tripleC 9(2): 702-714, 2011
ISSN 1726-670X
http://www.triple-c.at

Toward Trust as Result. A Transdisciplinary Research Agenda for the 'Future Internet'

Stefano De Paoli[*], *GR Gangadharan*[**], *Aphra Kerr*[***], *and Vincenzo d'Andrea*[****]

* stefano@ahref.eu, <ahref Foundation, Trento, Italy
** gangadharan@in.ibm.com, Institute for Development & Research in Banking Technology (IDRBT) Hyderabad, India
*** aphra.kerr@nuim.ie , Department of Sociology, National University of Ireland Maynooth, Ireland
**** vincenzo.dandrea@unitn.it, Department of Computer Science, University of Trento, Italy

Abstract: *Trust has emerged as one of the key challenges for the Future of the Internet and as a key theme of European research. We are convinced that a transdisciplinary research agenda – that we define as Trust as Result – shared by Sociology and Computer Science, is of paramount importance for devising sustainable trust solutions for the (Future) Internet stakeholders. The scope of this paper is to present some aspects we consider important for building such an agenda. We distinguish our agenda by comparison with one of the current mainstream interdisciplinary approaches to trust, that of Trust Modelling which assumes that trust is an input in the design of trustworthy ICTs. We propose a different approach based on the concept of Assemblage, as proposed by DeLanda, and focus on how we can create trust as the result of the design and use process.*

Keywords: Trust, Future of the Internet, Trust Modelling, Trust as Result, Assemblage

Prelude: Trust and the Internet

The Internet is a global network of interconnected computer networks that serves billions of users world wide and a technology that has transformed the ways in which we communicate and interact in our everyday lives. Today, the Internet faces several challenges, that can be described using the label the *Future Internet* (Zittrain, 2008). The 2008 *Bled Declaration* (a declaration of intentions endorsed by a range of European Technology Platforms and European Research Projects) describes the challenges of the Future Internet as follows:

> *With over a billion users world-wide, the current Internet is a great success – a global integrated communications infrastructure and service platform underpinning the fabric of the European economy and European society in general. However, today's Internet was designed in the 1970s for purposes that bear little resemblance to current and foreseen usage scenarios. Mismatches between original design goals and current utilisation are now beginning to hamper the Internet's potential. A large number of challenges in the realms of technology, business, society and governance have to be overcome if the future development of the Internet is to sustain the networked society of tomorrow.*

There are indeed many challenges facing the Future Internet at different levels. For instance, the Internet faces structural limitations in terms of scalability, mobility, flexibility, security, trust and robustness (Stuckmann and Zimmerman, 2009). It is also clear that the decisions and actions that the research community takes for the Future Internet research will impact future European societies at different levels. The Bled Declaration continues by saying that:

> *A significant change is required and the European Internet scientific and economic actors, researchers, industrialists, SMEs, users, service and content providers, now assert the urgent ne-*

> *cessity to redesign the Internet, taking a broad multidisciplinary approach, to meet Europe's societal and commercial ambitions.*

Approaching the challenges of the Future Internet requires a common effort of different disciplines, as the Future Internet does not just involve technological problems but has implications for the economy, society and governance. But is talking about a multidisciplinary approach just enough? Is the multidisciplinary approach the right direction to follow? Of course this depends on the meaning we give to the word "multidisciplinary[1]" and from the ways we build this shared effort among disciplines. For instance, reflections on how to build interdisciplinary research emphasizes how there are several challenges involved. This includes creating the conditions for the integration between different disciplinary approaches and epistemologies and also reflecting on the outputs of this type of research (Stewart and Claeys, 2011). However, the very notion of inter-disciplinary research seems to involve a separation among disciplines that altogether try to reach a shared agreement on their different provinces of knowledge.

Other starting points are however available. Having different disciplines working together but each defending its own territory of knowledge (Hunsinger, 2005), might not be necessarily the only direction to take, nor the best approach to follow. Transdisciplinarity, for instance, offer a different starting point: an approach that goes beyond (that transcends) traditional divisions among disciplines, an approach in which the solution to problems can be tackled by common shared repertoires of concepts and actions. We are convinced that the limitations and challenges of the Future Internet need to be addressed with a transdisciplinary perspective, rather than with an interdisciplinary one. Creating transdisciplinary research, however, is not an easy task in itself and requires – we think – moving step-by-step.

Recent research conducted by the authors has focused our attention on the problem of trust[2] for the Future Internet:

> *The challenge is to obtain a greater understanding of how to create, obtain, assess, perceive or negotiate trust by taking into account information and context, and to use this understanding to realise a high level of trust by the citizen in the deployment, economic viability and social acceptance of systems and services* (Clarke, 2008).

Indeed, among the various challenges faced by the Future Internet the problem of trust seems to require special attention, as this is clearly an area where different disciplines and conceptions of trust not only meet, or even clash sometimes, but also require a common effort for addressing current and future challenges. As Clarke (2008) says, trust in the Future Internet: "*will require expertise and joint research in a broad set of disciplines that includes sociology, governance, economics and legal, as well as technology*". The problem of how we can begin to tackle this common effort – and especially the collaboration between Sociology and Computer Science – is the focus of this paper. In this work therefore we begin describing our transdisciplinary approach to trust research, that we define as *Trust as Result*. We also identify and propose the use of a theory – the Assemblage Theory as described by DeLanda (2006) – that can serve as a shared platform for building a transdisciplinary research agenda around trust for the Future Internet. In the concluding section of this paper we list some aspects of a research agenda for trust as transdisciplinary research area.

This paper is organized as follows: In section 1, we briefly describe the problem of trust for the Future Internet. In section 2, we position ourselves under the umbrella of "ICT and Society" as transdiscipline. Section 3 reviews the current mainstream interdisciplinary approach to trust and introduces Trust as Result[3]. In section 4, we introduce the concept of assemblage as a shared

[1] See Section 2 of this paper for a discussion.

[2] These include that many of us work in the area of Trust research or in areas in which Trust is important. In addition Trust seems to be a promising research area for transdisciplinary research, given that as a research problem it overlaps several disciplines.

[3] For Trust as Result and Trust Modelling we use capital initials, as they are names of design paradigms.

"platform" for building transdisciplinary research on trust. Section 5 explicates an empirical example that supports our point of view, followed by discussion of transdisciplinary research agenda on Trust as Result in Section 6.

1. The Problem of Trust

Trust is considered one of the key challenges for the Future Internet and under many aspects we can consider it as a sort of privileged ground for interaction among disciplines in Information and Communication Technology (ICT) and Society (ICT&Society). It is clear to everyone that the challenges of trust for the Future Internet cannot be solved purely in technological terms, and Social Sciences are required to play a prominent role. The ways, however, Social Sciences and Computer Science can collaborate on this challenge should be discussed carefully as this has important implications for both the design of our computerized artifacts as well as for users.

To begin with, we would like to recall how the European Advisory Board "Research and Innovation on Security, Privacy and Trustworthiness in the Information Society" (RISEPTIS) described the crucial role of trust for the Future Internet:

> *Trust is at the core of social order and economic prosperity. It is the basis for economic transactions and inter-human communication. The Internet and the World Wide Web are transforming society in a fundamental way. Understanding how the mechanisms of trust can be maintained through this transformation, is of crucial importance* (RISEPTIS, 2009).

This is the opening statement of the report entitled *Trust in the Information Society* that describes a series of policy recommendations to promote research and initiatives to tackle the challenges of trust. As we can see this report begins by describing trust as the core of social order.

Sociologists have indeed widely described how social order is strongly based on trust (Luhmann, 1979 and 1988, Giddens, 1990, Gambetta, 1988, Sztompka, 1999, Hardin, 2006). For instance, the German sociologist Nicklas Luhmann (1988, p. 103) defined trust as "an attitude which allows for risk-taking decisions". Trust, for Luhmann, is directly related with the subjective ability to assume risk-taking decisions, in those situations in which we posses scarce knowledge about the possible outcomes of our actions. For instance, when we decide to deposit our money in a bank, we are initiating a trust relationship with the bank as we cannot be sure that our money will necessarily be safe, and we trust the bank to keep our savings safe. As such, trust helps social actors to reduce complexity in the presence of several alternative actions (e.g. keep the money at home or deposit it in a bank). A further example is when we decide to leave our baby with a babysitter: this action involves initiating a trust relation between ourselves and the babysitter and from our side a reduction of complexity as all the possible outcomes of this action (will the baby be safe or not?) cannot be foreseen by applying a rational calculation. Trust is therefore used by social actors when pure rational calculation of the advantages/outcomes of action is not possible.

Trust is certainly a key sociological problem. However, sociologists are perhaps unaware that today Computer Science research uses sociological concepts to design trustworthy services and applications. To a large extent, this shift from a "pure social" trust to an informational trust might be defined as e-trust (see on this Floridi and Taddeo, 2011). The problem for us however is not to discuss whether there is a difference between trust and e-trust, our focus is the collaboration among disciplines: we are interested in how Sociologists and Computer Scientists work together on the problem of trust for the Future Internet.

The problem of what is trust for the whole field of computing is outside the scope of this paper. However, a brief introduction, that mirrors the above brief introduction to the sociology of trust, will help to frame the problem.

In Computer Science, trust emerged as a problem during the 1960s and 1970s as part of the military's effort (especially in the United States) to control access to information in networked computer systems (see for instance DoD, 1983). For instance, Nibaldi (1979) explains that "Trusted

computer systems are operating systems capable of preventing users from accessing more information than that to which they are authorized". Trust in these systems was literally generated by enforcing rules – called security policies – on the basis of which a system could assess whether a user (but this is valid also for computer programs themselves) is trusted to access information. In the Computer Security dictionary, a security policy is a statement which regulates how active entities – such as users – in computer systems can access information (in which context, at what time or according to what laws, standards, organizational rules and so on). This kind of approach to trust is known as *Access Control* (Lee, 1999).

With the advent of distributed systems – such as large computer networks, with multiple terminals – we have witnessed a shift in the complexity of trust: "the system access control policy", rather than being a single statement/rule enforced by a single operating system, "is more likely to be a composite of several constituent policies implemented in applications that create objects and enforce their unique access control policies" (Abrams and Joyce, 1995). Distributed systems require a more complex trust based on the dynamic creation and enforcement of security policies. With the Internet – that can be seen as a very large distributed system – this problem of multiple policies implemented in multiple services, produces enormous complexity. By reformulating this problem not just in technological terms, we can say that the Internet is a huge ensemble of systems, platforms, applications, services, people, companies, public administrations and other stakeholders that are located all around the globe in locations that have different systems of laws, cultures, economies and requirements. In this scenario, generating trust on the basis of universal rules – such as security policies – that can be enforced dynamically or decided upon in a secure way is therefore a very complex and challenging task. Designing systems that can provide effective solutions to this complexity is a challenge for Future Internet research, and computer scientists are relying more and more on the knowledge that social sciences gave on trust. It is precisely here that Sociology and Computer Science are required to work together and find common solutions to a shared problem[4].

2. A Note on the Concept of Transdisciplinary Research

The scope of this section is not to provide a literature review on the works discussing transdisciplinary research, especially in the area of ICT & Society. More modestly, we would like to position our work under the umbrella of the call for papers of "ICT & Society as transdiscipline" and link this area with the problem of trust for the Future Internet. Indeed, we are not ourselves transdisciplinary theorists, but rather a group of people belonging to different disciplines (Sociology, Computer Science) trying to approach a common research problem. In this light, we agree with Helga Nowotny (2004) when she said that: "If joint problem solving is the aim, then the means must provide for an integration of perspectives in the identification, formulation and resolution of what has to become a shared problem". Therefore our approach to ICT & Society as transdiscipline is practical rather than theoretical and focuses on the identification, formulation and resolution of the problem of trust for the Future Internet.

We would like to begin our discussion of this problem by referring to an interesting paper by Stewart and Claeys (2011) that helps us to clarify our terminology. In this paper the authors follow a distinction between interdisciplinary and multidisciplinary research that was proposed by the OECD[5]. Interdisciplinary is an adjective describing the interactions among disciplines whereas multidisciplinary is a mere juxtaposition of disciplines. Interdisciplinary research involves the communication of ideas and working toward a possible integration of disciplines. There are therefore important qualitative differences between multidisciplinary (simple juxtaposition) and interdisciplinary research (communication and integration). However, we must note, in both cases there is a separation between disciplines. Differently, transdisciplinary research approaches the object of study beyond and across disciplinary and interdisciplinary perspectives (Nicolescu, 2003; Nowotny,

[5] Organisation for Economic Co-operation and Development, http://www.oecd.org

2004; Hunsinger, 2005). As Nowotny (2004) argues, the semantic implied in these terms is not of secondary importance:

> *transdisciplinarity has a semantic appeal which differs from what one often calls inter- or multi- , or pluri- disciplinarity. Note that the prefix - trans- is shared with another word, namely transgressiveness. Knowledge is transgressive and transdisciplinarity does not respect institutional boundaries.*

There are therefore different starting points for interdisciplinary and transdisciplinary research. In the first case (interdisciplinary) we work toward an integration of two or more separate and distinct entities, but we are asked to respect institutional boundaries and different epistemologies and approaches. In the second case (transdisicplinary) the goal is to start from the beginning by rejecting these boundaries, and aim to create a shared repertoire of concepts that transcends differences.

We can now go back to the Future Internet and to Internet research more generally. In this regard, according to Hunsinger (2005, 277), Internet research is clearly "building a body of knowledge that is pertinent to many disciplines". In the interstices between different and various disciplinary knowledge about the Internet, there are spaces and problems that require collaborative efforts to solve substantive problems. Trust is clearly one such problem. A transdisciplinary effort is arguable here to solve these shared problems because, as Hunsinger (2005, p. 278) points out, by focusing on disciplinary knowledge: "Internet research could end up being fragmentary, and to some extent unintelligible as it progresses". On the contrary adopting a transdisciplinary approach enables one to avoid this fragmentation of knowledge: "because it has been recontextualized for the broader audience of multiple disciplines, is more accessible and interpretable." We follow Hunsinger (2005), arguing for a transdisciplinary approach for Internet, and especially for trust research.

3. Trust Modelling and the Interdisciplinarity of Trust

The mainstream computing approach that seeks to take advantage of sociological approaches to the problem of trust - an approach that we call *Trust Modelling* - is based on the idea that it is possible to "*capture the essence of trust*" and implement it in computer systems (see for example Sabater and Sierra, 2001; Jøsang et al, 2007; Nielsen and Krukow, 2003; Carter and Ghorbani, 2004). We take this statement on *capturing the essence of trust* from a paper by Varadharajan (2009) entitled A *Note on Trust-Enhanced Security.* This paper is very paradigmatic of the trust Modelling approach . For instance the author states:

> *From a Computer Science viewpoint we can think of software agents and computing machines as representing humans, reflecting complex trust relationships and exhibiting the behavioral patterns of human social interactions* (Varadharajan 2009, p. 57).

Following this argument, "trust models" that can guide the development of Trusted Systems can be: (1) formulated and extrapolated from social dynamics and contexts and (2) formalized as computer programs by using various forms of representations to achieve trust. Trust Modelling seeks to reproduce in a computerized form modelled social dynamics. In other words, this approach considers trust through an 'objectivity' lens: trust is a decontextualized object that can be captured in its essence and that can be implemented as such in computer systems.

Trust Modelling can be seen as an approach that sees or postulates a division/separation among disciplines, even though this approach clearly implies also some forms of integration and communications of ideas between disciplines (Figure 1). In trust Modelling the relations between disciplines are as follows: Social Sciences produce social models of trust based on their empirical research, after that this model is communicated to Computer Science which integrates and implements it in computer systems. Trust Modelling assumes that Computer Scientists should not know

much about social dynamics - they just want to have an implementable model from Sociologists - and Sociologists should not take part to design and implementation of systems - their goal is to communicate the trust model to their colleagues.

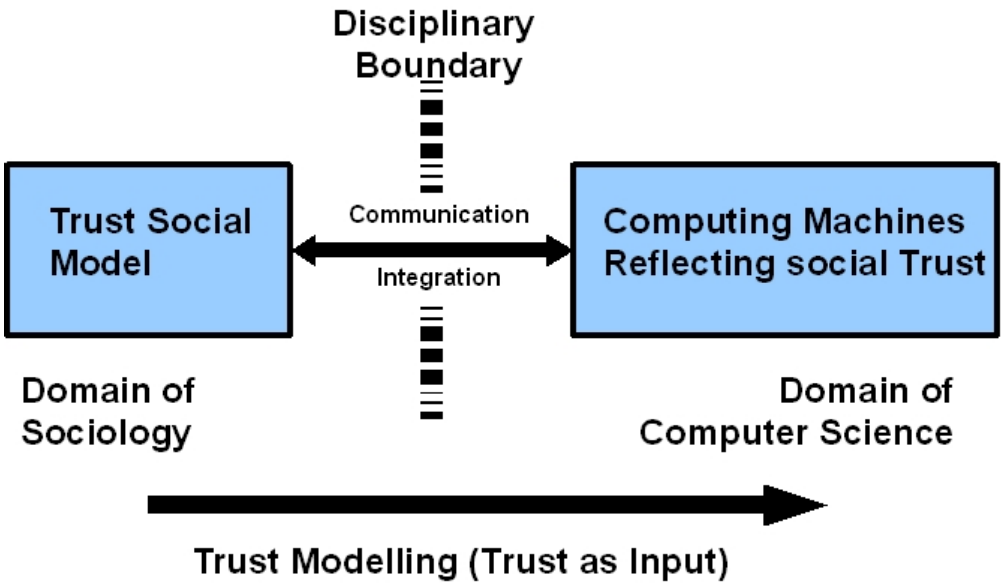


Figure 1: Trust Modelling, an interdisciplinary approach

Our opinion is that Trust Modelling ignores a whole range of social and technical epistemological issues. For instance, according to Nissenbaum (2004), nothing can ensure that Trust Modelling will generate trust as an outcome of the system design, development and deployment. It seems to us that Trust Modelling makes only sure that a formalized trust model is used as input in the design of trustworthy services and applications.

While the interdisciplinary approach of Trust Modelling is certainly a possible direction to take for the Future Internet, it is also based on the existence of strong boundaries between disciplines and on a binary subject-object model that undermines the situation. Indeed, in this approach the sociological research produces a subjective trust model – which is universal - and computer science implements – objectifies – this universal model which is enforced back on particular situations.

4. Toward a Transdisciplinary Trust: The Assemblage Theory

Based on the previous discussion, we argue for a different approach to build trust for the Future Internet as transdisciplinary research. Our goal is to begin devising a transdisciplinary agenda for the "design-for-social-trust" technology whose goal is to enable a novel, collaborative, and socially accepted way of creating trust for the Future Internet. Our vision considers therefore not bridging disciplinary differences under the umbrella of an interdisciplinary approach, but rather building from the beginning a shared repertoire of concepts and actions that can transcend disciplinary differences. Embracing a transdisciplinary view can help include what is in-between disciplinary differences (Nicolescu, 2003).

In this line of reasoning, a good approach to conceptualizing trust would be that of seeing it as an effect - a result - of the interrelations between social and technical elements in the form of an assemblage and not as a sort of objective (pre)condition for interaction. Therefore, trust has to be built together with the interrelation of various socio-technical entities (people, services and so forth) and not as its presupposition (as for Trust Modelling). Trust is not an essence, which explains social order (*explanans*) and that can be captured and objectified, but rather an outcome (*explanandum*) – the result – of the relations among entities. This perspective, we believe, can lead to

a new understanding of trust (and also mistrust) in different Internet domains. In this light, we believe that the problem of Trust as Result, and the complexity and the interrelation of a variety of social and technical things / elements / entities that compose trust for the Future Internet can be viewed from the perspective of Assemblage as proposed by Manuel De Landa (2002 and 2006).

The concept of assemblage considers that social and technological entities should be characterized not on the basis of their essential properties and necessary relations as happens with for example the concept of 'system'. The concept of system, in both natural and social sciences, is also – like the assemblage - based on a conceptualization of the relations among elements that form a whole. The relations among parts of a system are however necessary and as a consequence the failure of one relation leads to the failure of the whole system. For example, the organs that compose a human body (e.g. heart or brain) are elements of a system (the body) that are in necessary relations with one another (if one organ fails to function the whole system is likely to fail). In social sciences the concept of 'social system' draws on a parallelism with natural systems, in which social institutions (for example religion or economy) are necessary for the integration of societies (Parsons, 1951). For example, the lack of ethical norms might lead to anomie in society (Durkheim, 1951) and to a disintegration of the social system.

The dynamics of an assemblage are different from that of a system. The entities composing the assemblage are characterized on the basis of what they are capable of doing when they interact with one another. These capacities depend on the entity properties but cannot be reduced to them since they involve an interrelation with other interacting entities. The concept of assemblage is useful to investigate the processes and inter-relational dynamics encompassing changes according to the different roles of entities in different assemblages. Entities in an assemblage can have material/expressive and territorialization/deterritorialization capacities. Here we focus on the second set of capacities (for a discussion see DeLanda, 2006).

According to DeLanda (2006, p. 13), 'Territorialization' is a process that 'increases the internal homogeneity of the assemblage' and that induces a stabilization of the relations within an assemblage. On the contrary, deterritorialization does the opposite, decreasing the homogeneity of the assemblage and destabilizing the relations among the elements. The entities can play also a mixture of territorialization / deterritorialization capacities.

The dimension of territorialization / deterritorialization relates to a spatial process, such as the difference between a face-to-face communication (territorialization) and a computer mediated communication (deterritorialization). An interesting example is the city as a territorialized entity/assemblage located in a specific area as opposed to nomadic groups that are deterritorialized and move on a rather large territory. This dimension of the assemblage also relates to non-spatial dynamics. DeLanda (2006) argues that territorialization can be a process which excludes a certain category of people from the membership of an organization or a group: this creates homogeneity among the members of that organization. Following the above dimension of the assemblage, we can have a process of stabilization/consolidation (territorialization) and of destabilization/dissolution (deterritorialization) of the assemblage.

5. An Example of Trust as Result

In our opinion, the complexity of building trust for the Future Internet can be tackled by using the assemblage perspective. We consider the Assemblage Theory an useful approach for building a shared platform for transdisciplinary research on trust. We provide an example from our research into cheating in Massively Multiyplayer Online Role-playing Games [MMORPGs] that illustrates the possibility of using the assemblage to reflect some issues related with Trust as Result. We illustrate the Assemblage approach with an example based on the research we are currently conducting on two MMORPGs: 1) Tibia, a 2D medieval game developed by Cipsoft, since 1997, with 120 thousands players and (2) World of Warcraft, a 3D fantasy game developed by Blizzard, since 2004, with a base of 10 million players.

MMORPGs are a successful sub-sector of the digital games industry whereby players participate in a persistent virtual world (Bell, 2008). MMORPGs are sophisticated technological as well as

complex social worlds (Castronova, 2005; Taylor, 2006) where millions of players cooperate, compete, and trade online.

MMORPGs have a number of specific characteristics. There is no need to describe them in-depth here (see for a discussion Kerr, 2006). However, we mention some interesting aspects.

An MMORPG is considered persistent because it is an online world that continues to function even after individual players have logged out and stopped participating. This is different from traditional digital games played by a single person or small groups, whereby the game ceases after the player(s) has logged out.

In many MMORPGs players usually assume a fictional role or character (via an avatar). A character's role determines her characteristics in many ways and different roles allow different types of gameplay, of attack and combat with both monsters and other characters. In a medieval-fantasy game, for instance, a Knight character might have particular abilities with melee weapons (such as swords or axes). By comparison, a Druid may have better abilities at casting spells and healing.

A further characteristic relates to the advancements that are obtained by players. The main activity in MMORPGs is levelling the character. This is carried out by players by killing monsters. By killing these monsters players can increase the level/experience of their avatar and in so doing increase their overall game ranking.

MMORPGs are particularly affected by cheating (ENISA, 2008). Cheating in MMORPGs involves a game player using non-standard or even illegal methods for obtaining an unfair advantage over other players. Cheats include duplication of items via exploitation of bugs or design weakness, or the use of software (often known as bots) to automate certain tasks, or again direct collusion with other players, and the manipulation of other players trust (See for a complete list Yan and Randell, 2004).

5.1. Architecting Trust in MMORPGs

A crucial element of MMORPGs is the 'architecture', the way by which computers involved in the game communicate and network with each other. The most common architecture used by MMORPG game companies is the client-server, which consists of a centralized server under the direct control of the company with several clients (the players' machines) connected to it (see figure 2), which are largely outside the direct control of the company. Most of the program-game code (software) is executed on the server, whereas the client only controls a small fraction of the code. Thus, the communication among computers involves a client sending a request to the server, the server validating, or not, the request, and then the server sending the request to all other target clients.

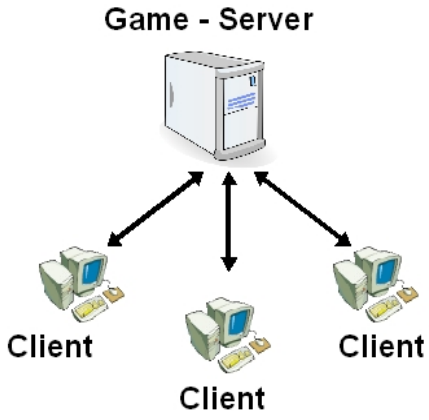
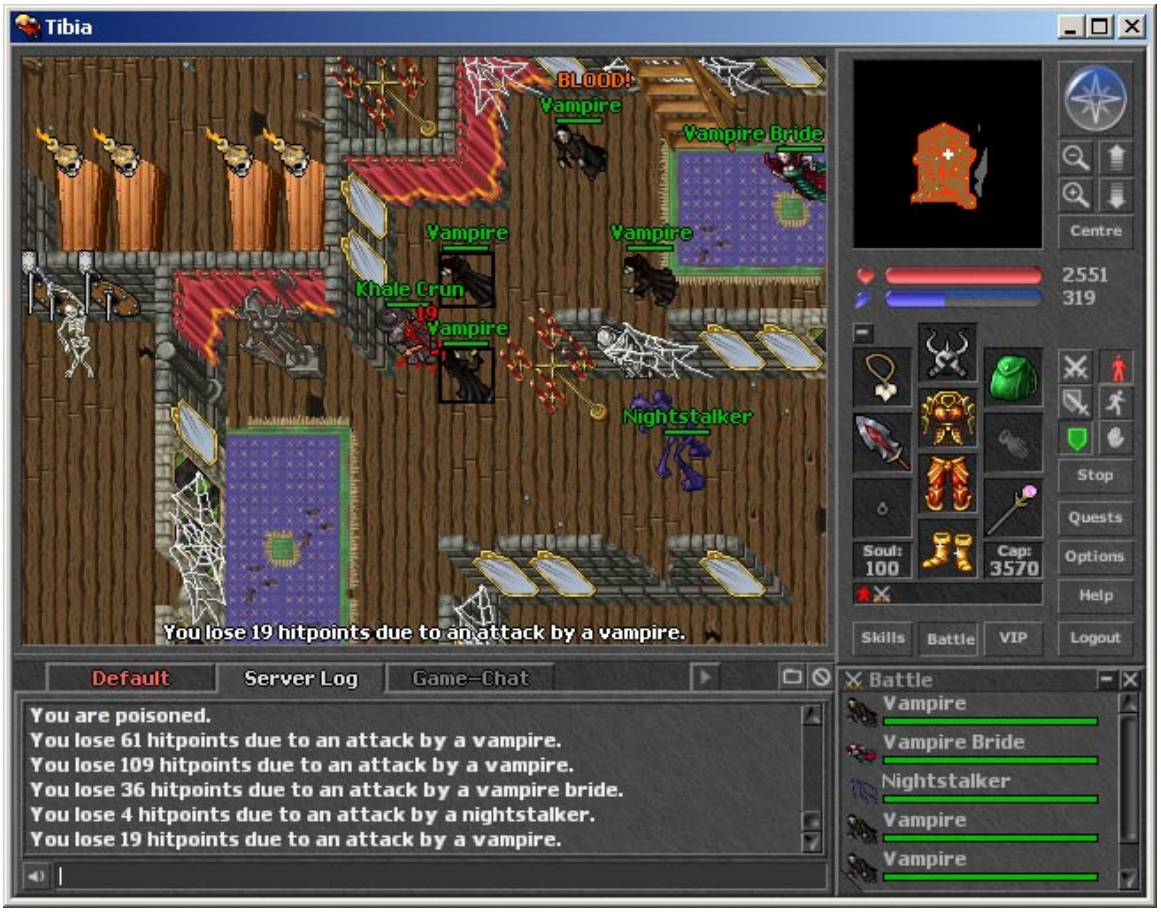


Figure 2: Client-Server architecture

For example, when a Tibia character such as *Khale Crun*' (Figure 3) kills a monster (such as a 'Vampire'), this action must be validated by the server and then the outcome of this action (the increase in level obtained by '*Khale Crun*') must be communicated back by the server to all the other



clients. In addition, because the server must validate all the requests made by the clients, it can also deny certain actions (for example, deny '*Khale Crun*' to enter the house of an enemy guild[6]).

Figure 3: An example of a Tibia character (Khale Crun) killing monsters (Vampires in this case)

The client-server architecture instantiates a set of trust relations including the game companies that control the game servers, the players that control the clients, the game code, the network communications, legal documents such as the End User license agreement and so on. This consideration is well supported by (Pritchard, 2000) as follows:

> *In client-server games, because so much is controlled by the server, the game is only as good as the trust placed in the server and those who run it.* […] And as a golden rule for game programmers he says "*Rule #8: Trust in the server is everything in a client-server game.*

Following (Pritchard, 2000), we conceptualize the client-server as a trust relation in the sense that in principle there is no trust at all in the game clients and that for game developers and providers all trust stays on the server. One of the reasons why the client-server architecture is preferred by game developers is because by executing a large part of the game on the server (including tak-

[6] In MMORPGs a guild is a group of players who share the same goals and collaborate to achieve them.

ing the most important game decisions), it is possible to keep the gaming activities under control (Kabus et al., 2005). In other words, gaming activities on the server are trusted.

Other architectures such as peer-to-peer offer the developers no control over gaming activities that are spread all over the network of peer computers. In other words, they are untrusted. All the information manipulated by the game clients implies in fact a degree of risk, in terms of cheating. It is easier to manipulate the code executed on the clients machines or on the peer nodes. In this regard the client-server architecture offers more trust than the peer-to-peer, because of the control that can be exercised by game companies. The client-server architecture is a trust relation that, implies a terrritorialization in which there is an attempt to reduce the range of possible cheating actions by exercising control over the execution of the game code: it is quite difficult to, for example, modify and exploit the code of the software stored, executed, and manipulated on the server, whereas by contrast, it is relatively easy to exploit the code stored and executed on the client. This observation is valid in general: all the game information and code controlled and executed on the client machines - including files, memory, drivers, services and so on - can in principle be manipulated illegally (Pritchard, 2000).

Therefore, the client-server architecture possesses a specific spatial territorialization capacity in which the game code is executed on the servers in centralized spaces, rather than being deterritorialized onto the player's machines. In technical terms this is often referred to as 'centralization', the idea that access, resources, and data security are controlled almost exclusively via the server. Centralization places all trust in the server.

However, the spatial territorialization of the architecture (the centralization) can never be total. Indeed, for performance reasons, all the game states cannot reside on the server. For example, Hoglund and McGraw (2008, p. 142), describe the organization of the data structure[7] of a MMORPG's character, and state that *"Clearly these data must be stored on the game server, but sometimes the client program controls the values directly"*. If the client controls some of the values of the character's data structure, then an expert programmer could easily manipulate these values to obtain an unfair advantage (for example increasing a specific skill of that character, by manipulating the values that refer to the skill). Another example comes from online Real-Time Strategy games where sometimes it is possible to illegally manipulate the client information that controls the "unexplored areas" of the map (Pritchard, 2000). This can bring an unfair advantage by allowing a player to know the location of enemy units. In conclusion, we always have some degrees of deterritorialization of information in the client-server architecture, an information that becomes less trusted therefore.

5.2. Deterritorializing Trust

One way that game companies can enhance the trust relation between their servers and the player clients is by using technologies known as anti-cheating tools. Anti-cheating tools are software devices that automatically enforce the terms of legal documents of a game: here we can investigate an instance of the enforcement of statements/rules as way to build trust, as described before.

To understand the functioning of anti-cheating tools, we briefly describe the operation of a well known anti-cheating tool known as 'the Warden' (Blizzard, 2005), used in the game World of Warcraft (WoW). Basically, when the player connects the client to the WoW server, the Warden is downloaded from Blizzard servers onto the user's client machine. The Warden is composed of small portions of code that are dynamically assembled at each download. This means that each Warden is different from one another and therefore it is difficult to create (cheating) code that can circumvent it. Indeed, if a cheater 'captures' a Warden and creates a software countermeasure then this measure will not be effective because the next Warden(s) downloaded onto the users' machines will be different from the captured one (Hoglund and McGraw, 2008).

[7] The data structure is a way of storing and organizing computer data.

The Warden operates in a manner similar to a spyware (Terdiman, 2005), scanning the RAM[8] of player machines and doing other intrusive actions such as making screen-shots of the user's computer screen and sending them back to the game servers. The Warden searches for code executed on the users' machines and compares it with a dictionary of WoW known cheating code, which is maintained on Blizzard servers. If the code executed on the user machine matches some of the cheating code in the dictionary, then this triggers a punishment such as a ban or even deletion of a game account. Interestingly the Warden operates a double movement of territorialization-deterritorialization. Indeed, the control over possible illegal actions (as defined in legal documents) is not in the first instance exercised on the company servers, but it is deterritorialized onto the users' machines: the Warden continuously monitors what is happening on users' machines and only at a second stage it reports the information back to the server, hence operating a territorialization.

In this way the trust relations between the game server and the clients can be strengthened, by the use of anti-cheating tools that possess territorialization and deterritorialization capacities. In conclusion, trust is not a model used as input but a relation among parts that gets realized as an outcome of the assemblage dynamics.

6. Discussion and Conclusion: Toward a Transdiciplinary Trust Research Agenda

Early in the paper, we briefly described the interdisciplinary approach of Trust Modelling whose goal is to implement social models of trust in computer systems. This approach, although implying some exchange of ideas between disciplines (in particular Social Sciences and Computer Science), embodies in practice a disciplinary boundary between the social model produced by Sociology and the implementation of the model by Computer Science. This also implies a separation between the social and the technical.

We have described what we consider some of the limits of the Trust Modelling approach and said that a good approach to conceptualizing trust for the Future Internet would be that of seeing it as an effect (a result) of the interrelations between elements in the form of an assemblage. Via the support of the gaming example, it is interesting to see how the Assemblage Theory, allows us to reflect around the dynamics of trust as an outcome-result: trust is a negotiated socio-technical process, that does not stabilize easily and it is based on the interrelation of several entities and their strategies often focused on reducing the risk of exploitation: this includes the game companies, the players, the anti-cheating industry with their tools, the cheaters and the cheating companies, an array of computers (including server and clients) and code, such as the game code and so on. Trust is the result of the interrelations among these entities and their strategies and not something that could be applied on them from outside.

Our position therefore is that trust is not an essence, which explains social order (*explanans*) and that can be captured and objectified, but rather an outcome (*explanandum*) – the result – of the relations among entities composing an assemblage. This perspective, we are convinced, can lead to the design of novel systems that might support human production and understanding of trust and mistrust in practice in different domains for the Future Internet.

This observation can constitute the basis for a new research agenda. Indeed, moving toward a transdisciplinary agenda for trust for the Future Internet requires re-articulate and re-conceptualize the following elements of current design of trust:

1. It is important to focus on trust as the outcome of the design process (Trust as Result), and not on trust as a precondition-input (Trust Modelling) embedded in a model, subsequently implemented in computer systems. This Trust as Result can be achieved no just by integrating different disciplines, but rather with an approach that transcends disciplinary boundaries.
2. It is important for disciplines to work and collaborate on the creation and enhancement of a transdisciplinary conceptual framework for trust, grounded on a shared repertoire of concepts.

[8] Random Access Memory is a writable and volatile computer memory.

This can be achieved by identifying from the beginning concepts that can serve this goal, rather than try to mix already developed concepts often based on different epistemologies.

To achieve the previous goals:

3. it is important to focus on the hybrid nature of trust, that involves already a mixture of technical and social.
4. Finally it is important to rely on concepts that transcends common assumed separations. In our case we argue for the Assemblage Theory for designing trust. Other solutions however are not only possible, but also desirable in order to increase the repertoire of transdisciplinary approaches.

In conclusion, we are aware that the design of trustworthy ICT for the Future Internet requires more than just reshaping a few assumptions of the design, leaving intact the current core elements of systems design theories. Shifting from Trust Modelling (Trust as Input) to Transdisciplinary trust (Trust as Result) implies also a politics of transdisciplinarity. Indeed, we live in a world populated by Epistemic Cultures (Knorr-Cetina, 1999), in which how we know and what we know are often difficult to change. Current thinking in term of trust as it relates to ICTs is strongly bounded with a core set of assumptions that cannot just be modified on the basis of pure technology success. Therefore enhancing a transdisciplinary trust agenda for the Future of the Internet is also a political problem. We do not have yet an answer on how to solve the techno-political challenges we are facing, but we are convinced of the importance of working toward this goal and this paper is a first concrete effort in this direction.

References

Abrams M. D. & Joyce M. V. (1995). Trusted Computing Update. *Computers and Security*, *14*(1), 57-68.

Bell, M. V. (2008). Toward a Definition of Virtual Worlds. *Journal of Virtual Worlds Research 1*(1), Retrieved from http://journals.tdl.org/jvwr/article/download/283/237

Blizzard Entertainment (2005). A Statement on Our Hack-Scanning Process. Retrieved from http://web.archive.org/web/20051211091852/http://forums.worldofwarcraft.com/thread.aspx?fn=blizzard-archive&t=33&p=1&tmp=1

Bled Declaration (2008). Retrieved January 10, 2010 from http://www.fi-bled.eu/Bled_declaration.pdf

Carter, J. & Ghorbani A. A. (2004). Towards a formalization of trust. *Web Intelligence and Agent Systems, 2*(3),167-183.

Castronova, E. (2005). *Synthetic worlds: The Business and Pleasure of Gaming.* Chicago: Chicago University Press.

CipSoft (2009). Second Patch Teaser: Stamina, Experience Counter and More. Retrieved from http://www.tibia.com/news/?subtopic=newsarchive&id=945&fbegind=29&fbeginm=2&fbeginy=2009&fendd=29&fendm=3&fendy=2009&flist=11111111

Clarke J. (2008). "Future Internet a Matter of Trust", URL: http://www.tssg.org/eMobility_Newsletter_200811.pdf

DeLanda M. (2002). *Intensive Science and Virtual Philosophy.* London: Continuum.

DeLanda M. (2006). *A New Philosophy of Society: Assemblage Theory and Social Complexity*. London: Continuum.

Department of Defense (1983). *Trusted Computer System Evaluation Criteria*. Retrieved from http://nsi.org/Library/Compsec/orangebo.txt

Durkheim, E. (1951/1897). *Suicide: A Study in Sociology*. Glencoe: The Free Press.

ENISA (2008). Virtual worlds, real money security and privacy in massively-multiplayer online games and social and corporate virtual worlds. Retrived from http://www.enisa.europa.eu/pages/02_01_press_2008_11_20_online_gaming.html

Floridi L. & Taddeo M. (2011). "The Case for e-Trust". *Ethics and Information Technology,* 13(1), 1-3.

Gambetta, D. (1988). *Trust: Making and Breaking Cooperative Relations.* Oxford: Blackwell.

Giddens, A. (1990). *The Consequences of Modernity*. Cambridge: Polity Press.

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

Hoglund, G. & McGraw G. (2008). *Exploiting Online Games: Cheating Massively Distributed Systems*. First Addison-Wesley Professional.

Hunsinger J. (2005). Toward a Transdisciplinary Internet Research. *The Information Society, 21*(4), 277-279.

Kabus, P., Terpstra, W. W., Cilia, M. & Buchmann, A. P. (2005). Addressing cheating in distributed MMOGs. *In Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support For Games,* New York: ACM, 1-6.

Kerr, A. (2006). *The business and culture of digital games: gamework/gamplay.* London: Sage.

Knorr-Cetina K. (1999). *Epistemic Cultures: How the Sciences Make Knowledge.* Cambridge: Harvard University Press.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems, 43*(2), 618-644.

Lee, S.E. (1999). *Essays about Computer Security.* Retrieved October 2008 from http://www.cl.cam.ac.uk/~mgk25/lee-essays.pdf.

Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives'. In Gambetta D. (Ed.) *Trust: Making and Breaking Cooperative Relations*, (pp. 94-107). Oxford: Blackwell.

Luhmann, N. (1979). *Trust and Power.* New York: John Wiley.

Nibaldi, G.H. (1979). *Proposed Technical Evaluation Criteria for Trusted Computer Systems.* Bedford: MITRE Corporation.

Nicolescu, B. (2003). *Manifesto of Transdisciplinarity.* State University of New York Press.

Nielsen, M. & Krukow, K. (2003). Towards a formal notion of trust. I*n PPDP '03: Proceedings of the 5th ACM SIGPLAN international conference on Principles and practice of declaritive programming* (pp. 4-7). New York: ACM Press.

Nissenbaum, H. (2004). Will Security Enhance Trust Online, or Supplant It?. In Kramer R. & Cook K. (Ed.) *Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions,* (pp. 155-188). Russell Sage Publications.

Nowotny, H. (2004). The Potential of Transdisciplinarity. Retrieved from http://helga-nowotny.eu/downloads/helga_nowotny_b59.pdf

Parsons, T. (1951). *The Social System.* Glencoe: Free Press.

Pritchard, M. (2000). How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It', *Gamasutra.* Retrieved from http://www.gamasutra.com/features/20000724/ pritchard_pfv.htm

RISEPTIS (2009). *Trust in the Information Society*. Retrieved from http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html

Sabater, J. & Sierra, C. (2001). Social ReGreT, a reputation model based on social relations. *SIGecom Exch*. *3*(1), 44-56.

Stewart, J. & Claeys L. (2011). Problems and Opportunities of Interdisciplinary Work Involving Users in Speculative Research for Innovation of Novel ICT Applications. In Pierson Jo, Mante-Meijer E. snd Loos E. (eds.), New Media Technologies an User Empowerment (pp. 101-122). Peter Lang: Frankfurt Am Main.

Stuckmann, P. & Zimmermann, R. (2009). European research on future internet design. *Wireless Commun. 16*(5*)*, 14-22.

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

Taylor, T. L. (2006). *Play Between Worlds: Exploring Online Game Culture.* Cambridge: MIT Press.

Terdiman, D. (2005). Game players say Blizzard Invades Privacy. *CNET News*. Retrieved from http://news.cnet.com/Game-players-say-Blizzard-invades-privacy/2100-1043_3-5830718.html

Yan, J. & Randell, A. (2004). A Systematic Classification of Cheating in Online Games. *In Proceedings of NetGames 05*, (pp. 1-9), Hawthorne: ACM Press.

Varadharajan, V. (2009). A Note on Trust Enhanced Security. in *IEEE Security & Privacy*, *7*(3) pp. 57-59.

Zittrain, J. (2008) *The Future of the Internet - and How to Stop it.* London: Yale University Press.