICATION

ABSTRACT

TABLE OF CONTENTS

CHAPTER 1 - Introduction

CHAPTER 2 - Literature Review: What do we know about trust?

CHAPTER 3 - The origins of trust in the Internet community

CHAPTER 4 - The crisis of trust in Internet organisations and Internet governance

CHAPTER 5 - Research Design

CHAPTER 6 - Findings, Data Analysis, Discussion and Comparisons

CHAPTER 7 - Conclusions

ABBREVIATIONS AND ACRONYMS

REFERENCES & BIBLIOGRAPHY

APPENDIX A – SURVEY QUESTIONS

APPENDIX B – FULL SURVEY RESULTS

CHAPTER 1

Introduction

This chapter explains why trust is relevant to Internet governance (IG) institutions, and how it has an impact on their everyday operations. It demonstrates that trust has a value to organisations and explains the motivation for analysing how it is therefore defined and acted upon in specific Internet governance institutions.

The Internet governance space is very important and complex. It deals with critical issues such as development, access, use, ownership and regulation of global communication infrastructure and networks known as the Internet, and the world's economies depend upon it operating effectively. Today the global network has close to 3 billion users connected to it as well as many billions of devices. However the majority of users, some 75% or 2.1 billion are located in just 20 countries.

Internet governance is a key element of the bigger picture of how the Internet will be further developed and deployed, and what norms and regulations will be put in place either to fragment it or keep it open. The future of society therefore depends not only on the Internet's technical development and its local deployment, but also on Internet governance acts with regards to new norms and regulations, and Internet governance institutions. In other words, lack of trust and overregulation may stifle and freeze any technical innovation and lead to further fragmentation of the global network.

Today an important watershed moment in the history of Internet governance can be observed. It is not currently known if the Internet as a network and platform operated today will continue to be trusted by Internet users and by stakeholders who want to regulate it and/or who operate it, and if it will continue to successfully develop at a pace that could get another 4 billion people online in a not too a distant future. At the same time it is observed that the recent Snowden revelations created a huge volume of distrust among Internet users and various stakeholders on a global level, but also may serve as an opportunity to constructively address and improve the underlying issues of trust, and the way the Internet and Internet governance will develop.

Informal communication between members of society plays an important role in how individuals make decisions, particularly when it relates to the discussion of how trustworthy certain behaviours or characteristics are. The manifestation of trust in society at different levels plays a very important role and impacts various different interactions in political, social, cultural and economic arenas.

The Internet's ubiquitous presence and increasing reach in the 21st century has made it technically easier to monitor individuals and organisations. It is arguably possible to make better judgements on how much to trust different entities due to the greater transparency online and increased ability to interrogate the accuracy of pledges, promises and statements.

The impact on the trust in different organisations of the Internet and Internet-enabled technologies over time is therefore important to consider. In general there has been an observed decrease in trust in different organisations in recent years. Trust fell in businesses (from 59% to 57%), Non-Governmental Organisations (NGOs) (from 66% to 63%) and the media (from 53% to 51%) between 2014 and 2015 according to the Edelman Trust Barometer (2015). Only trust in governments rose during this time (from 45% to 48%), but they were

still perceived as the most untrustworthy form of organisation in the study.

These figures indicate that the greater levels of transparency that the public has access to today are tools or mechanisms helping them to both navigate through the maze of trust issues and to make better decisions on who, and who not, to trust. They also demonstrate that there is a need to consider how to increase trust in various organisations, including NGOs which are the focus of this research, if it can be shown that trust plays an important role in their activity and success.

The function of organisational trust

Zak and Knack (2001) explained a clear correlation between societal trust and economic strength. This shows that trust in organisations, institutions and businesses that contribute to overall economic success at some level has an, at least indirect, impact on Gross Domestic Product (GDP). Different societal and cultural structures have also been observed to impact economies due to their approach to trust. Fukuyama (1995) argued that more successful economies and family businesses are observed in societies with greater interpersonal trust.

These assertions are intuitive; complex projects, such as those required to generate economic prosperity, involve numerous actors with specific responsibilities who must all collaborate to achieve success. Trust is essential in such processes, enabling greater levels of cooperation in many different sectors (Porta et al, 1996), including Internet governance.

The issue of trust in Internet governance

The large-scale information transfer and sharing abilities of the Internet is essential to its use in all manner of different sectors, making trust in the technology of paramount importance to

different stakeholders. Trust is vital to enabling everything from the provision of government services to entire national populations, to enabling secure financial transactions for a small local business. The institutions involved in governing the technology that enables such activity have an impact on the trust in the technology itself, and therefore the trust that is placed in these organisations is therefore a viable concept to research.

In any exploration of trust in this field scholars try to outline a holistic trust model of the Internet, and the components of this can include trust in systems, trust in people and trust in processes. While the first will be addressed in Chapter 3, major focus will be given to the two latter components and those will be considered in this dissertation to study trust in organisations.

It is also important to consider not only how trust is gained but also how it is lost, how it dissipates and how it is regained, as all four issues have an impact on the activity of an Internet governance organisation.

There are two additional reasons for researching how trust is manifested and operationalised in Internet governance institutions. Firstly the unique structure of the various forums and groups involved in the field make different demands on their members to traditional institutions in terms of trust (discussed in Chapter 3), and secondly the 2013 Snowden revelations have had a significant impact on trust in the Internet, giving significant context to this research (discussed in Chapter 4).

How can trust in Internet governance institutions be evaluated?

The question of trust in Internet governance institutions has not explicitly been defined as there are many facets to it; however one important aspect would imply that it would relate to

the rule of law and legitimacy, regarding IG processes and mechanisms.

The term IG institutions is currently also not comprehensively defined either but it is very flexible. A broader term would include various organisations and forums where a wide range of topics relating to Internet governance are being discussed, such as regulation of the Internet and control of online environment (Brown and Marsden, 2013), and therefore any instances of global, regional and local Internet Governance Forums (IGFs) which are not legally incorporated.

Internet governance institutions are still in development so any new global initiative where important Internet governance principles are being developed or declared jointly by stakeholders, such as the NetMundial principles for example which include Human Rights issues, stand a chance of turning into a recognised Internet governance initiative or an institution one day, if a sufficient level of trust is reached among stakeholders, leaders and proper use of understood trust mechanisms and processes.

For the purpose of this study on trust, a narrow definition of Internet governance institutions is used – which includes only entities that actively manage parts of Internet architecture such as global Internet resources (such as Internet addresses, domain names and protocol numbers and parameters), and who practice or adhere to a bottom-up policy development process (PDP). This is the definition referred to throughout this dissertation when Internet governance organisations are considered. A functioning and trusting system within a technical organisation is studied; a system that functions based on how the different pieces operate together, and due to the specialization of different operations.

As is discussed further in Chapter 2 – a complete objective and rigorous analysis of trust is not possible, as there is no widely accepted definition with which an empirical

analysis may be carried out. Therefore, in order to better understand the implications of trust issues in selected institutions, an approach combining the study of different indicators of levels of trust, and an investigation into the processes by which trust is developed, was used.

The research detailed in this dissertation focuses on one subset of IG organisations with specific set of norms, the so-called Regional Internet Registries (RIRs) that are used as a proxy to study trust in Internet governance organisations. The research will focus on, and is limited to, trust in these not-for-profit organisations, and the aim is to determine:

- How is trust defined and acted upon in the chosen organisations?

- What can be learned from the approach - both in terms of how to refine the methodology itself and how the organisations investigated (and similar institutions) can increase trust or better use trust information in their activities?

It is not the goal of this dissertation to measure the level of trust in an organisation, but instead to explore frameworks in specific settings by which trust can be investigated. The approach taken to research the concept of trust and achieve the above aims is detailed in Chapter 5, with the results discussed in Chapter 6 relating to Regional Internet Registries (RIRs).

RIRs are not-for-profit member organisations that manage the allocation and registration or assignment of Internet number resources within a particular region of the world. The Internet number resources in consideration include Internet Protocol (IP) addresses (IPv4, IPv6) and Autonomous System (AS) numbers, which are necessary for the effective global operation of the Internet.

The RIRs play an important role in day-to-day operation and development of the Internet. They manage global resources in a decentralized way on a local and regional level on five different continents, and this requires a lot of global coordination among RIRs. They have also become active stakeholders in Internet governance discussions by frequently providing expert opinion as the voice of the technical community of the Internet. The RIRs manage important global resources and their members have entrusted them with that role and the requisite authority to them early in the process of the formation of each individual RIR.

The RIRs differ from each other on how they go about organising their activities. This study was approached by defining and validating the kinds of trust indicators used, such as the level of trust in relationships, as well as looking at existing trust processes that exist today in these organisations. However it was important to bear in mind that the RIRs do not have the same sets of trusting relationships or processes in place, so they cannot be directly compared in all cases.

The IP addresses are a global resource and can be observed as common pool resources, so it may be helpful if RIRs are considered as organisations that manage social capital at the local or regional level – where the definition of social capital is expected collective or economic benefits through an ability of an organisation to make a credible commitment to a set of agreed policies, norms or rules, such as regulations determining that IP addresses are allocated and assigned according to the demonstrated needs.

The notion of "social capital" is used;

"to be able to analyse the social world as an accumulated history that cannot be reduced to a sequence of mechanical equilibria (Bourdieu, 1992, p. 49). Bourdieu defines social capital as the totality of all actual and potential resources associated with the possession of a lasting network of more or less institutionalized relations of knowing and respecting each other (Bourdieu, 1992, p. 63)" (Birner and Wittmer, 2003).

The technical community, including the RIRs, has often approached issues from the

point of view that aspects of the Internet that work successfully do not need to be overly considered or changed, a principle known as technological incrementalism. The approach of only fixing problems incrementally when they arise is orthogonal to technological determinism. This activity is often characterised by a sentiment attributed to Vinton Cerf, one of the founding fathers of the Internet; "if it ain't broke, don't fix it" (McCullagh, 2004).

Trust issues pertaining to technological incrementalism and the now "cliché" phrase – "if it ain't broken don't fix it" are often wrongly perceived as technological determinism by other stakeholders outside RIRs in the IG ecosystem. Organisations such as the RIRs can be studied on many levels (including social, psychological and philosophical), and analysed in areas such as the relationship between different stakeholders in the Internet governance ecosystem, or forums in general, and the roles they each play to build trust. Other areas can include relationships between the technical community and business, the technical community and civil society, or the technical community and states. In addition, the set of trusting relationships between different IG institutions may also be studied.

When the Internet, as a global network platform, began to be widely discussed in meetings convened by intergovernmental organisations, such as the UN, for the first time, this technological incrementalism might have created an element of stigma, and raised the question whether policy makers with no technical background or expertise, e.g. an NGO or a government stakeholder, should be part of any technical discussions that have policy implications. There were questions over whether their advice and opinions could be trusted.

Members of the technical community have often been praised with not having a political orientation, but they have been observed as a group which favours meritocracy and technocracy.

Technical community meetings within RIRs almost always run with "an open door policy" meaning that anyone with an interest in the topic *can* be at the policy decision making table in presence or contribute online, rather than an approach that determines all and every stakeholder *should* be at the table at all stages of a decision making process, the so called "equal footing" multistakeholder model.

The technical community however has not always been able to play a role in all relevant policy discussions. During Phase I of the World Summit on Information Society (WSIS) governments did not accept any additional stakeholders in the room when discussing public policy issues pertaining to the Internet. How informed could their discussion have been without the expert opinions of the technical community?

After Phase II of the WSIS, the role of stakeholders in public policy discussion was better defined as per the following, with the Geneva Resolutions and Tunis Agenda providing significant clarity on stakeholder roles:

- States were given a sovereign as policy authorities,
- Day to day 'technical and operational matters' . . . 'that do not impact on international public policy issues, role was assigned to business'
- Civil society was understood to have 'played an important role on Internet matters…at the community level'

In his presentation, Muller (2013) explains that this division of the roles of the stakeholders does not work, as it is impossible to separate public policy issues from technical and operational matters: "also the 'public' in the 'public policy' referenced by states is transnational, not national, therefore states are inadequate representatives of the global public."

Lessig (1999) wrote in his "The Code is the Law" on inseparability of technical issues with policy issues. He argued that technical code writing or programming happens automatically as a part of permission-less innovation, and the way the code is written affects its legal or normative aspects, e.g. sets boundaries and permissions.

However, it is also worth noting that the Internet's technical community has not always been particularly focused on explaining why the public should actually trust the systems and technology of the Internet. Likewise it has not been universally successful in transferring the trust that is inherent or implied in the engineering approach that *"isn't broke"* to the people, organisations and political processes that underpin it. Or, where they have been successful, such as in an epistemic technical community like the Internet Engineering Task Force (IETF), which is an Internet standards body organisation that believes in consensus and the running code, there have been challenges to the approach that may be useful to study.

While trust in technology may not be transferrable to people, there are implicit trust independencies in the Internet's functioning systems that need research to further understanding of how trust is defined.

For those reasons the RIRs are highly appropriate research objects. The five RIRs studied are:

- **African Network Information Centre (AFRINIC)** for Africa - http://www.afrinic.net
- **American Registry for Internet Numbers (ARIN)** for the United States, Canada, several parts of the Caribbean region, and Antarctica - https://www.arin.net
- **Asia-Pacific Network Information Centre (APNIC)** for Asia, Australia, New Zealand, and neighbouring countries - http://www.apnic.net

- **Latin America and Caribbean Network Information Centre (LACNIC)** for Latin America and parts of the Caribbean region - http://www.lacnic.net
- **Réseaux IP Européens Network Coordination Centre (RIPE NCC)** for Europe, Russia, the Middle East, and Central Asia - https://www.ripe.net

The research into these organisations will enable a better understanding of how trust is understood, built and considered in their daily activity. The RIRs have also been chosen as they play a critical role in the Internet's ongoing operation and stability, and because their structure and activity is representative of many organisations in Internet governance, and so conclusions drawn from the investigation into trust in these organisations could potentially be extended to other institutions and actors in the field.

Now that it has been explained why a consideration of trust is important and relevant to Internet Governance institutions, the next chapter summarises previous research and thinking about trust relevant to this topic area.

CHAPTER 2

Literature Review: What do we know about trust?

Trust is an important aspect of our everyday lives, and determines how we engage with organisations, how we consider individuals and how we characterise everything from relationships to finances. Over two hundred years before the birth of Jesus Christ the Romans placed such a high regard in the concept that they even worshipped a goddess of trust known as Fides, whose temple was near to that of Jupiter in Rome.

In seeking to assess how trust is observed in the identity and activity of Regional Internet Registries (RIRs), and how this may impact their work and be extended to other Internet governance institutions, it is important to determine if there is a satisfactory definition or understanding of trust to use as a basis for investigation.

A thorough investigation in the topic of trust shows that there is no universally agreed upon definition of trust - and this very issue has been looked at closely (McKnight and Chervany, 1996). Instead, trust in different settings and in different varieties and amounts has been widely investigated. In this chapter a number of those selected definitions are explained along with how they may be applied to the dissertation study of RIRs.

Introduction to definitions of trust

What we know today about trust comes from various branches of science, such as psychology, and philosophy. Philosophers such as Kant (Kant, 1797), Hobbs, Putnam and Rousseau (1762) have produced much of the key thinking in this area.

Trust also has strong links with ethics and other social constructs. Hardin for example discussed the social concept of *encapsulated trust* (Hardin, 2002, p.1), stating that:

"*I trust you because I think it is in your interest to take my interests in the relevant matter seriously in the following sense. You value the continuation of our relationship, and you therefore have your own interests in taking my interests into account."*

Hardin also makes an important differentiation between the trust and trustworthiness (Hardin, 2006), explaining that trust is a positive belief that does not need to be proven whereas trustworthiness is an earned quality, representing someone reliable, proven and honest.

Hardin's example trustworthiness criteria show the challenges of combining different notions and characteristics of trust into a common definition, something attempted by Misztal (Misztal, 1996). Misztal set out three basic functions of trust in everyday life; creation of a sense of community, making social life predictable and enabling people to work together. Considering trust as a fundamental element of human interaction and behaviour is observed in much of the social theory literature on the topic (Sztompka, 1999).

In general it can be observed that there are well meaning individuals in which we can place our trust, or that there are organisations that put public interest or the notion of social capital before, or overlapping with, their own interests, that can be trusted to carry out certain tasks according to the set of agreed rules and not deviate from them.

Social situations in which trust has an important role are also understood and discussed in terms of game theory by economists. Game theory offers concepts that help us better understand trust in this way, such as the iterated prisoner's dilemma for example.

In this problem the classic prisoner's dilemma is played by several participants repeatedly, and transactions between group members that require trust and cooperation over time can be modelled. It is also known as the "peace-war" game (Press and Dyson, 2012) and demonstrates another theoretical setting in which trust relates to behaviour that has applicability to our topic of study.

In addition, traditional thinking on trust and its role in society also impinges on how organisations should operate. Gandhi for example discussed and advocated *trusteeship* as the basis for how those in positions of wealth or power should operate and behave (Gandhi, 1957).

This consideration of organisational trust (i.e. trust in a group, company or institution), and the extension of existing thinking and definitions of trust in different contexts to an organisation's structure and activity, provides the theoretical foundation for the specific research into trust in RIRs in this dissertation, observed in understanding trust indicators and processes, described in Chapter 5.

Interpersonal and organisational trust

Trust between people can be understood in a variety of ways, and is very dependent on the situation. Trust can be understood as the amount of risk one party takes on when expecting another to perform a specific action, or the reliability one has that another party will perform

some action.

However, if another party is legally required to carry out the action expected of them, then this can impact the trust in them. It is valid to question whether the party would carry out the action were they not legally required to, and if the answer is no then it can be said that one party *trusts* the other to perform the action (as they are legally obliged to) but still may not find them *trustworthy*.

As an extreme example; it can be said that it is possible to trust that a proven violent criminal will murder an enemy given the opportunity, and yet said criminal would be described as far from trustworthy - that is to say, would certainly not be trusted in a different situation.

It is therefore important that situations and conditions are taken into account in the determination of a workable understanding of trust that can be used to investigate the RIRs. It has also been shown for example that trust and distrust/fear take place in different function areas of the brain - meaning that one cannot both fear and trust a party at the same time (Dimoka, 2010). As the investigation into RIRs is a broader study than considering an individual's response under a certain set of conditions, this point is not as relevant as others, showing that judgement must be used in extending definitions too far.

Instead, a useful definition of interpersonal trust to begin considering has been developed by Bamberger (2010) based on combined examples in literature and the work of Kassebaum (2004), and has been stated as follows:

"Interpersonal trust is an expectation about a future behaviour of another person and an accompanying feeling of calmness, confidence, and security depending on the degree of trust and the extend of the associated risk. That other person shall behave as agreed, unagreed but loyal, or at least according to subjective expectations, although she/he has the freedom and

choice to act differently, because it is impossible or voluntarily unwanted to control her/him. That other person may also be perceived as a representative of a certain group."

To use this explanation of trust to analyse RIR organisations, the "other person" who is expected to provide some defined future behaviour would be one of these organisations. In this case the organisation, if they were trusted by a consumer (member, user, stakeholder etc.), would:

- Carry out the future behaviour expected of the member/consumer,
- Do so in a manner that makes the member consumer feel calm, confident and secure,
- Behave as agreed – according to agreed norms and credible commitment made,
- Or if behaving as not agreed, do so in transparent manner to provide justification for the behaviour, while maintaining loyalty,
- Or at least behave according to subjective expectations of the member/consumer,
- Carry out such behaviours despite the fact that consumer/member does not have the power to directly control it (e.g. legal obligations to disclose data to a consumer do not necessarily build trust in an organisation - things may be different if the organisation were not legally bound).

Another definition of fundamental trust by Mayer et al (1995) building on work of Kee and Knox (1970) is stated as:

"The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party."

Although similar to Bamberger's definition of interpersonal trust, the idea of **vulnerability** as well as **expectation** is emphasised. If it is considered that one of the *"parties"* described is an Internet governance organisation and the other is a consumer; then in this case the consumer, if they trusted the organisation, would be willing to be vulnerable

to the actions of the organisation - based on the expectation that the organisation would perform a particular action important to the consumer - regardless of the consumer's ability to monitor or control the organisation.

The examples above show the important role that trust plays in the proper functioning of society, helping human beings to agree on how they organise world experiences and how they communicate with and view the world. Lack of trust in other people, in communication media and/or in our ability freely express ourselves and exchange ideas, can all prevent effective communication, leading to a negative impact on progress in society. On the Internet this issue translates to a lack of privacy, further demonstrating the importance of considering trust in relation to Internet governance.

Trust is also an important concept in diplomatic negotiations and treaties, whether between multilateral organisations, in state-to-state bilateral agreements, business negotiations, or arrangements between intergovernmental organisations and state actors. There are many examples of diplomatic relations in which trust has played an important role, particularly between countries of different sizes, such as the relationship between the US and Israel and agreements between the UK and its Commonwealth partners.

In International relations, superpower relationships are often understood in terms of a concept known as "trust but verify." This defines a situation in which parties only build, or rebuild, trust when statements are backed up by verifiable deeds. This shows further the importance of trust, as it can make the difference between the war and peace. As Khydd (2005) states:

"I define trust as a belief that the other side is trustworthy, that is, willing to reciprocate cooperation, and mistrust as a belief that the other side is untrustworthy, or prefers to exploit one's cooperation".

It is in considering these issues and understanding the array of definitions described above that the basis of a theoretical understanding of trust that can be applied to the RIRs, detailed further in Chapter 5, may be formed.

Internet and technology-specific definitions

Alongside the characteristics and research on interpersonal and organisational trust detailed above, it is also important to consider other areas in which trust is manifested in the Internet.

As was noted in Chapter 1, one of the key challenges to Internet governance institutions is to extrapolate or translate the trust that is widely held in the technology they manage, e.g. in the internet architecture and administer to the organisations themselves. It is therefore important to consider this formulation of trust also.

Grandison and Sloman (2001) explained that trust is an important aspect of decision-making relating to internet applications, particularly in the specification of security policy. In this context they gave the definition of trust as *"the firm belief in the **competence** of an entity to **act dependably, securely and reliably** within a specified context."*

Another example of trust in a purely technical setting concerns certificate authorities (CAs), also known as called trusted third parties (TTP), which vouch for entities that are linked to their public key with digital certificates (DeNardis, 2014, p. 95):

"A basic governance question is what makes these third parties sufficiently trustworthy to vouch for the digital identities of web sites. This is a classic problem of infinite regress in that someone has to instil trust in the entity that certifies trust in another entity that certifies trust in a web site, and so forth."

In addition, the European Commission Joint Research Centre have defined trust with

relevance to technical situations as *"the property of a business relationship, such that **reliance** can be placed on the business partners and the business transactions developed with them"* (Jones, 1999).

Trust issues manifest in the Internet also encompass the open movement. The open movement consists of various initiatives inspired by the success of Open Source software (Open Source Operating Systems: GNU/LINUX, Ubuntu etc.) such as Creative Commons, Open Data, Open Science, Open Access, Open Government etc. This particular movement is specific to the Internet and an area in which **trust and transparency** are also important (Lerner and Tirole, 2002).

The open movement also considers different software licenses such as Berkeley Software Distribution (BSD) and General Public Licence (GPL) that vouch for the openness of the source code in which software is written (that can be read and copied, modified or improved, documented and published). This is an example of how software, hardware and infrastructure are also important fields in which to consider trust issues, and the extension of that to trust in the Internet as a medium/system.

Conclusion

This chapter has described how trust is dealt with and discussed in a wide range of settings and literature. The concepts and descriptions of trust as found in philosophy and ethical political discourse, described by Kant and others, game theory, social and ethical issues, as discussed by Gandhi and others, and in technical or non-technical definitions described above will be applied specifically to an analysis of RIRs.

In order to achieve such an analysis it is important that the theoretical concepts described in this chapter are understood alongside the origins of trust and trust issues in the internet community - the organisations, institutions and businesses that have a significant effect on the Internet - and this is the topic of the next chapter.

CHAPTER 3

The origins of trust in the Internet community

This chapter relates the explanations and descriptions of trust detailed in Chapter 2 to the history of Internet organisations and events, explaining how trust issues have evolved over time and their importance and relevance to the development of the Internet.

Who is the Internet community?

The term local Internet community appears in the IETF's Request for Comments (RFC) 1591, whereas the global internet community today is meant to include close to three billion users. The term Internet technical community started being used more formally around WSIS and during formation of Internet Governance Forum, recognising it as a stakeholder together with academia, civil society, international organisations, governments and private sector. The term described by the Internet technical collaboration group (ISOC, 2014) says that the community *"consists of individuals and organizations from around the world that understand the global Internet as a complex interaction of technology, standards, implementation, operation and application"* (Internet technical collaboration group).

An examination of the beginnings of the IETF's early technical and academic community shows that principles that have enabled and sustained the development of the Internet since its inception have included the following: permission-less innovation, inclusive participation, consensus-based decision-making, transparency, collective stewardship and collaboration, and voluntary standards adoption.

The various individuals, institutions, groups and organisations that are broadly understood to make up the Internet technical community still adhere to these principles.

Trust in the system - self regulation

Trust in the Internet as a medium, or as a Transfer Control Protocol/Internet Protocol (TCP/IP) form of network, was drawn from a diverse and wide network of small groups of individuals and organisations that have worked together since the technology's early beginnings to connect new academic and private networks, locally and internationally, and to coordinate the day-to-day operations and development of the Internet. Such organisations include the University of California Los Angeles and Santa Barbara, the Stanford Research Institute and the University of Utah (Hafner and Lyon, 1998).

When non-US based institutions such as NORSAR in Norway joined the early packet switching project ARPANET, it could be said that the lab experiment was complete. Other organisations such as the Internet Engineering Task Force (IETF), a standards body organisation, continued the development of Internet protocols such as simple mail transfer protocol (SMTP) and many others (ISOC, 2013).

Therefore the trust in the system could not have been drawn from any single international organisation, although an Open Systems Interconnection (OSI) protocol was developed that made an attempt to create an interoperable network protocol by several European government organisations. Instead, trust in the Internet has developed from trust in early adopters and small epistemic communities that worked in internet technology sectors and developed the system as part of a job or hobby.

Although Internet "colonisation" (connecting large parts of the globe to the Internet)

was complete by end of the 1990s using satellites, fixed telephone lines, and new and existing undersea cables, the Internet was developed to run independently on top this infrastructure and therefore be self-regulated. The observed rules and norms and their enforcement therefore have deep roots in private sector self-regulation.

Trust in the coordination of unique global identifiers

Trust in Internet governance or how the Internet is governed can be drawn from, and is somewhat a by-product of, existing coordination and collaboration of many private networks of organisations that are involved in the daily operation of the Internet. On 9/11 for example the Internet continued to work with no interruptions - while other communications networks such as telephone did not, or were stopped manually, which contributed to it being seen as a more resilient and trusted form of communication. Trust can be drawn not just from the technical argument that it works some 99% of the time or some higher network availability, but the fact that organisations and individuals choose to interconnect with each other. As mentioned in the earlier chapter, the cost of not interconnecting can be also observed as trust interdependency created by the network effects.

Therefore organisations that administer not only some critical parts of Internet's infrastructure, such as names (country code Top-level Domains (ccTLDs) and generic Top-level Domains (gTLDs)) and numbers databases (RIRs), protocol port and parameter numbers (such as IETF and Internet Assigned Numbers Authority (IANA)) and root server operators, all make a contribution to the overall trust held in the Internet, as they have an impact on the repeated experience of the Internet running by their best efforts (ISOC, 2014). Other organisations with a similar role include Internet service providers (ISPs), Internet Exchange Points (IXP), Network Operator Groups (such as the North American Network Operators Group (NANOG) or South Asian Network Operators Group (SANOG)) that are in charge of

maintaining a secure routing table, or anti-abuse working groups such as the Messaging Anti-Abuse Working Group (MAAWG).

Because of this vast and distributed ecosystem of suppliers, global users on the Internet do not draw their trust in the technology from any single international or national constitution, nor is their trust placed in specific intergovernmental agencies. Hofman (2015) has shown that users do not extend trust to Internet governance organisations from international organisations such as the International Telecommunication Union (ITU).

Users and members of such organisations also determine their own levels of trust through the use of credible commitment as a source of generalized trust. This can be observed in the development of open standards by organisations such as the IETF. The Internet standards are developed in an open process and their acceptance is voluntary not mandatory, meaning that there is scope to attribute greater trust to the output. The majority of technical organisations in the Internet community also operate with a defined charter or mission that incorporates their credible commitment and gives them the authority to run parts of the system.

Mapping of Trust

Trust in the Internet and Internet-enabled technologies, products, organisations, services, etc. is a complex and multifaceted issue. It covers areas such as:

- Trust and e-commerce (e.g. E-bay, PayPal)
- Trust and technology - reliability, resilience, performance, security
- Trust in technology, car, etc.
- Trust in Internet organisations

- Trust in Internet stewardship
- Trust and cyberspace
- Trust in Internet governance
- Trust – privacy, distrust and rise of dark networks

It is important to separate issues relating to trusting the Internet itself, trusting private organisations offering services relating to the technology, and trusting those organisations who are critical to running and maintaining it - particularly the RIRs that are the focus of the research, and are involved in the coordination and management of unique identifiers necessary to operate a secure internet, part of the Internet's core architecture. Consider online payments for example:

- People's trust in using PayPal has gradually grown enough for it to be a widespread means of sending money using the Internet.
- But PayPal, as a global payments provider, is obviously subject to Internet governance issues at a variety of levels, and so itself must rely on and trust certain organisations that impact its data and operations; such as its domain name service provider and the underlying internet DNS protocol that provides a paypal.com naming address. PayPal must trust its operation that it would be resolved globally under an accurate IP address for any user on the global network.
- Do the end users of PayPal therefore trust the IG organisations by extension? They cannot monitor what PayPal's interactions are with these organisations, or how their data is used and shared, but must still act as if they trust in PayPal's commitment or judgement in governance issues in order to continue to use it.

There are also trust issues observed in services and systems simply due to the fact that they are accessible to and used by others; this is very evident in the Internet. Early adopters

may have a role to play in building initial levels of trust in services, and it is also important to ask what users can actually do if they lose trust in a system that holds their data. Additionally, as mentioned in the literature review, trust *ex ante* as opposed to trustworthiness – *ex post* - involves risk taking. Therefore it can be observed that trust is mostly invisible until something breaks. It is challenging for an average Internet user to make a connection where exactly the breach of trust takes place if the data was lost, within a particular company for example, and so see beyond the intricate set of trust security interdependences in the Internet ecosystem and make the link, if appropriate, to governance institutions and its processes.

All of these examples demonstrate why trust is such a central issue on the Internet. The value of trust in the Internet is high (although as has been discussed, this depends on the situation and setting of each interaction) and trust in internet technology is impacted on by trust in those governing it. So it is important that they are part of the discussion moving forwards.

The evolution of Internet governance

Trust has played a central role in Internet governance organisations, which have been characterised as initially being part of a relatively small community (relative to the number of end-users of the Internet and Internet-enabled products and services) with a high academic influence.

This has led to there being implicit trust in many organisations and activities which at the outset can be understood in terms of Swift Trust Theory (Meyerson, Weick and Kramer, 1996), whereby trust is initially assumed between partners so that projects can be started or developed rapidly.

Over time however, Internet-enabled networks and cooperatives have grown in power, influence and importance (Ronfeldt, 1996), evolving from informal, self-organising groups to more formal organisations today. It is therefore useful to understand how the Internet community has developed, so a brief overview of important Internet governance milestones is included below, based partially on work by DeNardis (2010):

1986 - the Internet Engineering Task Force (IETF) was established. Operating with a unique collaborative governance structure (no legal structure) and the motto known as "rough consensus and running code" the IETF manages technical aspects of the Internet's development, such as standards development.

1989 – trust and ethical issues are present in many early conversations and working groups relating to internet technologies including the Internet Activities Board (IAB, 1989) and IETF. RFC 1087 in particular discussed Ethics and the Internet.

1992 - the non-profit Internet Society (ISOC) was formed with the aim of voluntary interconnection of global networks (ISOC, 2013) and supporting the work of open Internet standards development and the work of the IETF, as well as being tasked with informing members of society of the Internet's global and regional growth and evolution.

In April, Réseaux IP Européens Network Coordination Centre (RIPE NCC) was formally established as the first Regional Internet Registry (RIR).

1994 – greater involvement by national governments and businesses began to change the IETF's decentralised governance approach (Kurbalija, 2014). In addition, the backlash from the United States (US) National Science Foundation's (NSF) decision to sub-contract control of the Domain Name System (DNS) to a private sector company Network Solutions led to a

period of friction in the Internet community, known as the 'DNS War' (Simon, 2006).

Also in 1994 the Internet Assigned Numbers Authority (IANA) publicly recognised the Asia-Pacific Network Information Centre's (APNIC) status, delegating the IPv4 address ranges 202/8 and 203/8.

1995-1997 – as the Internet continued to grow it became necessary to introduce more generic Top-level Domains (gTLDs) to account for the increasing pressure and need for new website addresses. As a result of extensive debate on the Internet's operational and technical communities, the International AD Hoc Committee (IAHC) was formed in order to manage the introduction of seven new gTLDs, and subsequently dissolved.

Also in 1997 the American Registry for Internet Numbers (ARIN) was established as the second regional RIR.

1998 - Following the release of a white paper in 1998 by the National Telecommunications Information Administration (NTIA), the International Forum on the White Paper (IFWP) was convened to discuss issues that the white paper raised. These included internet security, privacy, management of the DNS and similar topics.

To better manage the establishment and accreditation of new domain registrars the US Department of Commerce (DOC) established the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN carries out much of its activity through IANA which coordinates the allocation and assignment of three sets of unique global identifiers: namely Domain names (DNS), Internet Protocol (IP) addresses and autonomous system (AS) numbers, and protocol port and parameter numbers.

2001 - the Latin American and Caribbean Internet Addresses Registry (LACNIC) was established in Uruguay.

2002 – the structure of ICANN was substantially altered (Lynn, 2002).

2003 – in Geneva, the first of two phases of the United Nations (UN) sponsored conferences, known as the World Summit on the Information Society (WSIS), was held. Because of lack of agreement between governments on how the Internet is being governed, and the predominant role of the US, conference established the Working Group on Internet Governance (WGIG) supported by several bodies including International Telecommunication Union (ITU), a UN agency involved in managing a variety of information and communication technologies.

The four existing RIRs (APNIC, ARIN, LACNIC and RIPE NCC) also entered into a Memorandum of Understanding (MoU) with ICANN and formed a coordinating body known as the Number Resource Organization (NRO).

2004 - the African Network Information Centre (AFRINIC) was incorporated in Mauritius.

2005 - the WGIG developed a detailed report on emerging Internet governance issues for the second WSIS in Tunis (Drake, 2005). The conference produced a written agreement known as the Tunis Agenda for the Information Society which resulted in the creation of the Internet Governance Forum (IGF), a pioneering multistakeholder organisation that would bring together participants from academia, civil society, business and government.

In addition, ICANN accredited AFRINIC as the fifth RIR, and it was then subsequently incorporated into the existing RIRs' MoU with ICANN and joined the NRO.

2006 - the first IGF meeting was held in Athens.

2008 - network neutrality (the concept of treating all internet data as being equal, or for not charging the content provider extra for their bits to be delivered to the end user over telco's networks) became an important topic of debate between Internet companies such as Yahoo!, Facebook and Google who supported its adoption, and telecommunications and Internet Service Providers (ISPs) who opposed it.

2009 - at the fourth IGF meeting in Egypt the future of the organisation was discussed with a debate over whether there should be greater UN and state involvement.

An Affirmation of Commitments between ICANN and the US DOC was also concluded, giving ICANN greater independence (Kurbalija, 2014).

2010 - Google closed its search operations in China after clashing with government authorities over access rights. This was carried out despite solving some earlier government operational requests in 2006, where search terms such as "democracy" or "Tiananmen square" were made to not produce search results but instead show searchers a warning page explaining that that such searches were not allowed.

In addition, the UN Commission on Science and Technology for Development (CSTD) opted to continue the IGF for another five years.

2011 - social uprisings in the Middle East and North Africa took place, known as the Arab Spring. The use of social media for organisational and political purposes on both sides of the uprisings was heavily debated in their aftermath.

2012 - ICANN introduced several new generic Top-level Domains (gTLDs), receiving over 1900 applications (Kurbalija, 2014). In addition, led by the ITU, the 2012 World Conference on International Telecommunications (WCIT-12) in Dubai resulted in amendments to the globally binding International Telecommunication Regulations (ITRs). This was the first time the ITRs had been amended since 1988.

2013 - Edward Snowden leaked thousands of classified files acquired from the National Security Agency (NSA) whom he had worked with as a contractor whilst employed by both Dell and consulting firm Booz Allen Hamilton. The files included evidence of global surveillance programs run by various national government agencies and other organisations.

The Snowden revelations in 2013, and their subsequent impact on an Internet governance has led to a crisis of trust in internet issues and in some IG organisations. This is discussed in the next chapter.

In addition, a variety of Internet community stakeholders, including participants from ISOC, the UN, the ITU and several countries attended the multistakeholder World Telecommunication Policy Forum (WTPF) event.

2014 - a wide variety of experts and stakeholders attended the Global Multistakeholder meeting on the Future of Internet Governance (NETmundial) event in São Paulo, Brazil. The impacts of the Snowden revelations and Human Rights were a key topic of discussion at the event.

In addition, the 9th UN IGF meeting was held in Istanbul. One of the main sub-themes at the event was an in-depth consideration and set of discussions on digital trust, and on the

restoring of trust in Internet governance.

Multistakeholder approach to Internet governance and trust

The governance of the Internet as discussed above is characterised by new term called multistakeholder dialogue and multistakeholder cooperation. A large number of technical experts, end-users and businesses are involved in setting agendas alongside policy-makers in the various forums and discussion arenas. This almost unique set up could result in more trust between members and stakeholders, as their voices and opinions can be heard and considered.

The 2013 IGF meeting in Bali featured many debates about the concept of multistakeholder approach to Internet governance. Various models or approaches were discussed. The first was a WSIS version where all stakeholders participate on an equal footing and are involved in all stages of the decision-shaping process (e.g. have a seat "at the table") at the IGF, but are not separated by their roles and responsibilities, as discussed in Chapter 1.

The other approach is one where all stakeholders are involved in the decision-making process at different stages, and it could be said that this is the operational model of ICANN. That model has not been operationalised in any intergovernmental organisation but operationally implemented at ICANN, where the balance seems to work. At ICANN the Governmental Advisory Committee (GAC) alongside the At-Large Advisory Committee (representing Internet users) comments on all Generic Names Supporting Organisation (GNSO) policies.

Therefore the so called multistakeholder approach to IG, practiced more often among the Internet not-for-profit internet governance organisations, allows participation to all interested parties or stakeholders, to have "a seat at the table" but not being required to

provide input at all stages in the decision-making process, particularly if they do not have enough knowledge or interest. This model emphasises necessary flexibility in the roles of interested parties and ability to participate. It is no surprise for example that governments do not view themselves as having the same rights in public policy-making as other stakeholders.

This approach also favours openness and inclusiveness over a rigid framework. Examples of this model are standards bodies such as organisations the IETF, which is an open organisation where anyone can join the Working Group. The IETF does not draw its legitimacy from the multistakeholder model directly, but from the participants in it and the way in which they interact. It endorses principles of open and inclusive participation and its standards are developed based on working group consensus, collective stewardship, transparency and voluntary adoption.

The IGF itself has created a venue for an annual interaction among stakeholders that otherwise would not necessarily come into contact with each other. It would be an interesting extension of this and other studies to determine whether there are indicators that repeated interaction among stakeholders would result in more trust, or whether repeated interaction means that stakeholders have learnt to work together without trust in their own silos.

At many IGF meetings sweeping generalisations and comments are made along the lines of: 'it is difficult to trust corporate stakeholders as they are only accountable to their shareholders.' However, while this is not an accurate description of the dynamics between stakeholders but someone's opinion based on *ex ante* trust experience, it is illuminating with regards to the task at hand and the bridges that ought to be built among all stakeholders, in the aim of achieving an open and interoperable internet.

Of course, business's agendas can change rapidly as management or the board may set

different directions and objectives. It is not new to hear about the lack of trust that this can lead to when businesses interact with other stakeholders. It is important to ask whether this can lead to entrenched opinion or biases coming to bear in discussion forums. Businesses, as opposed to not-for-profit membership organisations, are sometimes unable to contribute to long term benefits and make a credible commitment in the way that leads to greater trust in this area.

Trust in multi-lateral relations vs trust among stakeholders

When the multistakeholder cooperation enables dialogue rather than debate, it provides more transparency in the process of decision-making and therefore later on can enable greater buy-in of policies by stakeholders.

Within ICANN there are more and more countries that have become members of the Government Advisory Council or GAC. States have increasingly participated both in UN IGOs and in ICANN.

With greater involvement by states it is important to consider their opinions on the multistakeholder model (MSM) in operation. Within multilateral organisations, there are clear lines of responsibility and accountability of states as actors, because state representatives are directly accountable to those who elected them. In the MSM the question of trust and accountability is not so clearly defined, but greater involvement in organisations such as ICANN that do operate in this way (in GAC processes and RIR roundtables for example) does indicate a greater appreciation of the value of the MSM approach.

ICANN has survived as an organisation, and is seen as successful, while operating with an MSM and increasingly with states. Therefore it can be argued that states are

increasingly seeing the value in the MSM and therefore the trust issues and processes that are involved in it. Waz and Weiser (2013) described "Endorsement, recognition or direct participation by sovereign governments" as an identified characteristic, value, or best practice of multistakeholder organisations, further emphasising the important role that trust between stakeholders of all kinds plays.

Trust as decentralization of the Internet/Power

By its nature, control of critical Internet resources is decentralised – however there are some centralised areas such as the management of names, numbers and protocol and parameter databases, but however they too are further globally distributed. Any stakeholder can run such a database but their success is an issue of judgement and earned trust in managing the facilities so far without any deviations. A multistakeholder approach is also used to manage many key areas, so it is important to consider what role trust plays in the processes.

Beckstrom and Lambsdorff (2008) state that;

"In an age of globalization and rising levels of complexity, trust now takes the place of classical working relationships and must increasingly act as the glue for all kinds of organizations."

Trust is seen as key enabler therefore - without it we would expect to see the multistakeholder process fall apart.

These ideas show that higher levels of trust are required as globalisation and decentralisation increases and issues are observed in a global vs. national setting. Yet it is also decentralisation itself that could result in more trust, if it is seen as non-disruptive in key areas, and is implemented by stakeholders that are culturally aligned to embed the practices and thinking in their activity.

Ultimately, decentralisation of key internet functions, like those performed by the five regional RIRs, results in a separation of powers by traditional stakeholders and resists the unilateral accumulation of power by a single entity. As this increases, the value of trust and approaches used to consider it in everyday activity become more important, and provide motivation for this research.

However, any implementation or analysis of trust must consider the immediate context and environment of each sector, and in the current post-Snowden stage we are actually witnessing a crisis of trust in the governance of the Internet. This is covered in the next chapter.

CHAPTER 4

The crisis of trust in Internet organisations and Internet governance

This chapter discusses how key events that have impacted the evolution of trust in internet-related organisations and processes detailed in the previous chapter have led to the crisis of trust in certain areas.

As mentioned in Chapter 2, in 2013 an IT contractor working for the National Security Agency (NSA), called Edward Snowden, leaked thousands of classified files to the global media. The files were acquired by Snowden in his time contracting for the NSA whilst employed at Dell and consulting firm Booz Allen Hamilton.

The leaked material included a large volume of in-depth information on surveillance programs that were run by a number of national government agencies, and other organisations, on a global scale. The revelations provoked international outrage, and led to widespread scrutiny of the privacy and data management processes and protocols of various private companies, government departments in the US, Europe and elsewhere, and other organisations connected with the leaked details (Naughton, 2015).

The perceived erosion of trust in the organisations connected with the Snowden revelations has been an important area of debate since the events of 2013. More topically, 2014 and 2015 being the years of post-Snowden revelations, the awareness of lack of trust of the actual use of the Internet as a communication medium is also more widespread.

Post-Snowden there is much discussion on how trust has been derailed, and how one government (according to the information contained in the leaks) may have such power when it comes to mass surveillance.

Mistrust and scepticism in the US government has been affected by various perceived breaches in trust relating to the contents of the Snowden leaks. For example, it has been stated that the Obama Administration, through the National Security Agency (NSA), has:

"tapped into the central servers of nine leading U.S. internet companies, extracting audio and video chats, photographs, emails, documents, and connection logs that enable analysts to track foreign targets and U.S. citizens." (Glennon, 2014, p.3)

It should be noted however that the Snowden revelations relate directly to a loss of trust in nine major US companies who worked together with the US government and gave it access to private data. This does not necessarily translate to a loss of trust in Internet governance institutions nor in RIRs, all RIRs data is publicly available, but more to a loss of trust in how the internet can operate effectively as a communications medium with the perceived lack of privacy, with associated impacts on the scope and activity of IG organisations.

This response can be observed in the 2014 CIGI-Ipsos Global Survey on Internet Security and Trust, undertaken by the Centre for International Governance Innovation (CIGI) conducted by global research company Ipsos. The survey reached over 20,000 Internet users in 24 countries between October 7, 2014 and November 12, 2014 and acquired the following results (Centre For International Governance Innovation & Ipsos, 2014):

- Two thirds (64%) of users are more concerned today about online privacy than they were compared to one year ago; and,

- When given a choice of various governance sources to effectively run the world-wide Internet, a majority (57%) chose the multi-stakeholder option — a *"combined body of technology companies, engineers, non-governmental organizations and institutions that represent the interests and will of ordinary citizens, and governments."*

A decrease in trust has also been observed in other areas that have traditionally been important to communication and the development of culture, such as traditional news outlets (Mendes, 2013). The hardware and software on which various internet resources depends is also a key issue (CCCen, 2014).

It is also important to note that the Snowden revelations form only one part of the debate on trust in the Internet and Internet governance. The scale and importance of the international use of the Internet means that issues relating to cybercrime and cybersecurity are also very evident, particularly in business for example as the following statistics demonstrate:

- The estimated cost of cybercrime to the global economy is $400 billion, which is 0.8% of global GDP (Center for Strategic and International Studies, 2014).

- 3% of global organisations reported a loss of $1 million or more due to cybercrime incidents in 2013 (Mickelberg, Schive and Pollard, 2014).

- 59% *"of respondents said that they were more concerned about cybersecurity threats this year than in the past"* (Mickelberg, Schive and Pollard, 2014).

- 49% *"of respondents reported that they were worried about the impact of cyber threats to their growth prospects"* (Mickelberg, Schive and Pollard, 2014).

- 82% of global companies with high performing security practices stated that they *"collaborate with others to deepen their knowledge of security and threat trends"* (Mickelberg, Schive and Pollard, 2014).

As has been shown, the descriptions of the crisis of trust in Internet governance indicate that there is a clear need to examine this concept further, and to attempt establish a means for determining the level of trust in order to improve.

The next chapter details a proposed mapping system of trust in Internet governance institutions that can be applied in a specific context to move towards achieving this aim. Rather than looking at more abstract or higher level issues of trust in Internet governance, as in the rule of law and legitimacy, or as an overview of the diverse array of IG institutions, this study is instead looking at the live, functioning system of IP address allocation and assignment and how trust is operationalised within the organisations involved in this activity.

CHAPTER 5

Research Design

This chapter details the way that the research carried out in this dissertation has been designed. The first section explains the research question that will be answered, the second explains the approach taken to collect data that will help answer the research question, and the third explains the analysis approach used to interpret and understand this data.

Based on the background reading and research into trust detailed in Chapters 1 and 2, this chapter explains how the theoretical understanding of trust may be applied to the RIRs both in terms of desk research, and through further surveys and discussion.

Research question

The research undertaken as part of this dissertation seeks to answer the questions:

- How is trust defined and operationalised in RIRs, not-for-profit membership based organisations that manage global internet identifiers IP addresses and AS numbers?
- How can the current understanding and research into the study of trust in Internet governance be improved?
- What can be learned from the approach - both in terms of how to refine the methodology itself and how the organisations investigated (and similar institutions) can increase trust or better use trust information in their activities?

Mapping trust in selected Regional Internet Registries

In 2006 the title of the Computer Chaos Club's 23rd annual conference targeted at hackers, activists, and computer and security specialists in Berlin was 'Trust'. A keynote speaker John Perry Barlow, author of Declaration of Independence of Cyberspace, said that trust is connected to the experience, but if this is absent then individuals instead rely on intuition. As each organisation is comprised of individuals, one can approach the study of trust within an organisation by studying the expression of this intuition.

In a membership-based not-for-profit organisation, one can study relationships between individuals in various settings, or by looking at trust processes followed by the head of the organisation, or its board and the executive team, therefore studying the trustworthiness of its leadership, as well as by learning about the motives for trust from members' direct experiences with the organisation.

As described later in the methodology section, an ethnographic approach would entail observing how participants are engaged in discourse or at public meetings, when operational and other reports from an organisation are being presented, as well as in the working meetings where policy is being developed.

However that would still not be sufficient for a thorough understanding of trust at the organisational level. Organisations are complex and operate with mandates, missions, and their own sets of norms and rules that impact on trust. Another method of studying trust in organisation would be to study any deviations from these agreed norms and rules, or the lack of them.

Further, approaches for studying trust could also come from the perception of

“outsiders” or individuals who are not familiar with an organisation but are presented with a set of information and facts, but have had no real engagement with them or are not familiar with organisation’s reputation. In absence of direct experience, reputation as a building block of trust can be observed especially in the press. It may also be possible to consider the perceptions and experiences of those from a different cultural background, or those who operate with a different set of morals. However, this methodology was beyond the scope of the research.

Trust is perceived differently by different stakeholders. For example, Law Enforcement Agencies (LEAs) place trust in the Internet ecosystem if they are able to access or decrypt communications for their investigative purposes. On the other hand, users trust the Internet if they are able to maintain an anonymous status online, and/or keep emails, messages and data encrypted and private. Diplomats also rely on confidentiality for all critical communication.

With this in mind, it is also important to note that at an organisational level there is little common ground to investigate as the five RIRs differ from each other in how they go about organising their activities. While this study was approached by defining and validating the kinds of trust markers/indicators that would be able to be applied across the different organisations, such as trust in relationships, as well as existing trust processes they have in place, the fact that the RIRs are organised and operate differently means that the most common denominators in the analysis approach were observed by studying certain basic sets of relationships that exist in those membership organisations.

It was therefore necessary to narrow the scope of the investigation to the live system of IP address allocation and AS numbers, and seek to determine how trust is operationalised within the RIRs in areas related to this activity.

Mapping of trust in RIRs - Trust framework

In this specific situation, Internet organisations who are in charge of the coordination of the technical elements that make the Internet work as a network of autonomous networks are considered.

It is observed that because of its global aspect of dealing with global resources, some common interests of RIRs or Network Operator Groups overlap with public interests. Common interests in the integrity of the numbers delegation and routing system incentivised early cooperation that has evolved into the respective RIR and network operator group ecosystems. As such, the Internet has become an increasingly critical infrastructure, as is characteristic of infrastructure with, broadly, an increasingly diverse set of public, private, and social goods which are facilitated by a global infrastructure whose numeric identifiers and route dissemination mechanisms are rooted in these common resource management institutions.

Given the implications of the institutions' management roles in the public interest, the resource managers have concomitantly growing shared interests with actors (typically state actors) formally charged with ensuring end uses of Internet resources do not harm the public interest. These shared interests are not always clear, as they lie in the multitude of common resource management policy and public policy.

Based on Sowell (2015), organisations that deal with assets that require global management processes, whether for IP numbers or routing tables are not competing with the state for authority and do not require an intergovernmental processes for their regulation.

As discussed in Chapter 1, it is useful to think of RIRs in the same way as organisations that manage social capital – where social capital is defined as an ability to make a credible commitment to a set of agreed policies, norms or rules, such as how IP addresses or AS numbers would be allocated according to the demonstrated needs.

Therefore, in order to investigate the RIRs it was necessary to look at trust indicators and trust processes through an in-depth survey of existing members and conversations with knowledgeable RIR executives. Conclusions and discussion points were then achieved through both qualitative and quantitative analysis, and the resulting indicators of how trust is operationalised were then developed.

The observatory trust framework detailed in the conclusion was built by further refinement of existing trust (or distrust) indicators identified in social science literature detailed below, and combining them with trust processes observed within the RIRs and sets of critical governance structure relationships. The framework presented is therefore an innovation as it combines for the first time trust indicators alongside of trust processes. The different aspects of the research design are discussed in more detail below.

Trust indicators

The trust indicators investigated are levels of expressed trust or distrust in an RIR, and were developed as a result of literature research. Inspiration was also taken from the existing framework developed by GovLab (http://thegovlab.org/) - a centre at New York University Polytechnic School for Engineering. Based on the Harper's Index (http://harpers.org/) GovLab have developed the GovLab Index on Internet Governance (http://thegovlab.org/the-govlab-index-on-internet-governance-trust/), a series of indexes that focus on the five main areas within Internet governance: access, content, code, trust, and trade. The trust index looks

at cybercrime, cybersecurity and preparedness, providing a variety of facts and figures.

The Edelman Trust Barometer (2015) was also reviewed, particularly its definition of trust: *"Trust is defined as "how much you trust the institution to do what is right". Respondents grade their level of trust on a scale of 1 to 9."*

For this study, trust indicators were defined to examine various sets of different bilateral, leadership, management, and community relationships that exist in RIR membership organisations (e.g. relationships among groups of actors from both within and outside the organisation i.e. with other stakeholders) to measure trust processes, such as transparency and accountability. The trust indicators chosen for investigation were based on literature examples detailed below:

Expertise-based indicators

- **Risk** - how at risk do you feel your users' data/money/resources etc. are when with you? (Coleman, 1990)
- **Competency** - do your users believe that you are competent in your area of expertise? (Grandison et al, 2001)

Reputation-based indicators (Colquitt et al, 2007)

- **Integrity** - do your users believe that use ethical business practices?
- **Responsibility** - do your users believe that you operate responsibly as a good corporate citizen?

Transparency-based (Mishra, 1993)

- **Honesty** - do users believe you communicate honestly?
- **Openness** - do users believe that you communicate openly?

- **Engagement** - do users believe that you engage often enough and listen to them?

These trust indicators were studied through the prism of certain sets of relationships existing in RIRs. Prioritising or measuring the importance of relationships is an indicator of where or how trust is being monitored, exercised, developed or broken. The study involved investigating the relationships between:

- Members and the Board
- Members and the RIR organisation
- Among members
- Relationships between RIR and the wider Internet community
- RIR and LEAs
- RIR and Governments

In order to study observed levels of trust in this set of relationships, and ascertain attitudes to the activity of RIRs regarding a survey of acting members was carried out.

Survey approach

A combination of qualitative and quantitative research questions were used in an online survey called "Trust in RIRs" that ran from March 20 until March 30, 2015. The survey questionnaire was disseminated via an online system known as SurveyMonkey (the full survey can be found in Appendix A). The questionnaire was developed and tested so as to take no than 15 minutes of the respondent's time. The choice of questions was therefore limited.

Questions were divided in the following sections:

- Section (1) on general questions on the demography of respondents;
- Section (2) on the general understanding of multi-dimensional aspects of organisational trust;
- Section (3) on trust indicators or markers (such as risk, competency, reponsibility, integrity, predictablity, business ethics, reliability, honesty (understood as open communication), and engagement);
- Section (4) on trust studied through different sets of relationships that exist within RIR and outside stakeholders, and measured by its cotextual set of trust markers;
- Section (5) on RIR trust processes;
- Section (6) on signals of how trust can be broken;
- Section (7) on overall trust perception; and
- Section (8) on recommendations how to improve or increase trust within the organisation, e.g. in terms of focus required, key relationships or governance processes.

All five RIRs, in geographically and culturally diverse regions of the world, Europe, Asia-Pacific, Africa, Latin America and the Caribbean and North America, were open for collaboration and promoted the link to the online survey to their members via their twitter accounts. A link to the survey was also sent via email to all five RIRs relevant members' mailing lists dealing with policy discussion in order to get feedback from most active members – those who are already actively involved in the policy development process within an RIR.

Additionally a blog article was written for the APNIC's website (Miloshevic, 2015) in order to generate more interest in the survey.

The survey generated 102 responses in total from all five RIRs. The majority of the

responses came from ARIN (46) and RIPE NCC (32), followed by equal numbers of respondents from AFRINIC (9) and LACNIC (9) region, and then fewer from the APNIC region (6).

There were 23 survey questions in total, 4 out of which were of socio-demographic nature and 19 on the subject matter of trust. The latter set posed questions about members' perception of trust definition within any organisation and then specifically about trust in their own RIR organisation.

Trust processes

The trust indicators investigated in the survey are considered alongside the organisational processes that define trust, such as accountability, openness, and transparency when following or changing the rules.

The trust processes are formal or informal processes or policies in place by the investigated organisation with the aim of monitoring, measuring and/or increasing trust in their activities. In order to additionally validate and investigate such trust processes, the CEOs of the five RIRs were interviewed through a set of unstructured questions.

The interviews involved more unstructured and open-ended questions on validity of questions asked in the survey and what processes and policies are in place in their organisation to monitor, measure and increase trust. This involved investigating the following areas of trust process:

- Accountability mechanisms for members and other stakeholders in the Internet ecosystem, (existing mechanisms to redress accountability issues)

- Governance structures
- Transparency in decision-making
- Consensus building
- Transparency-based (level of knowledge about RIR actions).

Other questions asked about uniqueness or similarity of RIRs to other not-for-profit membership organisations that are in charge of managing important global resources, and how organisational trust has been operationalised and managed over time.

Methodology and Data Analysis

In order to analyse the data and information collected in the surveys and discussions described in the previous section, a combination of methods were used: analytical methods of the survey questions, and interviews. The qualitative data set was too small to follow up with some of considered methodologies such as Grounded Theory.

In addition, existing theories in sociology literature such as Game Theory (Prisoner's dilemma); Theory of Social Contract (Rousseau, 1762) and Russel Hardin's Public Choice – were used to test the proposed framework of trust indicators relating to the Internet's stewardship organisations, as they involve political economy aspects as well as philosophical and psychological ones. This methodology was only used in interviews.

CHAPTER 6

Findings, Results & Analysis, Discussion and Comparisons

As has previously been asserted, trust is subjective, multi-dimensional and a property of people rather than of technology or of an organisation, therefore trust within an RIR can be analysed through the views of interviewees, in this case its membership. Therefore in general, all, or a greater majority, of the survey findings represent a subjective view of trust of the members within an RIR. Essentially, this involves an investigation into the psychological and sociological concept of trust.

Data Sample, Validity and Limitations of the Data

The validity and reliability must be considered. The total number of responses of the survey was 102. Broken down by the number of respondents, the ARIN region came first with the total of 46, RIPE NCC with 32, LACNIC with 9, AFRINIC with 9 and APINIC with 6 respondents. Therefore, the vast majority of participants were primary users of RIPE NCC's and ARIN's services (total of 76%). Only six participants indicated APNIC as their primary RIR, and only nine indicated AFRINIC and LACNIC (total of 24%). Thus, all findings from the present study should be considered as biased towards the Northern American and European users of RIR's services.

Though the aggregated data of all 102 respondents was used to analyse the findings, because of the size, the survey data gathered from APNIC region does not adequately represent the views of the members in this region. The interview with the APNIC CEO provided a useful additional data set for that region (it is also worth noting that the organisation offered to run and promote the survey again).

The data size gathered from the survey respondents is adequate for our purpose of data analysis although it is not representative of views of all 30,000 members in five RIRs. This can be seen through the example of ARIN's latest in-house survey in March 2015 that had 699 individual responses out of a few thousands of its members(see https://www.arin.net/about_us/corp_docs/customer_survey/2014.pdf). It should also be noted that the survey in this study was not sent directly to all members but only seen by those who actively read mailing lists, so 46 is a satisfactory response in terms of data size from that region.

The survey ran for 7 days in North America (ARIN), Latin American and Caribbean (LACNIC), African (AFRINIC) and Asia Pacific (APNIC) region, while it was launched three days earlier in the European, Middle East and Euro-Asian (RIPE NCC) region. The fact that the survey was featured as an external academic survey featuring a new topic, and that the ratio of responses between AFRINIC and LACNIC, and the RIPE NCC does, seem reasonable when the size of their membership is compared (AFRINIC's close to 2,000 and RIPE NCC's close 11,000). The response rate seems to be fairly proportional. Of course, the response rate could have been better if the survey ran for a longer period of time, or if it were sent directly to all the RIR members.

Findings

These findings detail results of the trust survey of members of all five RIRs.

Data Analysis of the Case Study Sample

1.A Questionnaire on Trust in RIRs – see chapter 5

Questions were divided in the following sections:

- Section (1) on general questions on demography of respondents;
- Section (2) on general understanding of multi-dimensional aspects of organisational trust;
- Section (3) on trust indicators or markers (such as risk, competency, reponsibility, integrity, predictablity, business ethics, relaiability, honesty (understood as open communication), and engagement);
- Section (4) on trust studied through different sets of relationships that exist within RIR and outside stakeholders and measured by its cotextual set of trust markers;
- Section (5) on RIR trust processes;
- Section (6) on signals how trust can be broken;
- Section (7) on overall trust perception and
- Section (8) on recommendations how to improve or increase trust within the organisation, e.g. in terms of focus required, key relationships or governance processes.

1.C Case Study Sample

Answers from 102 respondents were collected. Questions on participants' gender and age were optional. 69 participants reported on their gender, out of which only 6 were female. As for the participants' age, only 1 participant was younger than 24 years, and only 3 were older than 60, out of 72 who responded to this question.

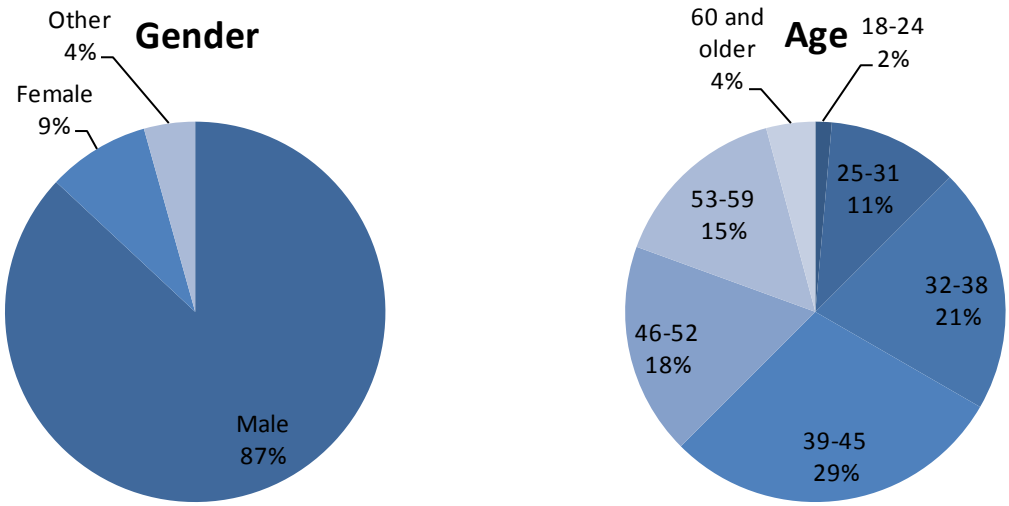


Figure 1. Gender and Age

All 102 participants have reported on their primary RIR organisation (*Q1. Please indicate the primary RIR organisation of your membership*). A vast majority of participants were primary users of RIPE NCC's and ARIN's services (total of 76%). Only 6 participants indicated APNIC as their primary RIR, and only 9 indicated AFRINIC and LACNIC (total of 24%). Thus, all findings from the present study should be considered as biased towards the Northern American and European users of RIR's services.

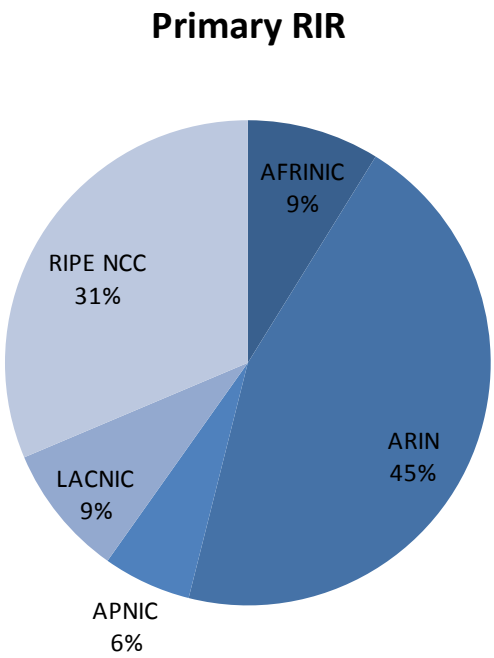


Figure 2. Primary RIR organisation

2. Results and Analysis

2.A Understanding and Perception of Trust in RIRs

The participants were first asked to select the features of a trustworthy organisation in general (*Q2. Please select all that, in your view, applies to a trustworthy organisation*). They were offered a list of statements describing the characteristics of a trustworthy organisation and asked to select all characteristics that apply. The participants have described a trustworthy organisation as the one that communicates its activities to its members promptly (79.4%, N=81), is predictable (77.5%, N=79), true to its mission (75.5%, N=77), and reliable (74.5%, N=76).

Efficiency was perceived as an important feature on the behalf of only 38.2% participants (N=39), a lower number than for good risk management (52%, N=53) and competence (66.7%, N=68). Interestingly, the features that would probably be recognised as essential from a managerial viewpoint (efficiency, good risk management, and competence) were recognised as important by a smaller fraction of participants than those that seem to describe a more 'essentialist' understanding of trust (communication of activities, predictability, holding up to its mission, and reliability).

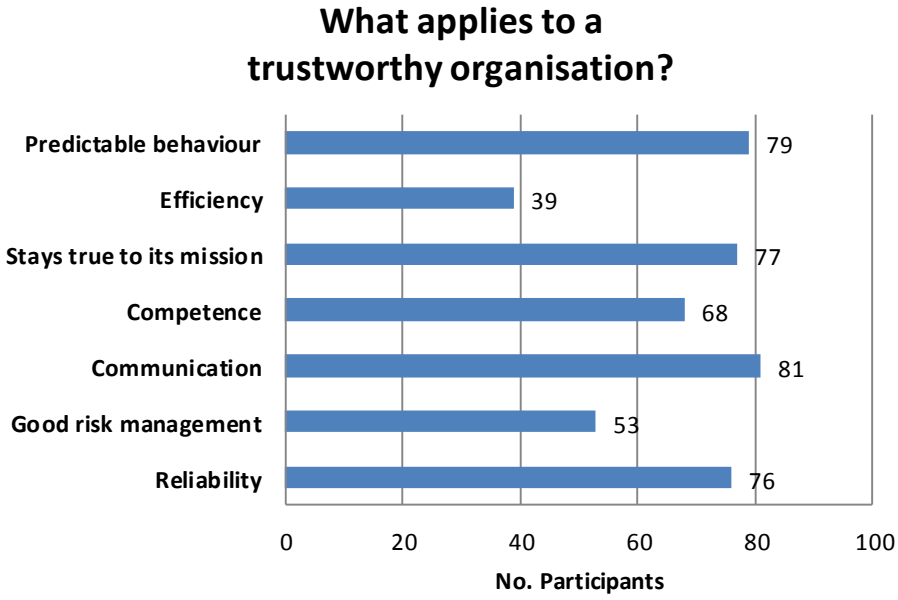


Figure 3. The characteristics of a trustworthy organisation

A set of trust indicators was used to study the structure of the understanding or trust in RIRs. Six sentences were formulated, each referring to a different important component of trust in RIRs:

	Trust indicators
1.	*I feel at risk when providing my own sensitive data to my RIR.*
2.	*People who manage and operate my RIR are competent in their area of expertise.*
3.	*I believe that my RIR operates responsibly as a good corporate citizen.*
4.	*I believe that RIRs use ethical business practices.*
5.	*The RIR organisation of my primary membership communicates transparently.*
6.	*I, as a member, have a thorough understanding of our RIR's objectives.*

Table 1. List of trust indicators in RIRs

The participants were asked to express their level of agreement with each of these sentences using a 5-point Likert scale, ranging from "*strongly disagree*" (1) to "*strongly agree*" (5), and encompassing a "*don't know*" option. One question (*I feel at risk when providing my own sensitive data to my RIR*) was negatively framed and reverse scored. 92 participants have responded to these 6 questions; Table 2 presents mean responses and standard deviations. The number of participants who gave a "*don't know*" response was never higher than 4.

	Mean	Std. Deviation	N
I feel at risk when providing my own sensitive data to my RIR.	3.58	1.38	92
People who manage and operate my RIR are competent in their area of expertise.	4.28	1.09	92
I believe that my RIR operates responsibly as a good corporate citizen.	4.13	1.22	92
I believe that RIRs use ethical business practices.	3.93	1.24	92
The RIR organisation of my primary membership communicates transparently.	3.80	1.35	92
I, as a member, have a thorough understanding of our RIR's objectives.	3.85	1.28	92

Table 2. Components of Trust in RIRs

In spite of the fact that these 6 items were not specifically planned to present a set of converging indicators for a specific latent concept of trust in RIRs, they were submitted to a reliability analysis. Surprisingly, a very high value of Cronbach's $\alpha = .91$ for a scale that encompasses only 6 items was obtained. In fact, it seems that these 6 items present a successful operationalisation of a *single* concept of trust in RIRs. A principal component analysis confirmed this: with KMO[1] = .89, and a significant Bartlett's test of sphericity, $\chi^2 = 322.58$, $p < .01$, only one component having an eigenvalue larger than 1 was extracted (Table 3), explaining a total of 67.3% of variance.

	Eigenvalue	% of Variance	Cumulative %
Component 1	4.038	67.295	67.295
Component 2	.689	11.481	78.775
Component 3	.423	7.048	85.823
Component 4	.350	5.841	91.665
Component 5	.255	4.256	95.920
Component 6	.245	4.080	100.000

Table 3. Trust in RIRs indicators: principal components analysis

An external validation of this concept of trust in RIRs was provided by a linear regression analysis with Component 1 as a predictor and a more straightforward measurement of trust provided by *Q16: Please rate the overall level of trust that you have in your RIR organisation* (assessed by a 7-point numerical scale with higher numbers indicating higher level of trust) as a criterion: $R^2 = .62$, $F(1,82) = 135.91$, $p < .01$. Another independent external validation was attempted by means of a linear regression with Component 1 as a predictor and *Q17: Please rate the overall level of trust that you have in other members of your RIR organisation* (measured in exactly the same manner as Q16). This time, the results were again statistically significant, but less encouraging: $R^2 = .13$, $F(1,82) = 11.9$, $p < .01$. In other words, the results of these two linear regressions point to the following conclusion: the concept of trust in RIRs as operationalised by the trust indicators listed in Table 1 relates to

[1] Kaiser-Meyer-Olkin Measure of Sampling Adequacy.

trust in RIRs *excluding the trust invested in other members of the primary RIR organisation* (see Figure 2). In other words, our indicators of trust in RIRs operationalise this concept specifically in relation to the RIR itself, without much significant dependence upon the perception of other organisations that primarily use the same RIR.

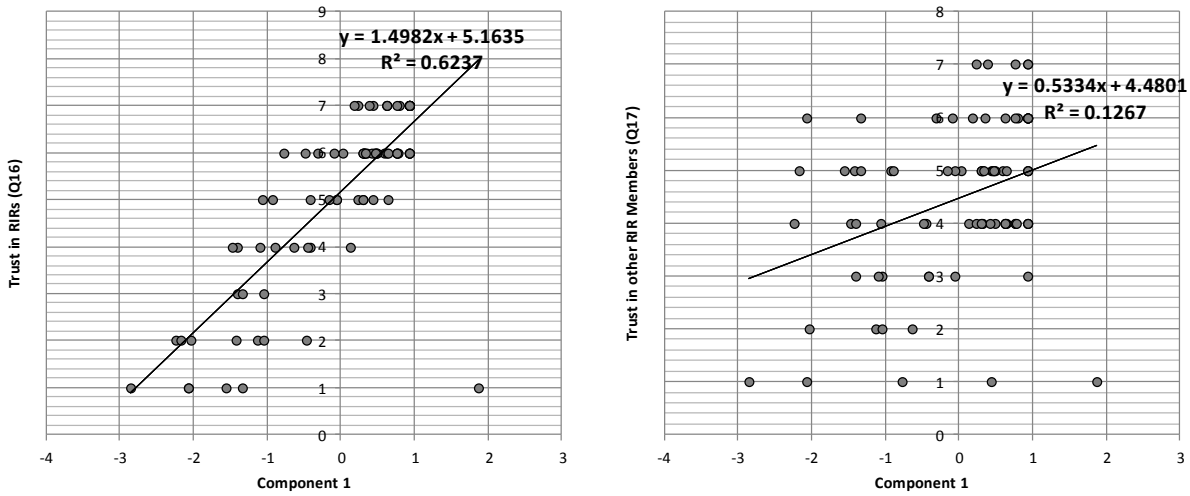
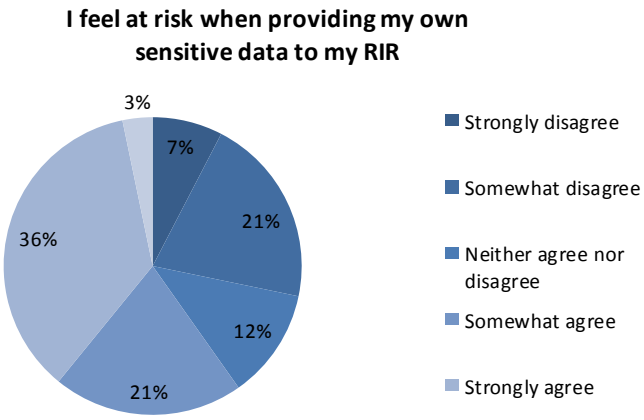


Figure 4. External validation of trust in RIR as measured by six trust indicators: (a) the relationship of trust in RIR as operationalised by the dominant principal component of the six trust indicators (Table 2, Table 3) and a straightforward assessment of trust in RIRs (Q16, left panel), and (b) the relationship of trust in RIRs from 6 trust indicators with the assessment of trust invested in other RIR members (Q17, right panel).

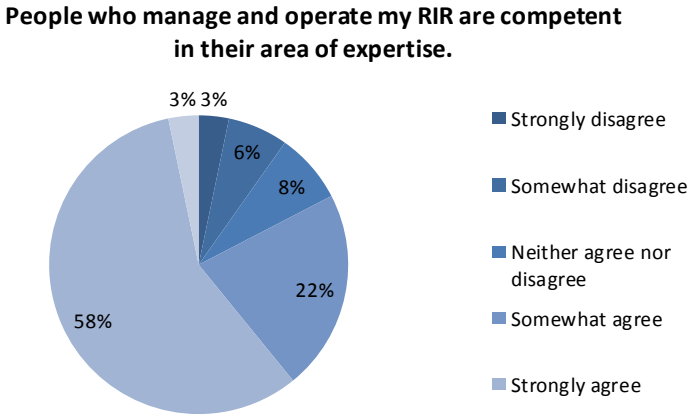
In order to find out about the contribution of individual trust in RIR indicators (Table 1) to the overall assessment of trust in RIRs (*Q16*), a multiple regression analysis with responses on trust in RIR indicators as predictors and the overall assessment of trust (*Q16*) as criterion was conducted, explaining approximately 83% of variance in the dependent variable (*Q16*): $R^2 = .83$, $F(6,73) = 57.32$, $p < .01$. In this multiple regression, the beta coefficients for the indicators of risk ($\beta = .17$, $t=2.52$, $p<.05$), competence ($\beta = .14$, $t=2.12$, $p<.05$), and responsibility ($\beta = .48$, $t=5.5$, $p<.01$) were found to be statistically significant. Thus, the perception of RIR as operating in a *responsible manner* has the most influence on the overall assessment of trust in RIRs, followed in its importance by the *perception of good risk management* and *competence*.

Six panels in Figure 3 present an overall overview of responses on six trust indicators

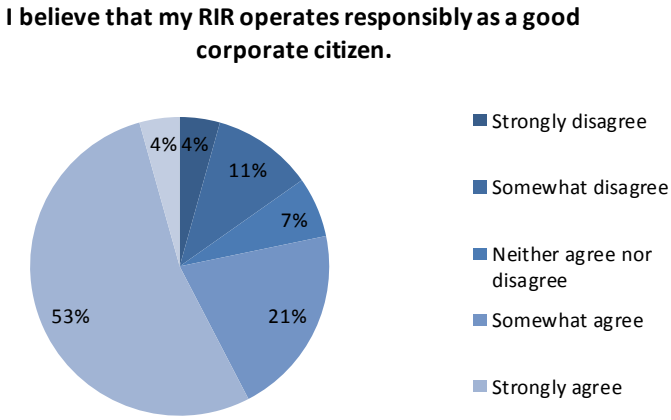
listed in Table 2.



Don't know: 3



Don't know: 3



Don't know: 4

Figure 5. Trust in RIRs indicators: responses

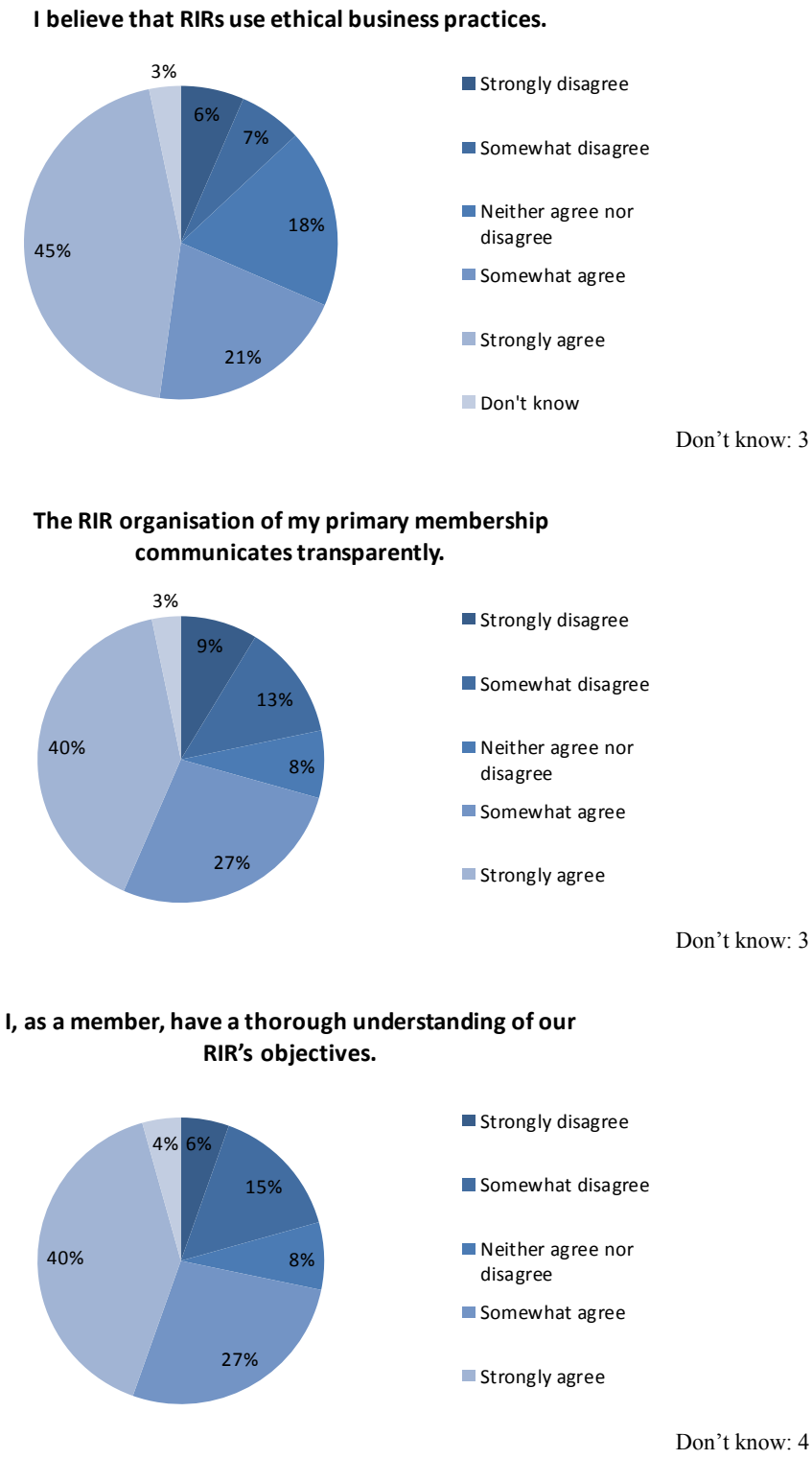


Figure 6. Trust in RIRs indicators: responses

2.B Factors of trust in RIRs

In this section, several factors of potential importance for trust in RIRs are elaborated on. Firstly the question of whether the RIR communicates effectively with its members (*Q10: Do you think that your RIR communicates effectively to its members?*) is considered. The study

focuses on the differences between the respondents that believe that their primary RIRs do and do not communicate effectively on the following variables related to the description of trust in our survey: (1) Component 1 (the dominant principal component of trust indicators, see Section 2.A), (2) raw responses on trust in RIR indicators (Table 2, 5-point Likert scales), (3) overall assessment of trust in RIR (Q16), and (4) overall assessment of trust in other members of the same primary RIR organisation. Table 4 summarises the means and standard deviations for these 8 variables.

Q10. Do you think that your RIR communicates effectively to its members?		N	Mean	Std. Deviation
Component 1	YES	59	0.36	0.63
	NO	15	-1.34	0.83
Risk	YES	58	3.91	1.23
	NO	15	2.33	1.11
Competence	YES	59	4.63	0.79
	NO	15	3.00	1.31
Responsibility	YES	59	4.53	0.94
	NO	14	2.79	1.19
Ethics	YES	59	4.39	0.87
	NO	15	2.53	1.19
Transparency	YES	59	4.46	0.82
	NO	15	1.80	1.08
Understanding objectives	YES	59	4.36	0.91
	NO	14	2.64	1.34
Trust in RIR (Q16)	YES	58	5.76	1.33
	NO	15	3.27	1.87
Trust in other RIR members (Q17)	YES	58	4.66	1.37
	NO	15	3.53	1.60

Table 4. The assessment of how effectively does an RIR communicate to its members, and nine different variables related to trust.

Even without statistical testing, it is obvious that the perception of whether the RIR communicates effectively to its members is an important factor of trust in RIR, operationalised via different variables and their combination (Component 1). It turns out that the mean responses to these different aspects of trust in RIRs are consistently higher for those participants who claim that RIRs do communicate efficiently than for those who claim

otherwise.

However, the hypothesis was tested statistically by performing nine separate Welch t-tests[2] for all variables in Table 4. Each Welch t-test assessed whether the difference in means for (a) those respondents who believe that RIRs communicate effectively and (b) those respondents who believe that they do not is statistically different or not. Table 5 summarises the results: all Welch t-tests are statistically significant.

In conclusion, if the RIR is thought to be communicating effectively to its membership, all six trust indicators, their linear combination (Component 1), as well as general assessments of level of trust (Q16, Q17) tend to increase.

Test Variable	Welch t-test	df	Sig. (2-tailed)
Component 1	7.39	18.306	.01
Risk	4.79	23.706	.01
Competence	4.61	16.647	.01
Responsibility	5.12	17.018	.01
Ethics	5.68	18.015	.01
Transparency	8.89	18.250	.01
Understanding objectives	4.56	15.943	.01
Trust in RIR (Q16)	4.86	17.821	.01
Trust in other RIR members (Q17)	2.49	19.663	.05

Table 5. Welch independent t-test for nine variables related to trust in RIRs

Next the study turns to an analysis of the impact of the perception of whether the RIR

[2] Welch t-tests were used to account for unequal variances and unequal sample sizes (i.e. a large respondents who believe that RIRs do communicate effectively vs. a small number of respondents who believe the opposite to be true).

is responsive to the information and requests provided to it by its members (*Q11*). The same methodology as in case of the previous analysis was used to answer this question. Table 6 summarises means and standard deviations, while Table 7 provides the results of Welch t-tests. The results obtained from this analysis are qualitatively no different from the results obtained in relation to whether RIRs communicate effectively, except for that whether RIR is perceived to be responsive or not is not related to the trust invested in other RIR members. Thus, whether the RIR is perceived to be responsive turns out to be another important factor of trust.

Another potential factor of trust in RIRs is related to the perception of its operations as effective (*Q12. Do you find your RIR's operations to be effective (i.e. is the RIR managed in a way to achieve its goals)?*). The same methodology as in previous cases was utilised; Table 8 and Table 9 summarise the findings; the results are not qualitatively different from those obtained in the previous analysis.

Q11. Is your RIR responsive to the information and requests provided to it by its members?		N	Mean	Std. Deviation
Component 1	YES	59	0.32	0.66
	NO	15	-1.13	1.09
Risk	YES	59	3.97	1.26
	NO	15	2.47	1.30
Competence	YES	59	4.63	0.74
	NO	15	3.00	1.41
Responsibility	YES	59	4.51	0.90
	NO	15	2.93	1.44
Ethics	YES	59	4.36	1.01
	NO	15	3.00	1.25
Transparency	YES	59	4.34	0.96
	NO	15	2.40	1.45
Understanding objectives	YES	59	4.27	0.94
	NO	14	2.86	1.61
Trust in RIR (Q16)	YES	58	5.88	1.27
	NO	15	3.20	1.78
Trust in other RIR members (Q17)	YES	58	4.66	1.47
	NO	15	4.00	1.46

Table 6. The assessment of how effectively does a RIR communicate to its members and nine different variables related to trust.

Test Variable	Welch t-test	df	Sig. (2-tailed)
Component 1	4.93	16.65	.01
Risk	4.01	21.16	.01
Competence	4.31	16.00	.01
Responsibility	4.05	16.87	.01
Ethics	3.88	18.91	.01
Transparency	4.9	17.21	.01
Understanding objectives	3.16	15.18	.01
Trust in RIR (Q16)	5.48	17.86	.00
Trust in other RIR members (Q17)	1.54	21.88	.137

Table 7. Welch independent t-test for nine variables related to trust in RIRs.

Q12. Do you find your RIR's operations to be effective (i.e. is the RIR managed in a way to achieve its goals)?		N	Mean	Std. Deviation
Component 1	YES	61	0.33	0.63
	NO	11	-1.37	0.92
Risk	YES	60	4.00	1.21
	NO	11	2.09	0.83
Competence	YES	61	4.66	0.73
	NO	11	3.18	1.33
Responsibility	YES	60	4.57	0.79
	NO	11	2.55	1.44
Ethics	YES	61	4.36	0.93
	NO	11	2.64	1.36
Transparency	YES	61	4.28	1.03
	NO	11	2.18	1.08
Understanding objectives	YES	61	4.23	1.04
	NO	11	2.64	1.43
Trust in RIR (Q16)	YES	60	5.83	1.30
	NO	11	2.64	1.80
Trust in other RIR members (Q17)	YES	60	4.68	1.42
	NO	11	3.82	1.83

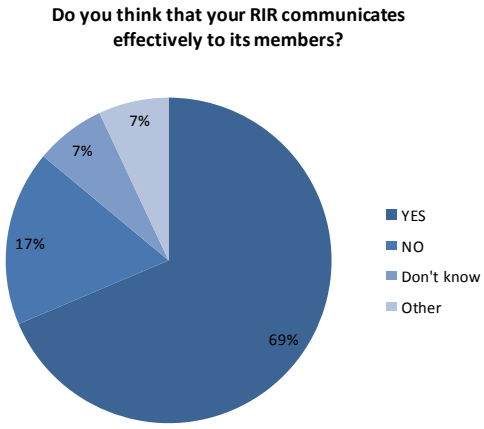
Table 8. The assessment of whether RIRs' operations are effective or not and nine different

variables related to trust.

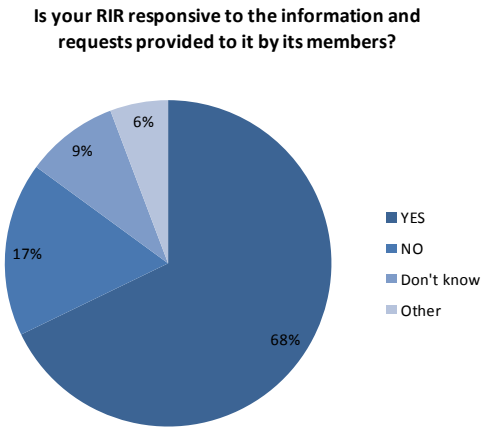
Test Variable	Welch t-test	df	Sig. (2-tailed)
Component 1	5.88	11.75	0.00
Risk	6.47	18.76	0.00
Competence	3.59	11.11	0.00
Responsibility	4.53	11.13	0.00
Ethics	4.03	11.74	0.00
Transparency	5.97	13.53	0.00
Understanding objectives	3.52	11.97	0.00
Trust in RIR (Q16)	5.61	11.99	0.00
Trust in other RIR members (Q17)	1.49	12.29	n.s.

Table 9. Welch independent t-test for nine variables related to trust in RIRs.

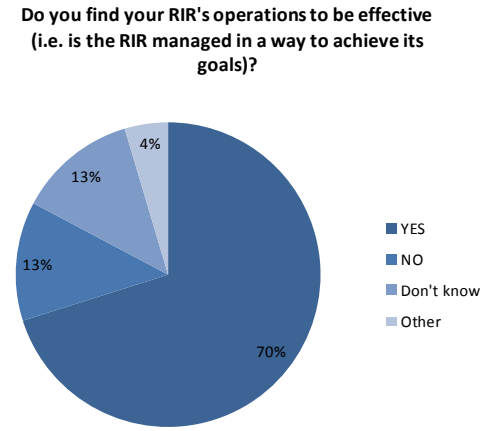
The following figures (Figure 7) provide the distributions of responses to previously discussed factors of trust (*Q10*, *Q11*, and *Q12*).



N = 86



N = 87



N = 87

Figure 7. Distributions of responses to previously discussed factors of trust (Q10, Q11, and Q12).

2.C RIR relationships and trust

The following table enlists several important RIR relationships. The respondents were asked to rank the importance of each of them according to how important the management of them is for their RIR in order for them to have trust in it. (*Q9*; the ranking was conducted by entering 1 for a least important to 5 for the most important relationship).

RIR relationships
Relationships among members.
Relationships between members and the board.
Relationships between members and the management.
Relationships between the RIR and the wider Internet community.
Relationships between the RIR and governments.
Relationships between the RIR and law enforcement agencies.

Table 10. RIR relationships

Figure 8 presents mean rankings of the importance of RIR relationships for trust in RIRs.

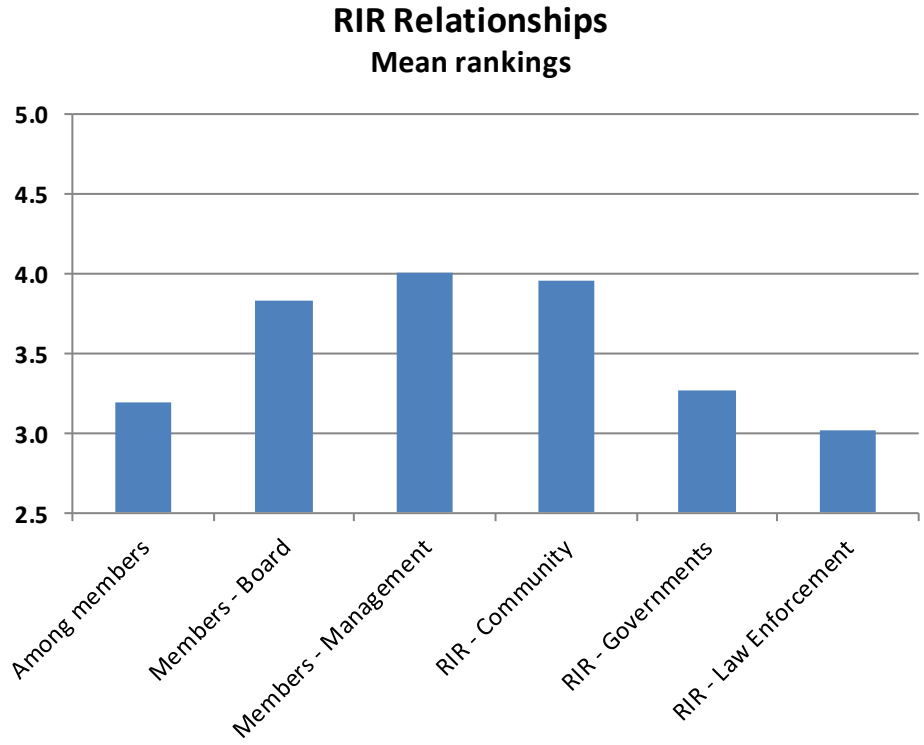


Figure 8. Mean rankings of RIR relationships.

Rankings of all six assessed RIR relationships were entered as predictors in the multiple regression model with the overall assessment of the level of trust in RIR (*Q16*) as a dependent variable. The overall model had a significant effect: $R^2 = .18$, $F(6,73) = 2.72$, $p < .05$, explaining only 18% of variance in the dependent variable. However, an important finding relates to significance of beta coefficients: only the rankings of the relationship between the RIR and *the wider Internet community* ($\beta = -.35$, $t = -2.88$, $p < .01$) and the

relationships between the RIR and *law enforcement agencies* (β= -.30, t=2.00, p<.05) were statistically significant. Given the signs of the standardised regression coefficients, it can be concluded that those respondents who believe the relationships between the RIR and the wider Internet community to be important in respect to trust in RIR actually have a *lower* trust in their primary RIR, while those who believe the relationships between the RIR and the law enforcement agencies to be important in respect to trust in RIR *trust more* to their primary RIR.

2.D Relationships between RIR members

Three questions addressed the issue of relationships and communications with other members of the same RIR organisation (*Q13: How often do you communicate with other members of your RIR organisation?*; *Q14: What is the main topic when you discuss the RIR with other members?*; *Q15: How would you characterise the level of the interaction between the members of your RIR organisation?*).

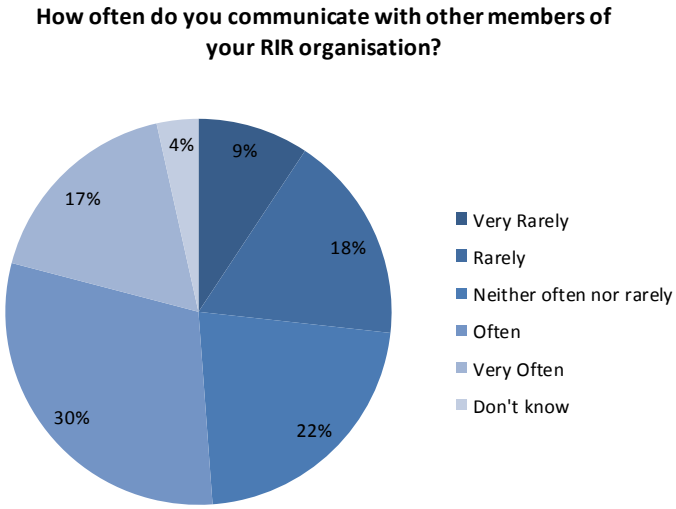


Figure 9. Q13: How often do you communicate with other members of your RIR organisation?

Interestingly, the communication between the RIR member organisations seems to be well developed: in total, 47% respondents reported that they communicate often or very often

with other members, while only 27% reported that they communicate rarely or very rarely.

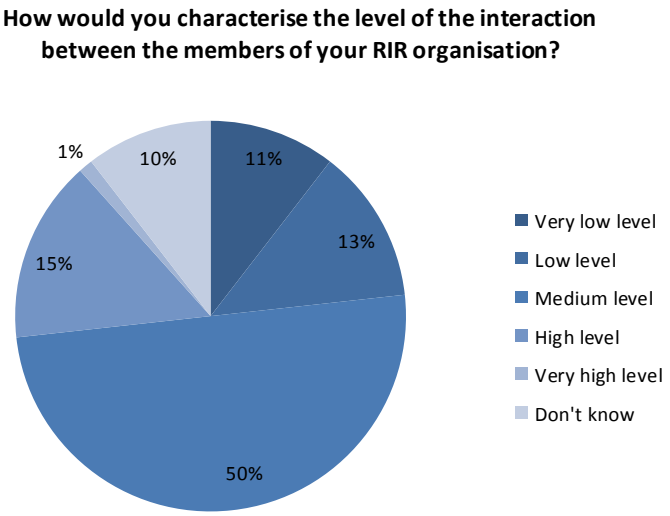


Figure 10. Q15: How would you characterise the level of the interaction between the members of your RIR organisation?

However, from the responses to *Q15* we can see that 50% of respondents believe that the level of interaction between RIR members is only medium; only 16% believe it to be high or very high, while 24% claim that the level of interaction is low or very low.

2.E Signals of Risk

A multiple response question (Q18) was used to assess the respondents' recognition of potential signals of risks in relation to their trust in the RIRs. They were asked to select as many potential signals of risk that they can identify as treats to their trust in RIRs from the following list:

Signals of Risk
External regulatory threats
Deviation from RIR's policies
Budget non-transparency
A non-transparent act by an RIR
Challenges in policy implementation
Challenges in policy development process
Membership disagreements

Table 11. Signals of risk to trust in RIRs

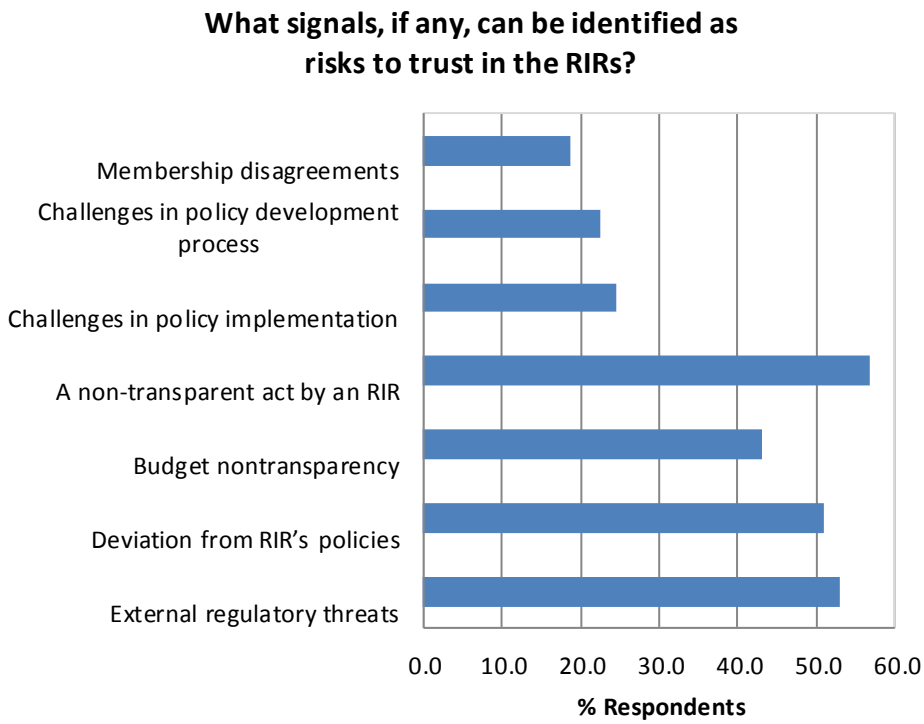


Figure 11. Q18: What signals, if any, can be identified as risks to trust in the RIRs?

More than 50% of respondents would be concerned in a case of a non-transparent act on behalf of a RIR, in a case of a deviation from RIR's policies, and in a case of recognising external regulatory threats. Membership disagreements and managerial issues of changes in policy development processes or policy implementation do not seem to cause much concern.

2.F Mapping the RIR membership

In order to study the distribution of trust (*Q16*) across the members of different RIR organisations and understand how similar they are in respect to their assessments of trust indicators (Table 2), a multidimensional scaling (MDS) has been performed based on the following variables: general assessment of trust in RIRs (*Q16*), I feel at risk when providing my own sensitive data to my RIR (*Q3*), People who manage and operate my RIR are competent in their area of expertise (*Q4*), I believe that my RIR operates responsibly as a good corporate citizen (*Q5*), I believe that RIRs use ethical business practices (*Q6*), The RIR organisation of my primary membership communicates transparently (*Q7*), I, as a member, have a thorough understanding of our RIR's objectives (*Q8*).

Euclidean distances were computed between all respondents from their responses on Likert scales to these questions. The distance matrix was than submitted to ordinal MDS, yielding a satisfactory two-dimensional representation with *Stress* = .08 (Figure 12).

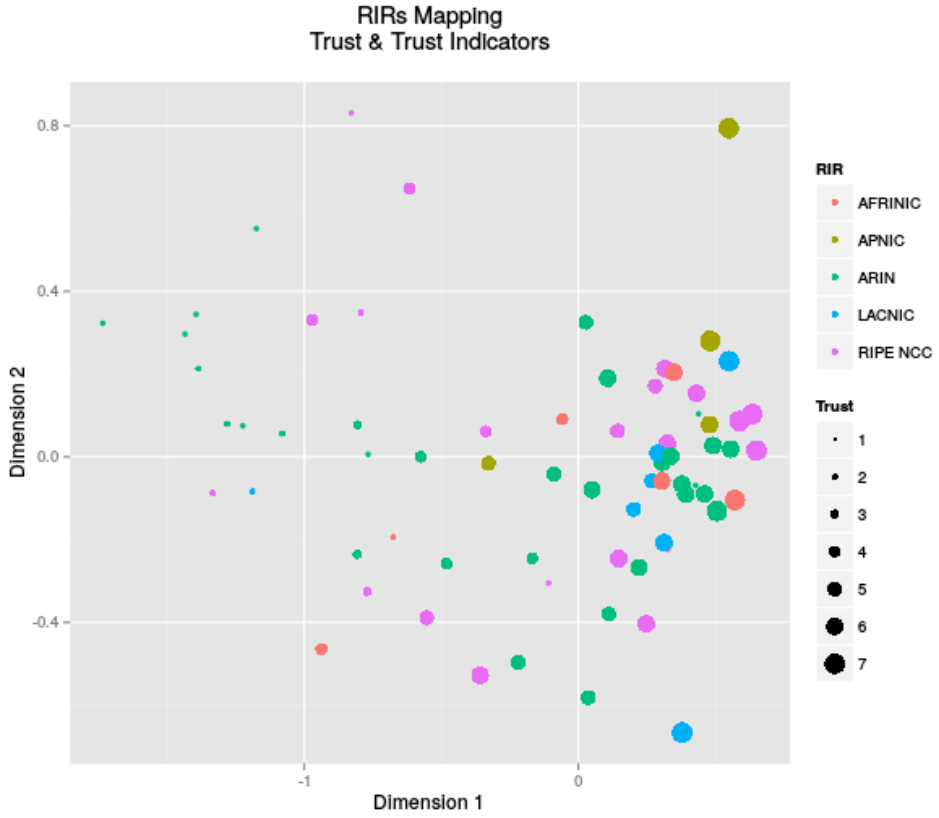


Figure 12. Two-dimensional, ordinal MDS representation of respondents. Point size represents the response to Q16 (general assessment of trust in RIRs) while colour codes the primary RIR of membership.

The map in Figure 12 represents only those respondents who did provide a general assessment of trust in RIRs (*Q16*; N = 83). It can be seen that the level of trust in RIRs exhibits a general increase from left to right, so Dimension 1 really represents trust. As of the respondents who expressed a very low level of trust in their primary RIRs, many (green points) who are members of ARIN (left side of Figure 12 can be found, approximately those with coordinates $x < -1$ on Dimension 1). However, many ARIN members also expressed higher levels of trust in their primary RIR organisation. Among those who generally express higher levels of trust in RIRs there is no clear pattern of membership to particular RIRs (right side in Figure 12, approximately those with coordinates above $x = 0$ on Dimension 1).

As of Dimension 2, it clearly represents whether the impact of the respondents' assessment of trust indicator correlates with the overall trust they have in their primary RIR. A multiple linear regression was performed with all variables used to produce the map in Figure 12 as predictors and the map y-coordinates as criterion available. The results **indicate a high degree of fit**: $R^2 = .89$, $F(7,72) = 84.69$, $p < .01$, with the $\beta_{Q3/RISK} = 1.13$, $p < .01$, $\beta_{Q4/COMPETENCE} = -4.95$, $p < .01$, $\beta_{Q5/RESPONSIBILITY} = -3.67$, $p < .01$, and $\beta_{Q6/ETHICS} = -.19$, $p < .01$; the contributions of other predictors were not statistically significant.

Thus, higher coordinates on Dimension 2 roughly represent respondents who fear they are at risk when providing their own sensitive data to their RIR organisations, while lower coordinates roughly represent those who believe their RIR organisations are competent, responsible, and ethical in their business practices. In comparison, the same set of predictors with the x-coordinates from the MDS map as criterion, provides for a great fit, $R^2 = .99$, $F(7,72) = 4049.06$, $p < .01$, except that the contribution of the general assessment of trust is

now the most pronounced, $\beta_{Q16/TRUST} = .356$, $p < .01$, with all other contributions positive and statistically significant at $\alpha = .01$ except for *Q8: I, as a member, have a thorough understanding of our RIR's objectives*. Because it is already known that a linear combination of trust indicators correlates well with the general assessment of trust in RIRs (Q16), it can safely be interpreted that Dimension 1 as *trust in RIRs*, and Dimension 2 as *confidentiality in RIRs*.

CHAPTER 7

Conclusion

This chapter summarises the results of the analysis in seeking to answer the following:

- How is trust defined and acted upon by chosen organisations?
- What can be learned from the approach - both in terms of how to refine the methodology itself and how the organisations investigated (and similar institutions) can increase trust or better use trust information in their activities?

Findings to these questions show that the there is a trust framework, composed of expertise-based, reputation-based and transparency-based trust indicators specifically developed to evaluate trust in sets of relationships in the organisation and trust processes. 'Trust processes' are defined as formal or informal processes and policies put in place by the organisation with the goal of increasing or maintaining trust in them. The framework proposed was applied in an investigation of five Regional Internet Registries (RIRs), to determine the trust in the governance models that exist within these not-for-profit organisations. The analytical data shows the validity of the marks, relationships and processes we have identified as critical to operationalise trust in an organisation. In spite of the fact that the proposed framework was developed and tested on a very constrained sample of 102 participants, the convergence of indicators and the overall validity of the results suggest it to be a more than good starting point for future attempts to study trust in IG processes and related organisations.

Firstly, the key findings are briefly summarised:

1. High validation of the research concept and the trust framework consisting of trust processes and trust indicators to study trust within a not-for-profit membership based organisation such as RIRs.
2. Validation of literature based trust markers queried to investigate members' trust in RIRs, therefore confirming a test framework of how trust is operationalised in such organisations. In the Results and Analysis sections it was shown that that in spite of the fact that six trust markers were not specifically planned to present a set of converging indicators for a specific latent concept of trust in RIRs, responses were further submitted to a reliability analysis. Surprisingly, a very high value of Cronbach's alpha of 0.89 was obtained, indicating that these six items measure one latent construct of trust.
3. Most strongly associated determinants of trust in any organisation for RIR members organisations are:

    - Transparency understood as; communication of an organisation with its membership in a timely manner.
    - Predictable behaviour of an organisation.
    - Staying true to its mission.

    At the same time, trust indicators (in questions Q10 and Q11) show that RIR members are not entirely certain if the communication is always as efficient or responsive, so that could additionally explain why "transparency" in Q2 defined as above has the highest ranking variable.

4. Key findings in Q17 about the overall trust of members in RIRs show that there is an equal distribution of members from all RIRs that both trust more and trust less their RIRs. So there was no single RIR where only trust or distrust was displayed – which also means

that there could be different perceptions of where trust can be improved in each of them. Overall there seems to be an indication of much higher trust than distrust of members within an RIR.

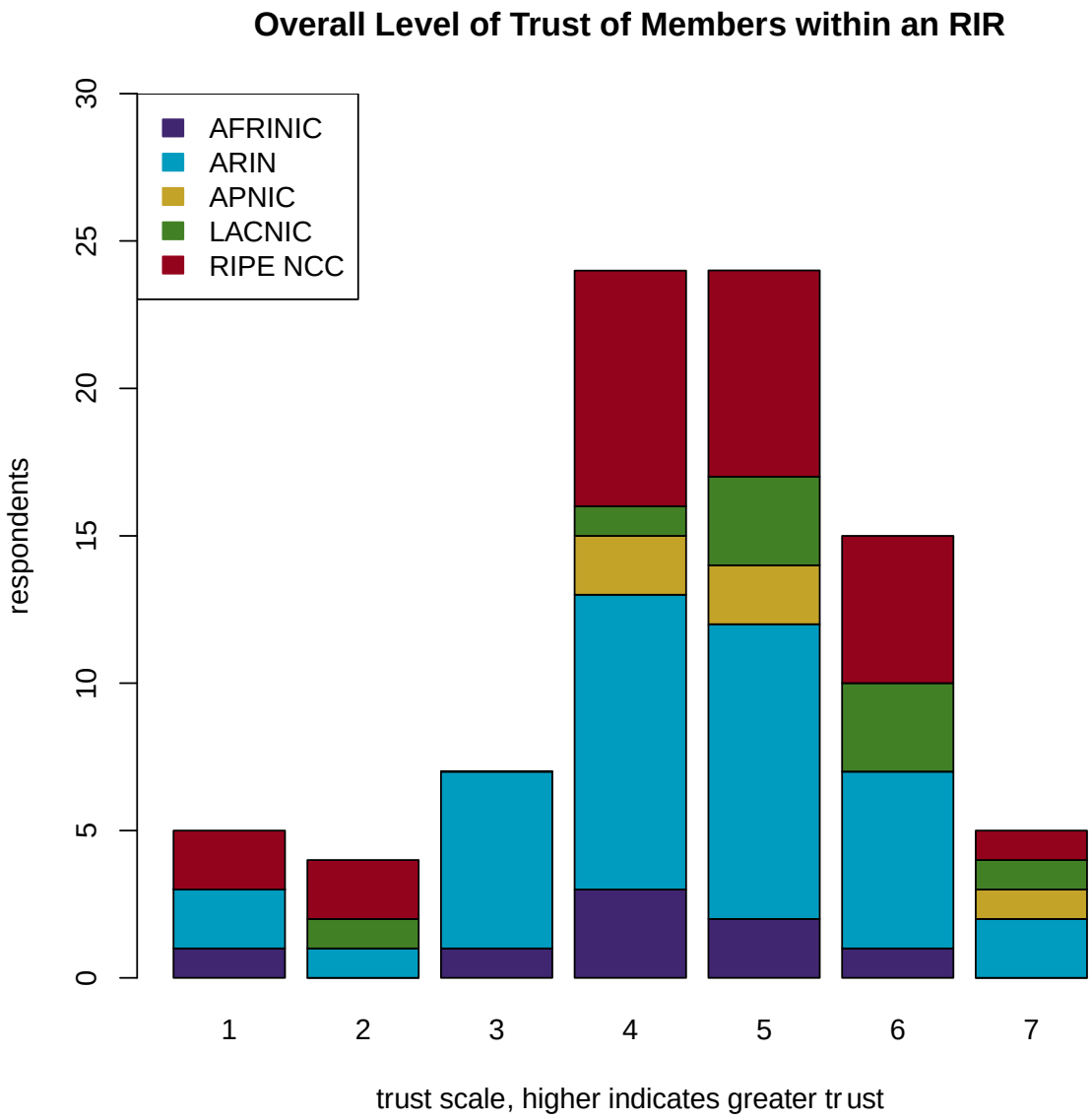


Figure 13. Overall level of trust in RIR members

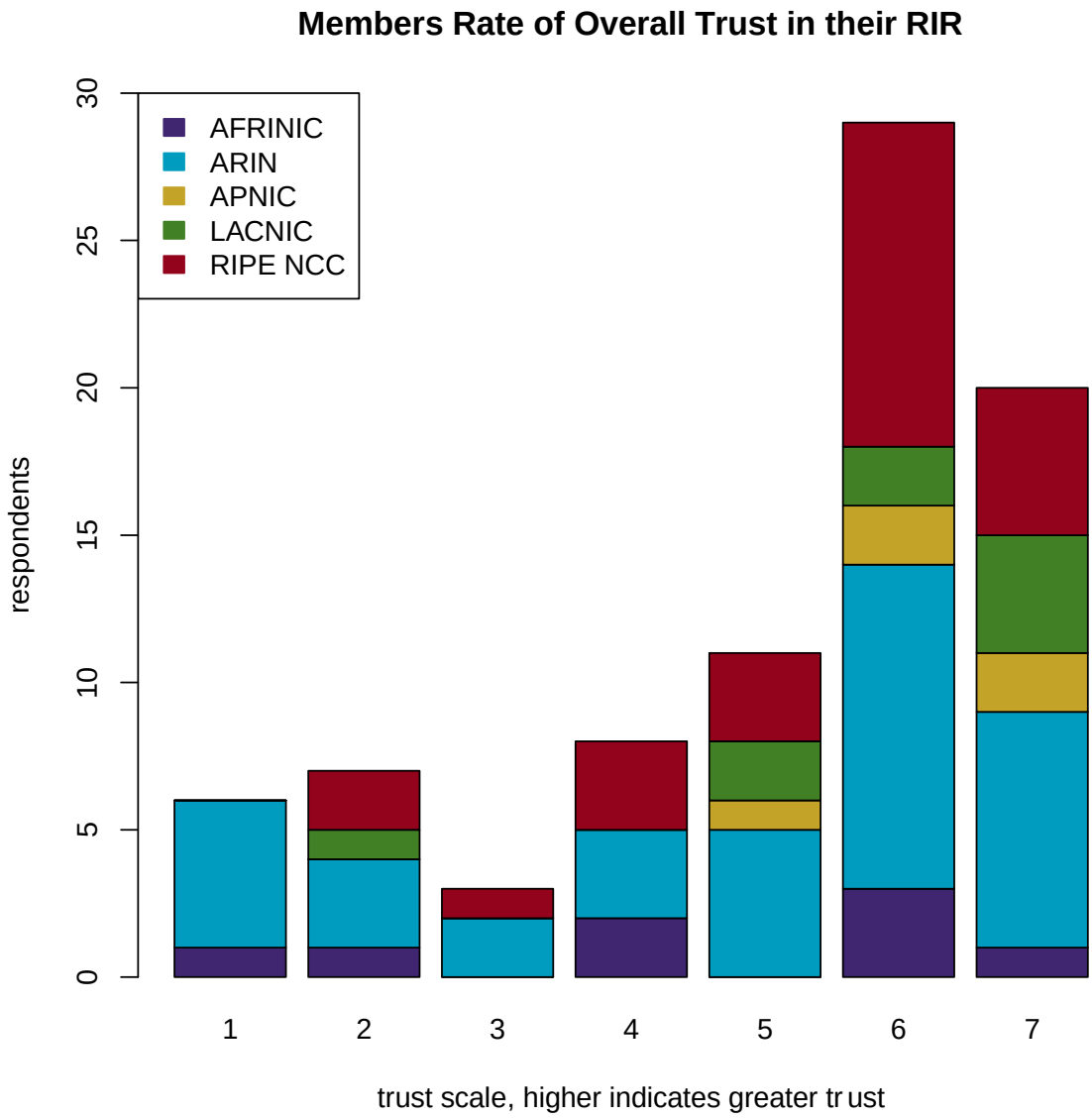


Figure 14. Members rate of overall trust in their RIR

5. A non-transparent act by an RIR is perceived overall as the highest risk to trust in RIRs.

It is hard to make comparisons among RIRs internally because of different structures, however, in this instance, some may be made using the data from the survey. The below graph (Figure 15) shows that, for both ARIN and LACNIC the highest risk to the trust in RIRs poses an external regulatory threat. This could be in a form of another organisation competing for authority in the same space and region, or through some other type of external regulation, perhaps from a state authority or an intergovernmental organisation. Or it could simply mean be that "the problem of trust lies elsewhere". To understand accurately the

nature of this response, additional research should be undertaken, perhaps by those regional RIRs. The third important perceived reason for losing trust in RIR is deviation from RIRs policies, which was no surprise.

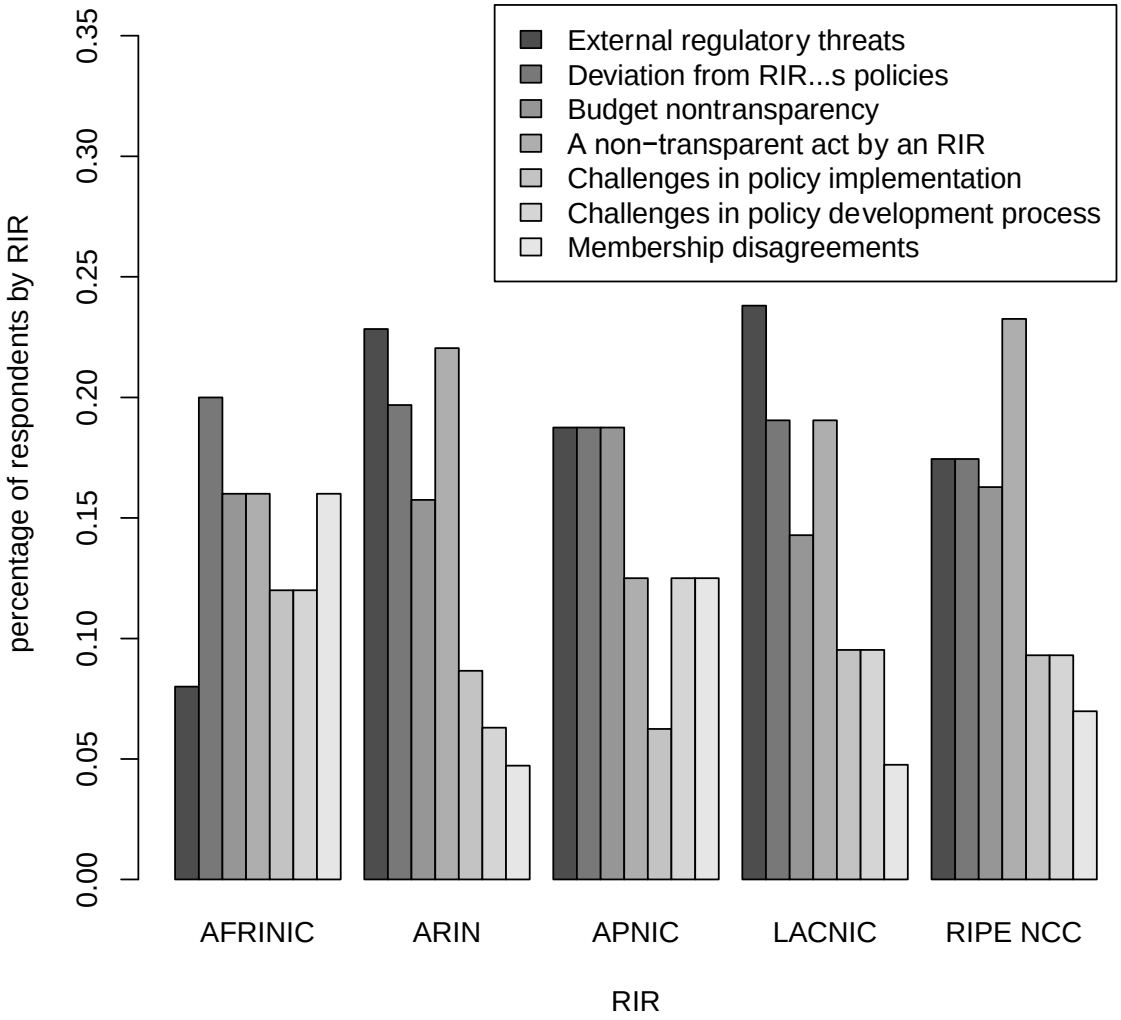


Figure 15. RIR member survey respondents views on risks to trust

6. Statistically, the most ***significant relationship*** to be monitored and/or that can be used to increase trust within an RIR is *the relationship between the organisation and the wider Internet community*. Further examination on the nature of this response should be undertaken, as motives for this answer could be different, e.g. due to monitoring or increasing RIRs' activities in the Internet governance ecosystem or through some other

cause – or through further work with IXPs, Computer Emergency Response Teams (CERTs) or other stakeholders. Although what exactly is behind this request is unknown, additional data analysis has been carried out and applied to the regression analysis test. Given the signs of the standardised regression coefficient, it can be concluded that those respondents who believe the relationships between the RIR and the wider Internet community to be most important in respect to trust in RIR actually have a lower trust in their primary RIR, while those who believe the relationships between the RIR and the law enforcement agencies to be most important actually place a higher level of *trust* in their primary RIR.

However, due to findings in the literature that point to trust as being a key element of social capital, the notion of each RIR member themselves also carrying some social capital, the history of the IG and organisational credible commitments made, this question could have been answered in an aspirational way or as an understanding of a necessity to further increase collaboration among stakeholders – which necessary for rebuilding trust.

Interviews

1. How is trust defined and operationalised in chosen organisations:

The research results from interviews made some additional points that complement the trust framework being defined here by exploring, monitoring and improving working relationships that exist among members and the organisation, but also how the organisation is prepared to deal with trust issues.

Findings from interviewees

As explained in the methodology section of Chapter 5, a survey on trust within RIRs was

carried out among members of all five global RIRs. Additionally, the management, represented by the five CEOs of each regional organisation, was interviewed to validate and complement some of the findings, and these are included in the discussion section.

Their answers provided further valuable insight in the specificity of trust frameworks applicable for internet not-for-profit membership-based organisations that manage global resources – from a particular perspective of public interest.

Additionally:

1. All interviewees agreed that trust could be studied within an organisation by measuring a set of specifically tailored trust indicators within a particular organisational process. Few RIRs (LACNIC, APINIC and RIPE NCC) would consider including some sets of the designed trust indicators in their annual or biannual membership survey questionnaire of RIRs' customer satisfaction. For example, if one wanted to measure the transparency of meetings as a process, certain indicators can be measured that would inform one about the level of transparency.
2. Transparency exists not only in the way that policies are developed, but also how they are implemented too. The RIRs operate on principles such as consensus-based policymaking, openness and inclusiveness. Their database is public so anyone can see if consensus-based developed policies have been faithfully followed and correctly implemented.
3. RIRs are unique not-for-profits because of the operational role the play in the IG system. As IP and AS numbers are unique, and the five RIRs are only organisations offering allocation and assignments of those resources, they have been a perceived as having a natural 'monopoly" by some actors, which heightened the need for trust and accountability measures.
4. Transparency: A small number of examples of management's lack of awareness of the

need for more detail (e.g. of how board level decisions are reported and communicated back to members and the community)have been perceived by the RIR's management as a matter of oversight that was promptly corrected. Because of their unique and visible role in the IG space, the RIR view inclusiveness, openness and transparency of their operations as highly important. Apart from annual or biannual member and community satisfaction surveys, there are 10 annual meetings with in-depth open plenary reporting of activities, (two by each RIR) for members and the wider Internet community. They allow participation in person, providing full webcast and remote real-time online communication and archives. There are other operational transparency mechanisms in place such as the NRO website. Overall this shows that a lot of resources are being put toward processes such as accountability and transparency in order to keep RIR and community members informed.

5. The most critically perceived trust process for RIRs' accountability are the implementation of IP policies developed by their membership, and there has been no case in the history of RIRs where policies have not been implemented.
6. Organisational trust is built over time, by interaction of organisational members/participants with the organisation itself, and through learning about each other's behaviour, therefore ultimately forming trusting relationships. It is not possible to form an organisation or an RIR without an initial amount of trust.
7. Similarities and common trust issues of not-for-profit membership based. The RIRs have similar accountability mechanisms when compared to other not-for-profits and similar governance structures, like the elected board and adopted bylaws.

Common issues: ultimately trust is defined by multiple and through new (in formation) and prior (existing) trusting or distrusting relationships, observed through the prism of existing and new sets of trusting processes and mechanisms such as (transparency, accountability).

8. Uniqueness: Internet governance institutions such as RIRs made credible commitments and have some normative rules around those commitments expressed through policies developed by its membership. In order to trust, credible commitments would be monitored and tested through trust processes.
9. Trust inside an RIR is not transferrable to another RIR. The RIR in a different region may need to carry out different activities with regards to trust relationship between organisation and the wider Internet community.

As can be seen in the survey results, trust has many building blocks or indicators, is multi-dimensional and subjective, yet it can be ultimately measured by specific indicators, within sets of group or individual relationships and organisational processes. While transparency is an important element, an RIR that deals better with transparency processes can be perceived as one instilling more trust.

Proposals for framework of improvements

As the quantitative analysis of survey questions Q10 and Q11, and Table 5, Table 7 and Table 9 from the data analysis shows, the efficiency of management, and responsiveness and efficiency in communications, have effects on the perceived level of trust in an RIRs, in the future, interviews of the RIR management should be more structured to include questions regarding their perception of how they see the same factors influence trust in RIRs. Therefore the methodology can be improved by studying management's understanding of trust in RIRs and to what specific indicators and processes they pay attention to, so that further comparisons and understanding of gaps and mapping can be made between the members and management.

Additionally running a longer survey may help to get a greater and more balanced data

set from all RIRs. As mentioned, the data set from APNIC is not considered representative for analysis and comparisons.

Governance structures, leadership and election processes are additional major building blocks of trust in many Internet organisations with a mandate to manage global resources and public policy development, with a not-for-profit legal set up. Trust processes have been presented and discussed which study the activity of IG leaders who have to live up to the expectations of organisations' core missions and credible commitments, as well as the expectations of members and the community, meaning a wide range of stakeholders should be part of future studies.

Although the survey was too short to study in depth correlation between members' trust in specific governance structures and processes, it gained an insight as to where and which important trust and distrust signals should further be examined in RIRs organisational processes, and the way trust is currently operationalised. However a more in depth study may be carried out within different IG institutions or IG initiatives to compare findings.

Conclusion

The study sought the answer the question of how trust is defined and operationalised with an RIR as an important organisation in the IG ecosystem.

Trust is pivotal to whether organisations are legitimate and effective. It is therefore important to understand what variables matter most. The premise of this study is that different contexts and organisations may rank different variables as less or more important.

Transparency, in the sense of timely communication of an organisation's activities to the members and community, was identified as the most dominant variable for any

organisation. It is an important further question to determine if this, in particular, can be clearly explained. While transparency usually implies visibility of the behaviour of certain groups or individuals, and in a generic social sciences understanding as a set of policies that allow citizens (members) to access information, it is important to ask whether the meaning is any different in the particular setting of RIRs and/or whether transparency in this form is linked with the culture of openness that is associated with the Internet.

This has implications for RIRs and for IG in general. It is important to embed openness within the structures of institutions. Processes such as transparency in decision-making, efficient and timely communication, openness and accountability when following or changing the rules matter.

Equally the study's question of how trust is operationalised is answered with the fact that conservative values, such as predictability, play an important role, as well as staying true to the organisational core mission.

The most important variable for RIR members for trust to be maintained is the relationship of the organisation as a whole with the wider Internet community – which confirms that trust in IG organisations may require further creation of a sense of a community, or more cooperation, enabling people to work together.

In order to make a prediction that an actor will behave cooperatively, one must also assume that they have some degree of trust that the others involved in their decision-making situation will also cooperate. Trust is an integral element of social capital, and trust may be built around the notion that "all benefit from more cooperation" as explained in Prisoner's dilemma.

For trust to be maintained in internet governance organisations, continuous building of bridges and trusting relationships among different stakeholders has to continue: namely working relationships among the Internet technical community, civil society organisations, government officials and private sector and academia. If all of these relationships and interactions can continue in an open and transparent manner, then it is expected that trust in all associated organisations can be maintained.

ABBREVIATIONS AND ACRONYMS

AFRINIC	African Network Information Centre for Africa
APNIC	Asia-Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
AS	Autonomous System
BSD	Berkeley Software Distribution
CA	Certificate Authorities
CERT	Computer Emergency Response Team
ccTLD	country code Top-level Domain
CIGI	Centre for International Governance Innovation
CSTD	Commission on Science and Technology for Development
DNS	Domain Name System
DOC	Department of Commerce
GAC	Governmental Advisory Committee, ICANN
GDP	Gross Domestic Product
GPL	General Public Licence
gTLD	generic Top-level Domain
IAB	Internet Architecture Board
IAHC	International AD Hoc Committee
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IFWP	International Forum on the White Paper
IGF	Internet Governance Forum
IGO	Intergovernmental Organization
IP	Internet Protocol
ISOC	Internet Society
ISP	Internet Service Provider
ITR	International Telecommunication Regulations
ITU	International Telecommunication Union
IXP	Internet Exchange Point
LACNIC	Latin America and Caribbean Network Information Centre
MAAWG	Messaging Anti-Abuse Working Group
MoU	Memorandum of Understanding
MSM	Multistakeholder Model
NANOG	North American Network Operators Group
NETmundial	Global Multistakeholder Meeting on the Future of Internet Governance
NGO	Non-Governmental Organisation
NRO	Number Resource Organization
NSA	National Security Agency
NSF	National Science Foundation
NSI	Network Solutions Inc.
NTIA	National Telecommunications Information Administration

OSI	Open Systems Interconnection
PDP	Policy Development Process
RFC	Request for Comments
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registry
SANOG	South Asian Network Operators Group
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transfer Control Protocol/Internet Protocol
TTP	Trusted Third Parties
UN	United Nations
US	United States
W3C	World Wide Web Consortium
WCIT-12	2012 World Conference on International Telecommunications
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society
WTPF	World Telecommunication Policy Forum
WWW	World Wide Web

REFERENCES

Aspers, P. (2005). *Markets in fashion, a phenomenological approach*. London: Routledge.

Bamberger, W., Technische Universität München, (2010). *Interpersonal Trust – Attempt of a Definition*. [online] Available at: < http://www.ldv.ei.tum.de/en/research/fidens/interpersonal-trust/> [Accessed 10 February 2015].

Beckstrom, R. and Lambsdorff, M. G., (2008). Why trust plays a central role in decentralized organizations. *The Focus Vol. XII/1*, pp. 68-71.

Bijker, W. E. (1997). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. Cambridge: MIT Press.

Birner, R., and Wittmer, H., (2003) Dolšak, N. and Ostrom, E., [eds.]. Using social capital to create political capital: how do local communities gain political influence? A theoretical approach and empirical evidence from Thailand. *The Commons in the New Millennium: challenges and Adaptations*, pp. 3-34. Cambridge, UK.

Brown, I., and Marsden, C. T., (2013). *Regulating code: Good governance and better regulation in the information age*. Cambridge: MIT Press.

CCCen, (2014). *Trustworthy secure modular operating system engineering [31c3]*. [online] Available at: <https://www.youtube.com/watch?v=4X0WjSqiIPs> [Accessed: 22 April 2014].

Center for Strategic and International Studies (2014). *Net losses: Estimating the global cost of cybercrime*. Santa Clara, California.

Centre For International Governance Innovation & Ipsos (2014). *CIGI-Ipsos Global Survey on Internet Security and Trust*. Waterloo, Canada.

Coleman, J. S., (1990). *Foundations of social theory*. Cambridge, MA and London: Harvard University Press.

Colquitt J. A., Scott B. A., and LePine J. A., (2007). Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships With Risk Taking and Job Performance. *Journal of Applied Psychology*, Vol. 92, No. 4, 909–927.

DeNardis, L., Yale Information Society Project Working Paper Series (2010). *The Emerging field of Internet governance*. [online] Available at: < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343> [Accessed 11 February 2015].

DeNardis, L., (2014). *The global war for internet governance*. New Haven: Yale University Press.

Dimoka, A., (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *Mis Quarterly*, 34(2), 373-396.

Drake, W. J. ed., (2005). *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)*. New York: The United Nations Information and Communication Technologies Task Force.

Edelman, (2015). Edelman Trust Barometer. [online] Available at: <http://www.edelman.com/insights/intellectual-property/2015-edelman-trust-barometer/> [Accessed 10 March 2015].

Fukuyama, F., (1995). *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press.

Gandhi, M., (1957). *The Story of My Experiments with Truth*. Beacon Press reprint 1993.

Geertz, C., (1973). *Thick description: Toward an Interpretive Theory of Culture*. New York: Basic.

Glennon, M. J., (2014). *National security and double government*. New York: Oxford University Press.

Grandison, T. and Sloman, M., (2001). A Survey of Trust in Internet Applications. *IEEE Communications Surveys and Tutorials, Fourth Quarter 2000*.

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

Hafner, K. and Lyon, M., (1998). *Where Wizards Stay Up Late: The Origins of the Internet*. Simon & Shuster.

Hardin, R., (2002). *Trust and trustworthiness*. New York: Russell Sage Foundation.

Hardin, R., (2006). *Trust*. Cambridge: Polity Press.

Internet Activities Board (IAB), (1989). Ethics and the Internet. [online] Available at: <http://tools.ietf.org/html/rfc1087> [Accessed on: 22 April 2015].

Internet technical collaboration group. Internet Governance Observations and Recommendations from Members of the Internet Technical Community. [online] Available at: <http://www.internetcollaboration.org/ig-recommendations-itcg/> [Accessed on 21 April 2015].

ISOC, (2013). *History of the Internet Society*. [online] Available at: <http://www.internetsociety.org/history> [Accessed 22 April 2015].

ISOC, (2014). *Who Makes the Internet Work: The Internet Ecosystem*. [online] Available at: <http://www.internetsociety.org/who-makes-internet-work-internet-ecosystem> [Accessed 22 April 2015].

Jones, S., (1999). *TRUST-EC: requirements for Trust and Confidence in E-Commerce.* European Commission, Joint Research Centre.

Kant, I (1797). *The Metaphysical Elements of Ethics*.

Kassebaum, U. B., (2004). *Interpersonelles Vertrauen: Entwicklung eines Inventars zur Erfassung spezifischer Aspekte des Konstrukts*. Ph.D. thesis, Universität Hamburg.

Kee, H. W. and Knox, R. E., (1970). Conceptual and methodological considerations in the study of trust and suspicion. *Journal of Conflict Resolution*, 14:357-366.

Kurbalija, J., (2014). *Introduction to Internet Governance (6th Edition)*. Geneva: DiploFoundation.

Kydd, A., (2005). *Trust and mistrust in international relations*. Princeton: Princeton University Press.

Lerner, J. and Tirole, J., (2002). Some simple economics of open source. *The journal of industrial economics*, 50(2), 197-234.

Lessig, L., (1999). The Code is the Law. *Industry Standard*, April 19-26, 1999.

Lynn, S. M., (2002). *President's Report: ICANN – The Case for Reform*. [online] Available at: <http://archive.icann.org/en/general/lynn-reform-proposal-24feb02.htm> [Accessed 15 March 2015].

Mayer, R.C., Davis, J.H. and Schoorman, F.D., (1995). *An integrative model of organizational trust*. Academy of Management Review. 20 (3), 709-734.

McCullagh, D., (2004). United Nations ponders Net's future. *CNET News*, [online] Available at: <http://news.cnet.com/2100-1028_3-5179694.html> [Accessed 11 March 2015].

McKnight, D. H. and Chervany, N. L., (1996). The meanings of trust. *Technical Report WP9604, University of Minnesota Management Information Systems Research Center*, [online] Available at: <http://www.misrc.umn.edu/workingpapers/fullpapers/1996/9604_040100.pdf> [Accessed 12 February 2015].

Mendes, E., (2013). Americans' Confidence in Newspapers Continues to Erode. *Gallup*, [online] Available at: <http://www.gallup.com/poll/163097/americans-confidence-newspapers-continues-erode.aspx> [Accessed 22 April 2015].

Meyerson, D., Weick, K. E., and Kramer, R. M., (1996). Swift trust and temporary groups. In R. M. Kramer and T. R. Tyler eds., *Trust in organizations: Frontiers of theory and research*: 166-195. Thousand Oaks, CA: Sage.

Mickelberg, K., Schive, L., and Pollard, N., (2014). *US cybercrime: Rising risks, reduced readiness, Key findings from the 2014 US State of Cybercrime Survey*. [online] Available at: <http://www.pwc.com/cybersecurity> [Accessed 14 March 2015].

Miloshevic, D., (2015). Research project by University of Malta. [online] Available at: <https://blog.apnic.net/2015/03/26/research-project-by-university-of-malta/> [Accessed 26 March 2015].

Mishra, A. K., (1993). *Breaking down organizational boundaries during crisis: The role of mutual trust*. Unpublished working paper, Pennsylvania State University.

Misztal B., (1996). *Trust in Modern Societies: The Search for the Bases of Social Order*. Cambridge: Polity Press.

Naughton, J., (2015). Don't trust your phone, don't trust your laptop – this is the reality that

Snowden has shown us. The Guardian, [online] Available at <http://www.theguardian.com/commentisfree/2015/mar/08/edward-snowden-trust-phone-laptop-sim-cards> [Accessed 15 March 2015].

Porta, R. L., Lopez-De-Silane, F., Shleifer, A. and Vishny, R. W., (1996). Trust in large organizations. *National Bureau of Economic Research*, No. w5864.

Press, W. H. and Dyson J. D., (2012). Iterated Prisoner's Dilemma contains strategies that dominate any evolutionary opponent. *Proceedings of the National Academy of Sciences of the United States of America*, PNAS 2012 109 (26) 10409-10413.

Ronfeldt, D., (1996). *Tribes, institutions, markets, networks: A framework about societal evolution*. Santa Monica, Calif.: RAND, P-7967.

Rousseau, J. J., (1762). *The Social Contract, or Principles of Political Right*. Translated 1782 by G. D. H. Cole, public domain, [online] Available at <http://www.constitution.org/jjr/socon.htm [Accessed 11 March 2015].

Simon. C., (2006). *Launching the DNS War: Dot-Com Privatization and the Rise of Global Internet Governance*. Ph.D. dissertation, University of Miami.

Sztompka, P., (1999). *Trust: A Sociological Theory*. Cambridge: Cambridge University Press.

Waz, J. and Weiser, P., (2013). Internet governance: The role of multistakeholder organizations. *Journal of Telecommunications and High Technology Law 10.2*.

Zak, P. J., and Knack, S., (2001). Trust and growth. *The economic journal*, 111(470), 295-321.

APPENDIX A – SURVEY QUESTIONS

This section of the Appendix contains a copy of the survey questions used to investigate the Regional Internet Registries.

Survey on Trust in RIRs

March 20-30, 2015 Research Study on Trust

This survey is conducted by Desiree Miloshevic as part of her University of Malta/DiploFoundation Master in Contemporary Diplomacy with specialisation in Internet Governance which is designed to conduct research into the trust that members have in the RIRs' work and overall governance processes.

The RIRs and their members have done a huge amount of good work during the past year on the IANA Stewardship Transition Process. This work is very important and will be ongoing. A number of issues will arise; two of them being Governance and Trust. This study examines existing views as a contribution to the overall work.

Participants are given an absolute assurance of individual confidentiality. The results of this study will be analysed on aggregate level only – your personal identity will not be recognised in any step of the process. This is not an RIR initiated survey.

This questionnaire should take no more than 15 minutes of your time. For any questions on this study, please feel free to contact the research team at research (at) relax.co.uk. Thank you for your time and patience.

Q1

1. Please indicate the primary RIR organisation of your membership:

- ○ AFRINIC
- ○ ARIN
- ○ APNIC
- ○ LACNIC
- ○ RIPE NCC

Q2

2. Please select all that, in your view, applies to a trustworthy organisation:

- ☐ A trustworthy organisation is one that is reliable.
- ☐ A trustworthy organisation is one that has a good risk management.
- ☐ A trustworthy organisation is one that communicates about its decisions and operations to its membership in a timely manner.
- ☐ A trustworthy organisation is one that is competent.
- ☐ A trustworthy organisation is one that stays true to its mission.
- ☐ A trustworthy organisation is one that is efficient.
- ☐ A trustworthy organisation is one that has predictable behaviour.

Other comments (please specify)

PAGE

Q3

3. Please mark your level of agreement with the following statement: “I feel at risk when providing my own sensitive data to my RIR”

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree
- Don't know

Q4

4. Please mark your level of agreement with the following statement:

“People who manage and operate my RIR are competent in their area of expertise.”

- Strongly disagree
- Don't know
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree
- Don't know

Q5

5. Please mark your level of agreement with the following statement:

“I believe that my RIR operates responsibly as a good corporate citizen.”

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree
- Don't know

Q6

6. Please mark your level of agreement with the following statement: “I believe that RIRs use ethical business practices.”

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree
- Don't know

Q7

7. “The RIR organisation of my primary membership communicates transparently.”

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree
- Don't know

Q8

8. Please mark your level of agreement with the following statement: “I, as a member, have a thorough understanding of our RIR’s objectives.”

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree
- ○ Don't know

Q9

9. Rank the importance of the following relationships according to how important they need to be managed by your RIR for you to have trust in? Please rate. (1 least important to 5 most important)

	1	2	3	4	5
Relationships among members.	○ *Rank the importance of the following relationships according to how important they need to be managed by your RIR for you to have trust in? Please rate. (1 least important to 5 most important) Relationships among members. 1	○ Relationships among members. 2	○ Relationships among members. 3	○ Relationships among members. 4	○ Relationships among members. 5
Relationships between members and the	○ Relationships between	○ Relationships between	○ Relationships between	○ Relationships between	○ Relationships between

board.	members and the board. 1	members and the board. 2	members and the board. 3	members and the board. 4	members and the board. 5
Relationships between members and the management.	○ Relationships between members and the management. 1	○ Relationships between members and the management. 2	○ Relationships between members and the management. 3	○ Relationships between members and the management. 4	○ Relationships between members and the management. 5
Relationships between the RIR and the wider Internet community.	○ Relationships between the RIR and the wider Internet community. 1	○ Relationships between the RIR and the wider Internet community. 2	○ Relationships between the RIR and the wider Internet community. 3	○ Relationships between the RIR and the wider Internet community. 4	○ Relationships between the RIR and the wider Internet community. 5
Relationships between the RIR and governments.	○ Relationships between the RIR and governments. 1	○ Relationships between the RIR and governments. 2	○ Relationships between the RIR and governments. 3	○ Relationships between the RIR and governments. 4	○ Relationships between the RIR and governments. 5
Relationships between the RIR and law enforcement agencies.	○ Relationships between the RIR and law enforcement	○ Relationships between the RIR and law enforcement	○ Relationships between the RIR and law enforcement	○ Relationships between the RIR and law enforcement	○ Relationships between the RIR and law enforcement

agencies. 1 agencies. 2 agencies. 3 agencies. 4 agencies. 5

Q10

10. Do you think that your RIR communicates effectively to its members?

- YES
- NO
- Don't know
- Other

Other (please comment)

Q11

11. Is your RIR responsive to the information and requests provided to it by its members?

- YES
- NO
- Don't know
- Other

Other (please comment)

Q12

12. Do you find your RIR's operations to be effective (i.e. is the RIR managed in a way to achieve its goals)?

- ○ YES
- ○ NO
- ○ Don't know
- ○ Other

Other (please comment)

Q13

13. How often do you communicate with other members of your RIR organisation?

- ☐ Very rarely
- ☐ Rarely
- ☐ Neither often nor rarely
- ☐ Often
- ☐ Very often
- ☐ Don't know

Q14

14. What is the main topic when you discuss the RIR with other members?

Q15

15. How would you characterise the level of the interaction between the members of your RIR organisation?

- ○ Very low level
- ○ Low level
- ○ Medium level
- ○ High level
- ○ Very high level
- ○ Don't know

Q21

21. Optional: Gender

- ○ Male
- ○ Female
- ○ Other

Q22

22. Optional: Age

- ☐ 18 – 24
- ☐ 25 – 31
- ☐ 32 – 38

☐ 39 – 45

☐ 46 – 52

☐ 53 – 59

☐ 60 and older

Q23

23. Optional: Contact email. Please leave your email if you wish to receive updates from our survey analysis.

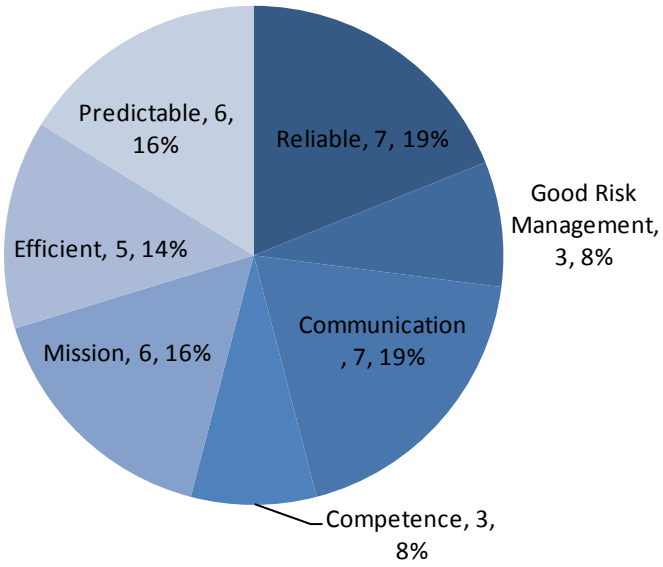
Thank you!

APPENDIX B – FULL SURVEY RESULTS

AFRINIC (N = 9)

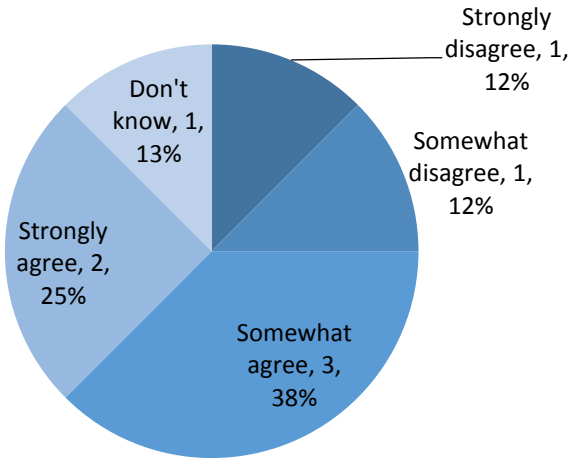
A. What describes a trustworthy organisation?

Q2. Please select all that, in your view, applies to a trustworthy organisation

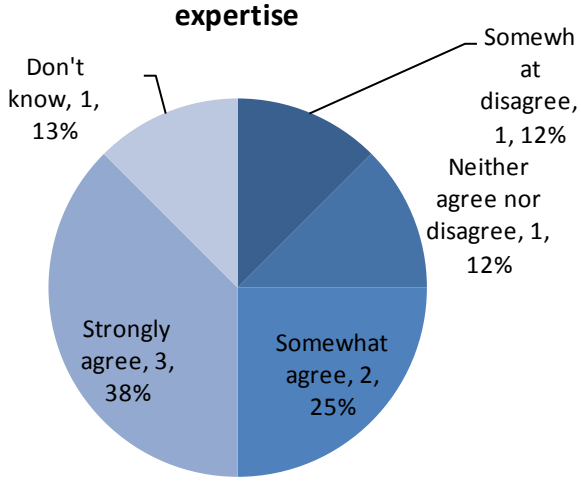


B. Trust indicators

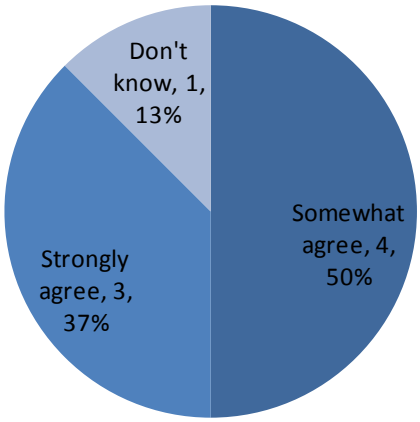
Q3. I feel at risk when providing my own sensitive data to my RIR



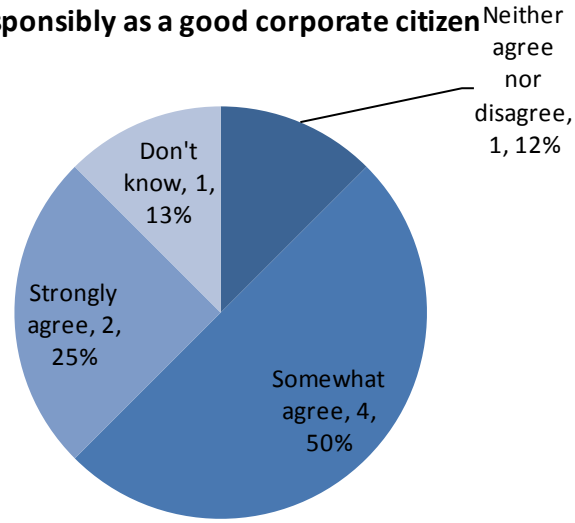
Q4. People who manage and operate my RIR are competent in their area of expertise



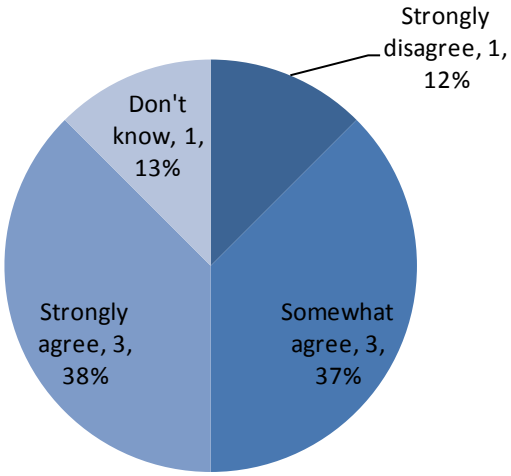
Q5. I believe that my RIR operates responsibly as a good corporate citizen



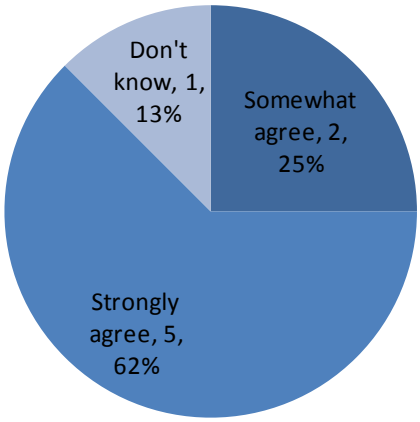
Q6. I believe that my RIR operates responsibly as a good corporate citizen



Q7. The RIR organisation of my primary membership communicates transparently

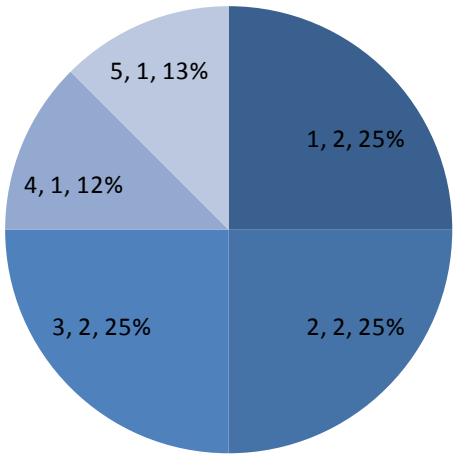


Q8. I, as a member, have a thorough understanding of our RIR's objectives

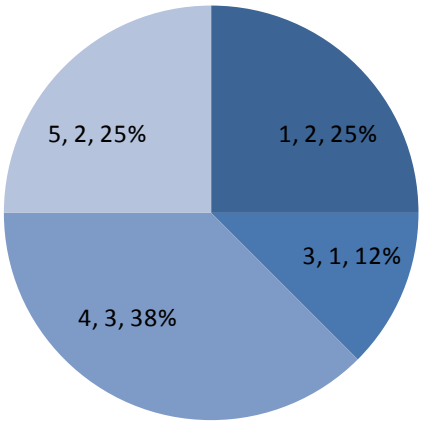


C. The importance different relationships to have trust in the RIR

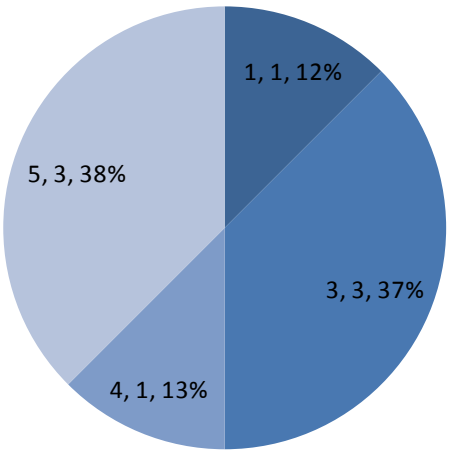
Q9. Relationships among members



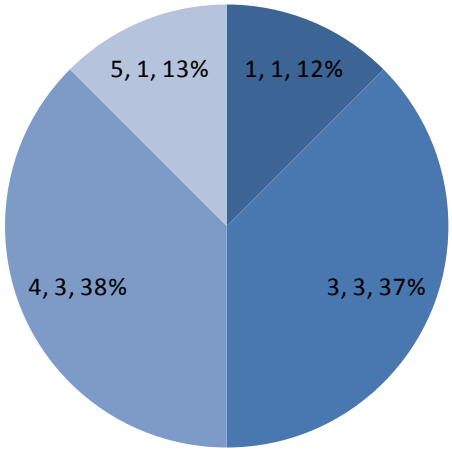
Q9. Relationships between members and the board



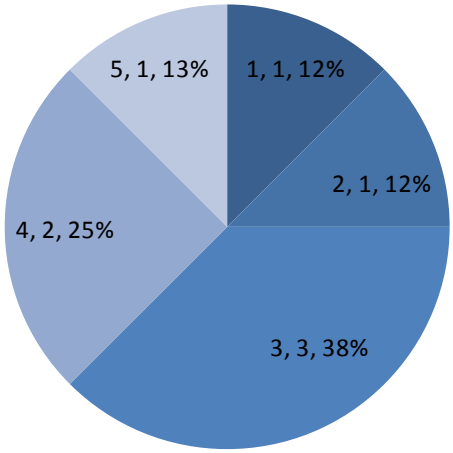
Q9. Relationships between members and the management



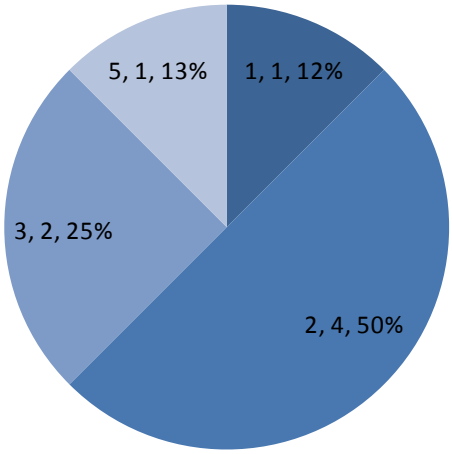
Q9. Relationships between the RIR and the wider Internet community



Q9. Relationships between the RIR and governments

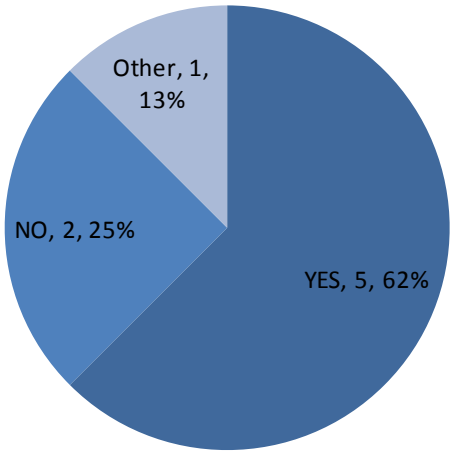


Q9. Relationships between the RIR and law enforcement agencies

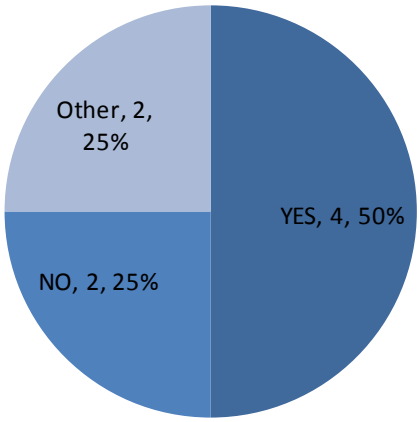


D. Assessment of the RIR's communication, responsiveness and effectiveness

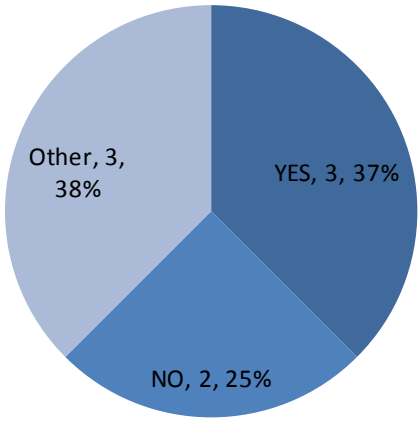
Q10. Do you think that your RIR communicates effectively to its members?



Q11. Is your RIR responsive to the information and requests provided to it by its members?

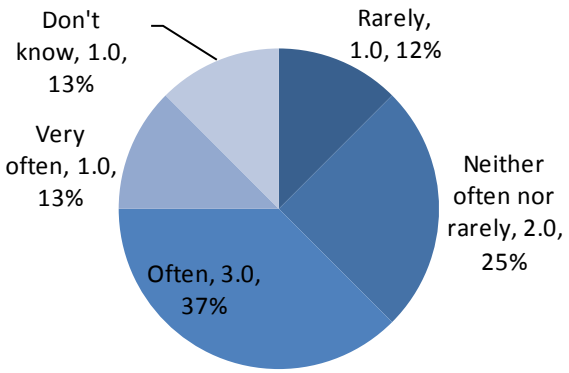


Q12. Do you find your RIR's operations to be effective (i.e. is the RIR managed in a way to achieve its goals)?

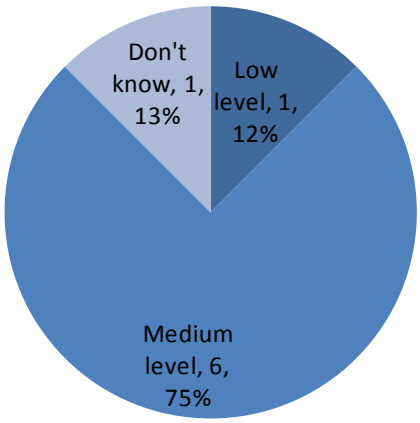


E. Communication with other RIR members

Q13. How often do you communicate with other members of your RIR organisation?

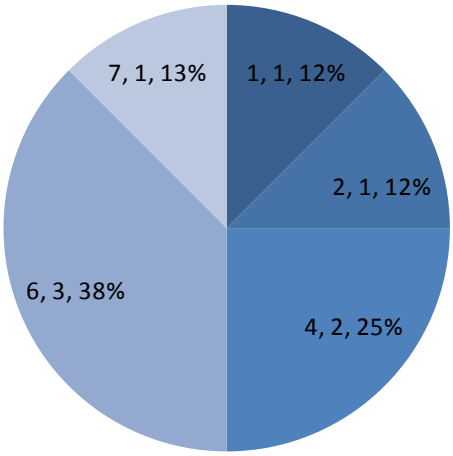


Q15. How would you characterise the level of the interaction between the members of your RIR organisation?

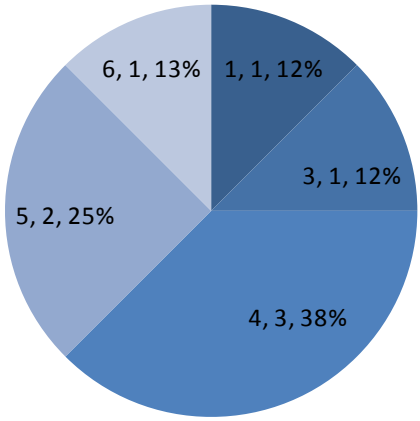


F. Trust

Q16. Please rate the overall level of trust that you have in your RIR organisation

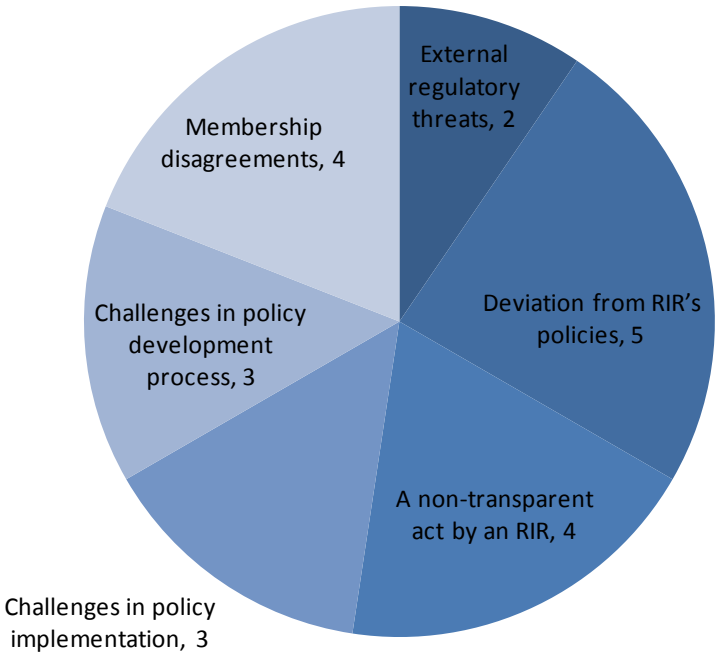


Q17. Please rate the overall level of trust that you have in other members of your RIR organisation



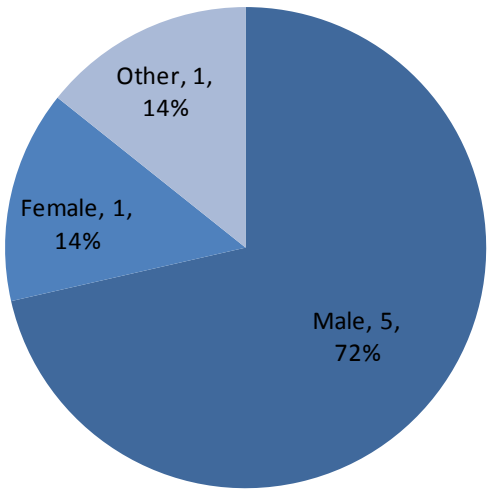
G. Signals of Risk

Q18. What signals, if any, can be identified as risks to trust in the RIRs?



H. Demography

Q21. Gender



Q2. Age