DIVSI

Deutsches Institut
für Vertrauen und
Sicherheit im Internet

DIVSI Decision-Maker Study on Trust and Security on the Internet

Condensed Version

www.divsi.de

DIVSI Decision-Maker Study on Trust and Security on the Internet

Condensed Version

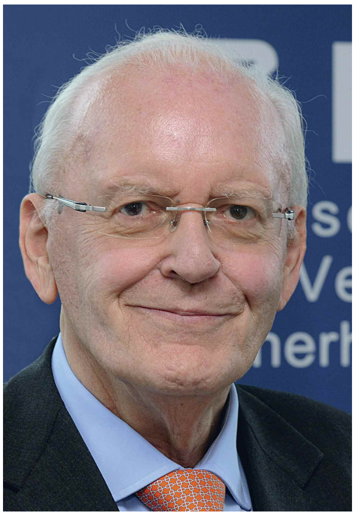
A study conducted by
SINUS-Institut Heidelberg
on behalf of
Deutsches Institut für
Vertrauen und Sicherheit
im Internet (DIVSI)

Heidelberg, February 2013

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 142, 20148 Hamburg, Germany
Matthias Kammer, Director
Joanna Schmölz, Head of Research
Dr Dirk Graudenz, Project Team Studies

SINUS-Institut, Heidelberg
Project Director: Dr Silke Borgstedt
Text: Dr Silke Borgstedt, Tamina Christ
Project Team: Matthias Arnold, Manfred Tautscher, Dr Marc Calmbach, Susanne Ernst

Contents



__Prof Dr Roman Herzog__, Patron of Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Foreword

When I agreed to become the patron for DIVSI in November 2012, I spoke during a Senate reception in the Hamburg Town Hall and addressed some of the burning issues raised for us all by the Internet. At that time, I noted the positive opportunities offered to us by the digital age, but also pointed out that their exploitation to the benefit of all will not be possible unless the unresolved questions are answered.

It seems to me that the experts have everything well under control in strictly technical terms, even though there will certainly always be something new, something surprising.

So what are the issues which must still be clarified? I made a clear statement of my position during this talk in the Hamburg Town Hall. There is little doubt that the course my life has taken inevitably leads me to a consideration of the constitutional questions raised by the subject. I am not claiming that the problems under discussion here revolve first and foremost around legal questions. But my experience has taught me that considerable progress can be made in answering the questions of ethics facing us today if we constantly remind ourselves to look over at our neighbours in constitutional law and listen to what they are saying.

I feel sure that questions of ethics will play an increasingly significant role in our digital age. Questions which virtually no one thought about at the beginning of the Internet age.

One of the tasks of the Deutsches Institut für Vertrauen und Sicherheit im Internet is to provide facts and background information based on generally accepted academic methodology. In the ideal case, the institute initiates interdisciplinary discussions which should ultimately come to conclusions with a common goal: ensuring that the positive aspects of the Internet can be used by everyone easily and without fear.

There is no question that the Decision-Maker Study presented here will prompt us to think in a number of directions. It will also encourage us to consider social and ethical questions from completely new angles. For the first time, and in a clarity never seen before, we can trace a possible socio-political upheaval in the results. This is for me one of the most fundamental revelations of this Decision-Maker Study.

One of the conclusions of this carefully prepared study is a source of major concern to me, namely: the Digital Vanguard among the decision-makers – the up and coming elite class of our country – displays the least trust of all of the study participants in our political system and even in the rule of law itself. This may be an indication of a growing disassociation from a state ruled by law and the guarantees given by the state.

What does this mean for our country and for the future of all of us? After all, the group of Digital Vanguard is the avant-garde among leaders. Is it possible that this natural process is steering us in the direction of a general crisis of confidence?

I do not intend to philosophise any further about this tendency revealed here in the study; I simply want to warn against dismissing it without a second thought. Discerning and describing a possible development is never anything more than the first step. We need to have trust in our political system, our state. I urge the people who bear responsibility for this system to take the findings of this study seriously.

I believe the study uncovers another tendency: our tonality, our interaction, our trust in one another appear to be suffering from increasingly greater strain. Blame and accusations are hurled back and forth, there is little faith that anyone – but especially politicians – will effect change for the better. The Internet illiterate are compared to Neanderthals.

I would like to see the focus shifted more to the community, the human aspects. Even – especially – in the Internet age. If we do not want to throw away the trust in the Internet, in the chances and opportunities it offers, we need a general discussion about the rules of the game that should be binding on us all. We need guide rails to keep us on the right path. A digital codex, honoured by all who bear responsibility, could be one possible route in this direction.

In any case, the Decision-Maker Study is highly suitable to initiate new discussions, as was the intention of DIVSI. Important issues of our time, empirically sound, have been put on the table. Let us accept the task – let us find answers!

__Matthias Kammer__, Director of Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Decision-Makers and the Internet

The release of the „DIVSI Milieu Study on Trust and Security on the Internet“ revealed the motivation factors and attitudes dominating the relationship of Germans to the Internet. The paper also describes the expectations people have with regard to security and data protection.

Just as almost all other investigations of the subject, the paper focused principally on the user perspective. The discussions about the study repeatedly gave rise to the question about responsibility for the Internet, about accountability for its structure. We have determined that very little is known about the people who actually shape the Internet. As we wanted to fill in this blank space, we commissioned an examination of a key question: Who are the decision-makers and doers for the Internet itself?

This DIVISI Decision-Maker Study, which has once again been carried out by the renowned SINUS-Institut, closes this gap. It expands the scope of our qualitative examination entitled „DIVSI Opinion Leader Study – Who Shapes the Internet?“ released in November 2012 into a nationwide representative study.

Who is behind the Internet? What opportunities to exercise influence do these actors have, how do they view users, what do they have to say about users’ needs for security and freedom? All of these questions are answered here.

Four essential statements can be derived from the results:

- Private-sector businesses are the drivers of current developments on the Internet. Companies are not simply actors who offer their products and services here. They also set the rules and change them continuously.

- No one is offline anymore. The Internet is becoming a significant factor in more and more areas of our lives. The distinction between online and offline spheres is becoming increasingly blurred.

- Decision-makers do not believe that a general responsibility for „the Internet“ is structurally possible, nor that it is desirable. Their solution is to pass responsibility on to the users to a substantial degree.

- It is becoming more and more difficult to establish generally valid regulations and mutual agreements for the negotiating space of the Internet. The focus of the discourse is rapidly moving from a purely technological perspective to the question of the „digital culture“.

Along with the empirical findings, the Decision-Maker Study reveals indications that a greater social upheaval is taking place. In comparison with all other decision-makers, the Digital Vanguard manifests the lowest level of trust in our political system and the rule of law in our state.

Those who are familiar with our first study will be struck by the differences, some of them major, between the views of the decision-makers and the attitudes and behavioural patterns of the general population ascertained last year. That study determined that 39 per cent of the people living in Germany are digital outsiders. That figure does not concern the decision-makers in the least. From their standpoint, the digital outsiders live in an environment which is marked more and more strongly by events in the online world.

The findings and conclusions of this study will certainly not be applauded by all. But that cannot, and must not, prevent us from presenting even unwelcome facts for discussion. If our commitment to the creation of a networked world which is more trustworthy and secure is to succeed, we must understand the situation as it actually exists.

With this in mind, I hope that the time you spend with the DIVSI Decision-Maker Study will be both informative and fascinating.

Matthias Kammer
Director DIVSI

1. Introduction: Why a Decision-Maker Study?

Business executives and social opinion leaders play a substantial role in shaping public attitudes related to issues of responsibility and trust on the Internet and consequently exercise major influence on what the general public thinks about the Internet. Surprisingly, however, we know virtually nothing about the way this group thinks about the Internet – a group which not only actively participates in this sphere, but to a large degree defines the rules of the game and has a dominant influence on general opinion.

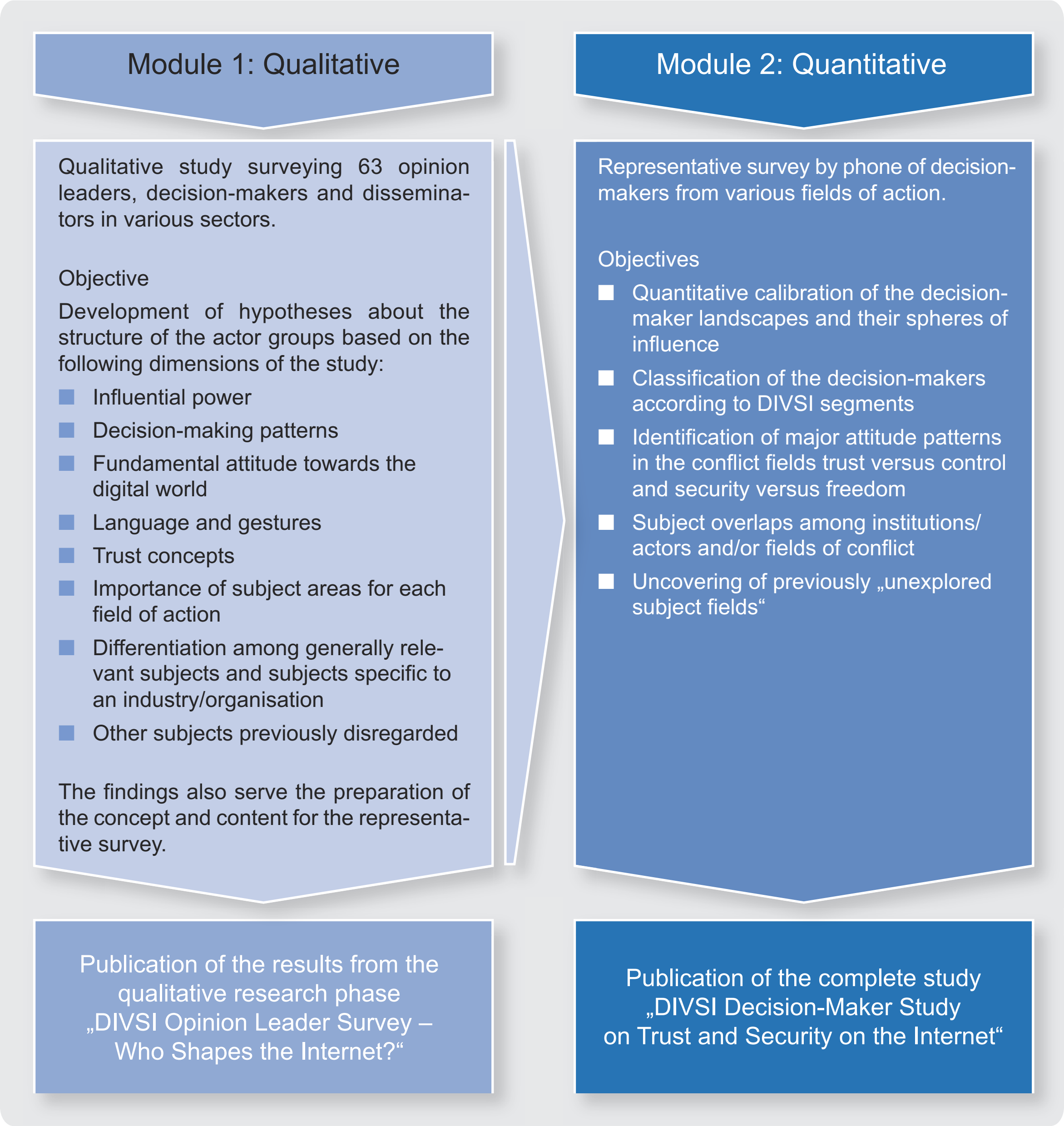
Conceived as a continuation and companion to the survey of the general population in the „DIVSI Milieu Study on Trust and Security on the Internet“ from February 2012, the DIVSI Decision-Maker Study gives representatives from business, politics, civil service, civil society, media, academics and research the opportunity to speak up. This study offers – for the first time – an overview of the digital milieus in the German decision-maker landscape and describes the fundamental attitudes of decision-makers towards the Internet and their requirements with respect to trust and security on the Net.

In the long run, if there is to be a feeling of trust in our use of the Internet, it is not enough for decision-makers to know what users are doing online; the users should also know how the decision-makers move around on the Net, what attitudes they have towards opportunities and risks and, equally important, what they think about users and other decision-makers and what they expect from these groups.

2. Methodology

The objective of the study is the description of key attitude profiles among German decision-makers with respect to various broad issues of trust and security on the Internet. Its scope is not restricted to viewing decision-makers as a single homogeneous block. The investigation delves more deeply into the fields of conflict among them (e.g. business versus politics) and their affiliation with the distinct digital milieus. The survey questions cover the sectors of data security/data protection, responsibility and trust.

A two-phase procedure was selected for use in the study.



Module 1: Qualitative

Qualitative study surveying 63 opinion leaders, decision-makers and disseminators in various sectors.

Objective

Development of hypotheses about the structure of the actor groups based on the following dimensions of the study:

- Influential power
- Decision-making patterns
- Fundamental attitude towards the digital world
- Language and gestures
- Trust concepts
- Importance of subject areas for each field of action
- Differentiation among generally relevant subjects and subjects specific to an industry/organisation
- Other subjects previously disregarded

The findings also serve the preparation of the concept and content for the representative survey.

Publication of the results from the qualitative research phase „DIVSI Opinion Leader Survey – Who Shapes the Internet?“

Module 2: Quantitative

Representative survey by phone of decision-makers from various fields of action.

Objectives

- Quantitative calibration of the decision-maker landscapes and their spheres of influence
- Classification of the decision-makers according to DIVSI segments
- Identification of major attitude patterns in the conflict fields trust versus control and security versus freedom
- Subject overlaps among institutions/ actors and/or fields of conflict
- Uncovering of previously „unexplored subject fields“

Publication of the complete study „DIVSI Decision-Maker Study on Trust and Security on the Internet“

Module 1 encompassed more than 60 expert interviews with opinion leaders, decision-makers and disseminators.[1] The second step was the drafting of a concept for a quantitative representative survey. Hypotheses were generated and operationalised on the basis of the findings from Module 1. During the period between 10 September and 2 November 2012, 1,221 decision-makers from business, politics, civil service, civil society, media, academics and research were interviewed (corresponding to 1,220 weighted cases). The data were collected in collaboration with teleResearch GmbH in Mannheim. The interviews lasted an average of 25 minutes each.

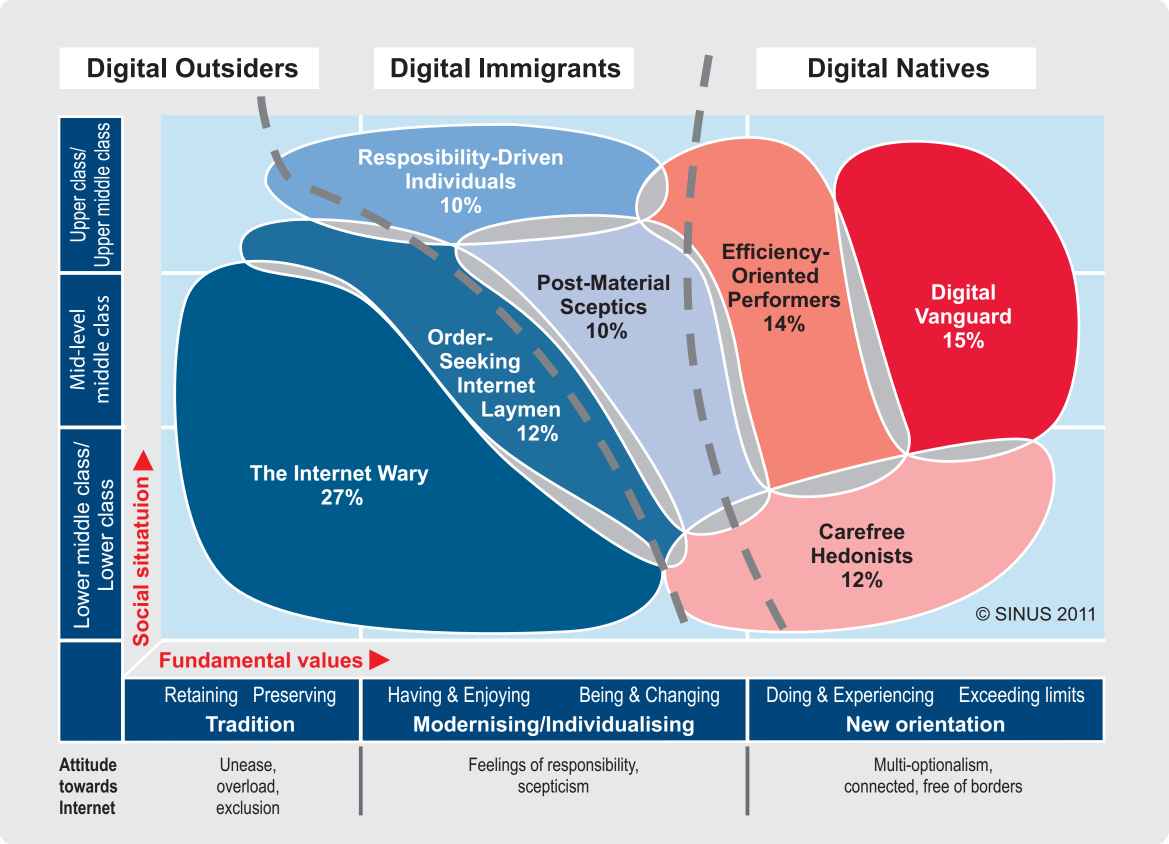
[1] This first part was published under the title „DIVSI Opinion Leader Survey – Who Shapes the Internet?“ in November 2012.

3. The Digital Milieus of Decision-Makers

As we strive to understand decision-makers with respect to their attitude profiles and approaches to the Internet, we discover that socio-demographic characteristics are inadequate as an explanation. We will not succeed in gaining comprehensive understanding of complex attitudes and behavioural patterns unless we also look at the milieus in which decision-makers operate.

A model illustrating digital milieus in society was created within the framework of the „DIVSI Milieu Study on Trust and Security on the Internet", an examination representative of the general population published at the beginning of 2012. It was based on the milieu model[2] of the SINUS-Institut. The chart below illustrates the seven Internet milieus of the general population.

Internet milieus in terms of trust and security on the Net differ from one another depending on social class and fundamental socio-cultural values



Digital Outsiders
Digital Immigrants
Digital Natives
Upper class/ Upper middle class
Mid-level middle class
Lower middle class/ Lower class
Social situatuion
Resposibility-Driven Individuals 10%
Post-Material Sceptics 10%
Efficiency-Oriented Performers 14%
Digital Vanguard 15%
Order-Seeking Internet Laymen 12%
The Internet Wary 27%
Carefree Hedonists 12%
© SINUS 2011
Fundamental values
Retaining Preserving
Tradition
Having & Enjoying
Being & Changing
Modernising/Individualising
Doing & Experiencing
Exceeding limits
New orientation
Attitude towards Internet
Unease, overload, exclusion
Feelings of responsibility, scepticism
Multi-optionalism, connected, free of borders

[2] The SINUS milieu model classifies people into groups according to their outlooks on life and life styles. So SINUS milieus® are target groups which actually exist. For more information go to www.sinus-institut.de/loesungen/sinus-milieus.html.

Analogous to the SINUS milieu model, the Internet milieus can also be presented in a two-dimensional matrix which depicts the positioning of the various groups within the social structure of society. The social situation (Lower class/Lower middle class – Mid-level middle class – Upper middle class/Upper class) is plotted along the vertical axis. The higher a group is positioned in the chart, the higher the levels of education, income and professional prestige. The fundamental values in a socio-cultural sense are shown along the horizontal dimension and become more modern as the position moves farther to the right. In reality, digital milieus cannot be precisely differentiated from one another. This is also represented in the model by the overlapping of the milieus.

The seven Internet milieus can be grouped into three segments:

- Digital Outsiders (39 per cent): They are either offline or are insecure when using the Internet. Assuming a population of 70 million people of the age 14 or older in Germany, the Internet is a digital barrier to a world from which 27 million people feel excluded.

- Digital Immigrants (20 per cent): While they regularly move around on the Internet, they are highly selective in their use. They did not grow up in the digital world and are highly sceptical towards many developments, especially when the subjects of security and data protection on the Internet are involved.

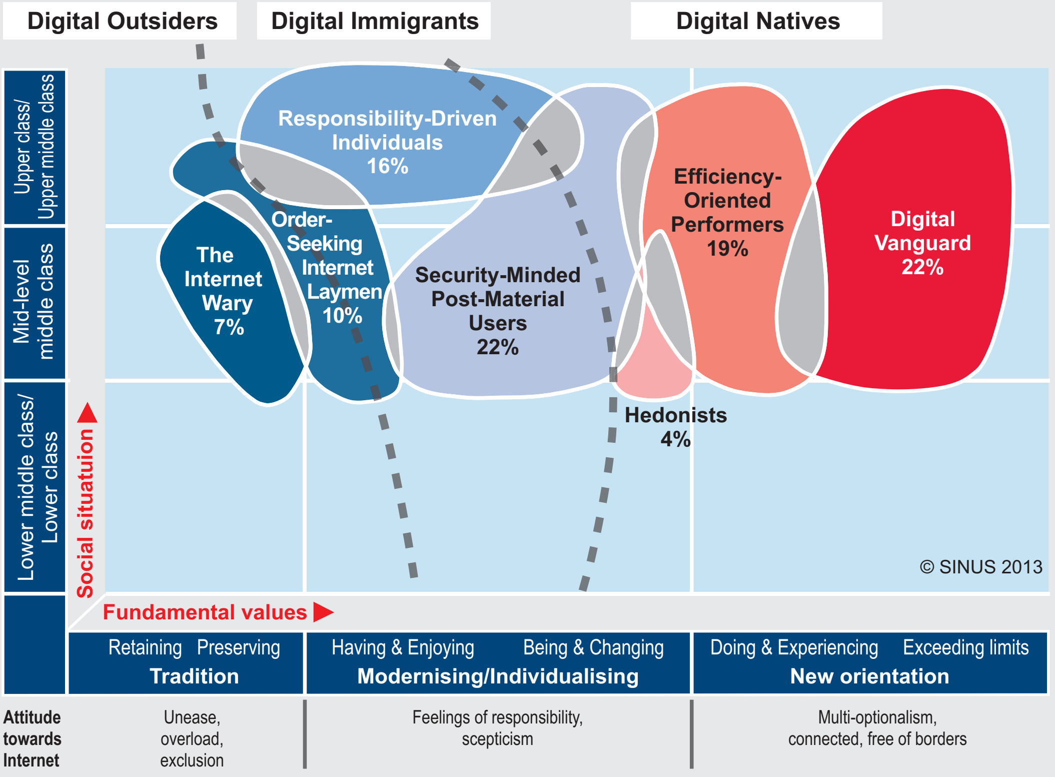
- Digital Natives (41 per cent): The digital world is a major element of life for the people in this group. They move around the Internet like a fish swims in water – their life motto is „I surf, therefore I am." Their attitude towards the Internet is highly positive, and they regard the progress of digitalisation primarily as a personal opportunity.

Based on the previous study of the general population (DIVSI Milieu Study), an indicator instrument for classifying the decision-makers in the various Internet milieus was developed. Decision-makers were distributed among the seven Internet milieus on the basis of their answer profiles, and the results are shown, just as in the general population study, in the form of a map.[3] While decision-makers are found in all seven Internet milieus, there are clear concentrations within the Internet milieu structure. The chart below illustrates the size and positioning of the Internet milieus in the German decision-maker landscape.

[3] Owing to the slight differences in attitude towards trust and security on the Internet, two milieus were renamed for the decision-makers: *Post-Material Sceptics* became *Security-Minded Post-Material Users* and *Carefree Hedonists* became *Hedonists*.

There are significantly different concentrations in the Internet milieu structure of the decision-makers compared to that of the general population

Representative for 2.69 million decision-makers in Germany
(= 3.8% of the general population of the age 14 or older)

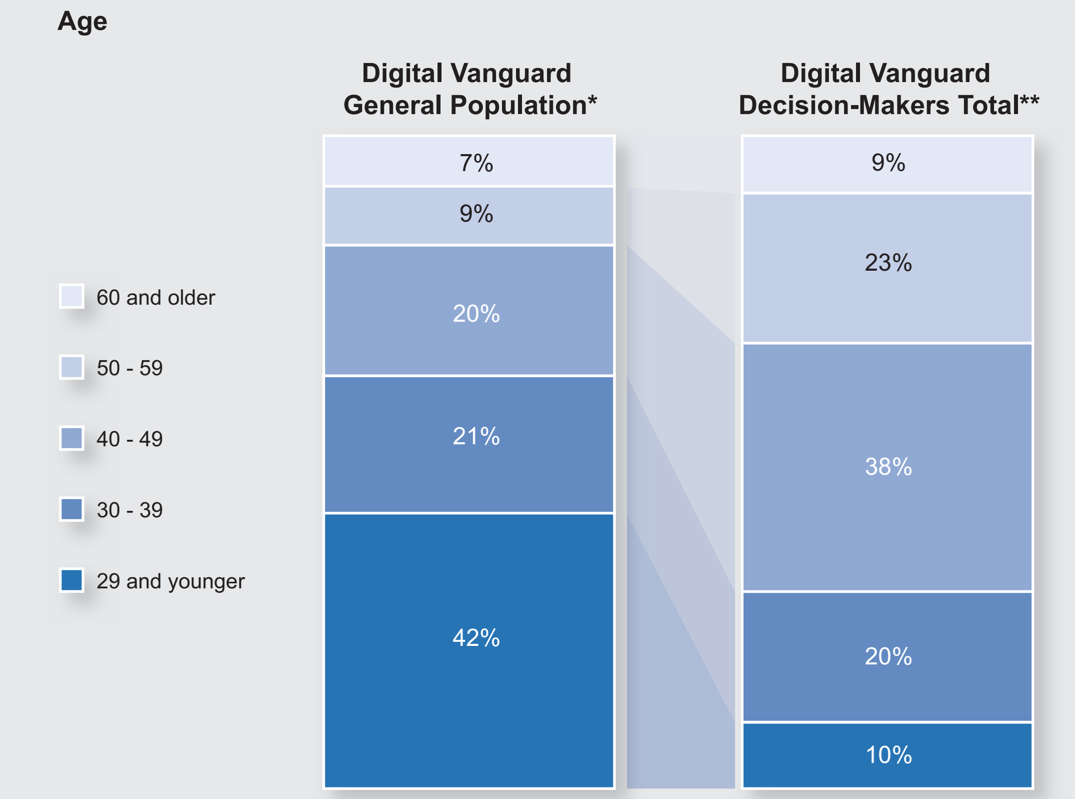


Sample: 1,220 cases, decision-makers

The milieu of the *Digital Vanguard* – the digital avant-garde with an individualistic fundamental attitude – at 22 per cent is represented most strongly among the decision-makers. This milieu has a share of barely 15 per cent among the general population. However, this difference is even more significant than is apparent at first glance because the *Digital Vanguard* in the general population is found primarily among young people: 42 per cent are below the age of 29. Yet hardly any people from this age group can be found among the decision-makers.

The fact that almost one out of three of the *Digital Vanguard* among the decision-makers comes from Generation 50+ is surprising and indicates that we need a broader understanding of the term „Digital Natives“. Digital Natives are no longer the „wild young ones“; the digital milieu has become established in the executive suites.

The Digital Vanguard age 50 or older represents a significantly greater percentage among decision-makers than in the general population

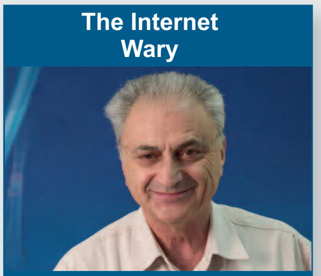


*DIVSI Milieu Study 2012, sample: 294 cases **DIVSI Decision-Maker Study 2013, sample: 273 cases

Brief profiles of the seven Internet milieus for decision-makers

Digital Outsiders

The Internet Wary



Overwhelmed Internet users, reserved attitude towards progress of digitalisation. Desire for security and control mechanisms.

Order-Seeking Internet Laymen

Defensive-careful Internet users from middle-class mainstream. Strive to keep pace with technological transformation.

Digital Immigrants

Responsibility-Driven Individuals

Educated establishment with a grasp of leadership. Responsibility-driven attitude towards digital progress.

Security-Minded Post-Material Users

Skilled, target-oriented Internet users with critical-reflective attitude towards data security and „blind" fascination with technology.

Digital Natives

Hedonists

Internet users without any fear of contact, enjoy experimenting. Virtually no concerns about security or awareness of risks.

Efficiency-Oriented Performers

Performance-driven Internet pros. Professionalisation as a guiding principle. Clear focus on efficiency and solutions regarding data security as well.

Digital Vanguard

Digital avant-garde with distinctly individualistic fundamental attitude. Strive for independence in thought and action.

3.1. Focus on Internet Milieus – Detailed View of the Decision-Maker Landscape

3.1.1. Digital Vanguard

The *Digital Vanguard* at 22 per cent, along with the *Security-Minded Post-Material Users* (also 22 per cent), makes up the largest Internet milieu within the decision-maker group. They are the digital avantgarde, who view individualism and independence as the starting point of their thinking and action.

The *Digital Vanguard* comprises individualists who like to express themselves creatively in their profession. They are flexible and able to adapt when required to adjust to new situations and corporate structures, but they have a mind of their own, want to realise ideas, do some things differently and think outside the box. Their career goal is not to „get to the top“, but above all to develop themselves personally and to seek new challenges constantly. For the most part, they have been in a management position for only a few years. The *Digital Vanguard* is geographically and mentally mobile, thinks in global dimensions and is demonstratively liberal and cosmopolitan. These traits lead them to view the Internet as an opportunity to discover new lands for themselves independently of time and space, to maintain extensive networks and to market themselves. The Internet is their omnipresent option pool which can also be the source of new business models and ideas – whether with respect to products and services or to customer and partner networks.

3.1.2. Efficiency-Oriented Performers

Efficiency-Oriented Performers make up 19 per cent of the group of decision-makers. These are career-oriented Internet pros with a pronounced focus on convenience and benefits.

Efficiency-Oriented Performers regard themselves as the modern pillars of society; career and success are absolutely essential for a fulfilled life in their eyes. They are goal-oriented, have tremendous self-confidence and a can-do mentality. Smart, dynamic and visionary, they carry out their professional plans with a fundamental attitude which is definitively competitive because no one makes it to the top without challenges. They do not want to become tied down to conventional patterns in life and are looking for something special. As they see it, their key skills are multi-optionalism, networking and multitasking. The Internet is an indispensable component in their life style and an infrastructure they take for granted; it enables them to access the full bandwidth of digital information and communications opportunities anytime, anywhere. Modern technology is for them both an aesthetic must-have and a working tool to increase efficiency.

3.1.3. Security-Minded Post-Material Users

The attitude profile of the *Security-Minded Post-Material Users* is strongly represented among decision-makers; 22 per cent belong to this group, a contrast to the general population where the group has less than half the share (ten per cent). They are selective Internet users with a critical, but nevertheless open fundamental attitude towards the Internet.

Security-Minded Post-Material Users are characterised by global thinking, a general openness towards other life styles and attitudes and a range of interests covering a wide span of subjects. They seek intellectual stimulation and intensive sharing of ideas and thoughts with like-minded people – including their colleagues. They have integrated digital technologies as far as possible into their everyday lives and utilise them masterfully, although very deliberately and selectively. Generally speaking, they expect a high level of quality in their consumption of material items and have an aversion to superficiality.

There is an ambivalent attitude towards the Internet among the members of this group. On the one hand, they profit from the simplification of opportunities for information and communication; on the other hand, they criticise the rapidity of digitalisation and the growing concentration of power in the hands of the few on the Internet. In their view, online activities are conducted with too little thought for consequences – they suspect that many of these activities are driven by the fear of being left behind.

3.1.4. Responsibility-Driven Individuals

Sixteen per cent of the decision-makers belong to the Internet milieu known as *Responsibility-driven Individuals*. Ten per cent of the general public as a whole belongs to this milieu.

Responsibility-Driven Individuals are the educated establishment with a grasp of leadership. They frequently hold management positions in larger companies or work successfully in freelance professions as doctors, lawyers etc. They can often look back over a longer career and feel at home in their own position, including their place in society.

Technology for them is a means to an end: they take care of things online when doing so offers concrete added value. While their fundamental attitude towards digital progress is open, it remains one of deliberation and awareness. In their view, digitalisation is not an end in itself; costs must be weighed against benefits according to the task at hand. They move selectively around the Internet, where they are guided by practicality and the calculation of benefits. When there are good arguments in favour of doing so, they are prepared to take certain actions online as well.

3.1.5. Order-Seeking Internet Laymen

One out of ten decision-makers is classified in the Internet milieu of the *Order-Seeking Internet Laymen*. This group maintains a great critical distance to the Internet and remains more defensive when online – especially as long as they cannot be certain that many applications do not bear a threat of possible harm.

The *Order-Seeking Internet Laymen* among the decision-makers are committed to middle-class values in their fundamental attitude. Many of them work in small and midsize businesses in the communities where they have also built their houses and raised their children. They strive for harmony and a sense of security, and they want to be assured of good order and reliability on the Internet as well.

3.1.6. “Fringe Groups” in the Decision-Maker Landscape

Besides the five Internet milieus described above, there are two more digital milieus – although significantly smaller ones – in the decision-maker landscape: the *Internet Wary* and the *Hedonists*. These two groups are described in more detail below.

3.1.6.1. The Internet Wary

Representatives of the group of the *Internet Wary* make up a mere seven per cent of the decision-maker landscape and are rarely to be found here. In contrast, 27 per cent of the general population can be classified in this Internet milieu, which can be characterised above all by a heightened perception of the risks on the Internet and the related demands for protection and control.

The *Internet Wary* among the decision-makers belong overwhelmingly to the traditional segment of society. These decision-makers are frequently managing directors in small companies with fewer than 20 people on the staff. They belong to a generation in which it is not unusual to be a successful entrepreneur or reach a top management position even without a university degree. These decision-makers are frequently over 60 and are in part preparing for the next chapter of their lives when their professional careers have come to an end. They seldom seek contact with the Internet during their everyday lives, preferring the direct communication between one person and another. The rapid pace of digitalisation and modernisation not only makes them feel insecure, it alienates them – many of the supposed „necessities“ appear superfluous to them, and in view of the flood of information and communications technologies, they sometimes feel adrift in a working world which is no longer theirs.

3.1.6.2. Hedonists

The attitude type known as *Hedonists* are very rarely found among decision-makers. Only four per cent can be classified in this milieu.

The *Hedonists* among the decision-makers simply want to try out many different things before they form an opinion. The Internet offers to them the opportunity to strike out on a journey of discovery without being too concerned about what might happen. They have virtually no interest in the subjects of data security and data protection. They are more likely to take the fatalistic attitude that data misuse cannot be prevented anyway.

These decision-makers appreciate the convenience the Net offers them. They do not want to waste time and effort taking care of unnecessary problems. In their online behaviour, the Hedonists among the decision-makers combine a low level of Internet expertise with an even lower level of concern about security.

4. How Do Decision-Makers Think?

Decision-makers are in agreement with respect to some key statements about trust and security on the Internet – despite the differences in the fundamental attitudes towards the digital world described on the preceding pages. This common view of the development of digitalisation, the significance of the subject of security, the distribution of power on the Net, the sources of risk and the responsibility of the general public are the topics in this chapter.

There is no longer such a thing as an offline life

- **The distinction between online and offline will soon become obsolete.** The majority of the decision-makers (64 per cent) believe that it will no longer be possible to be completely offline in the future. Technologies will become simplified and specialised to such an extent that the utilisation of various devices and their functions will require less and less digital basic knowledge, general understanding of technology or fine motor skills.

- **The phenomenon of people genuinely being offline will be a phase that „outgrows“ itself.** Before long, people will no longer „get on the Internet“ because more and more everyday processes will be steered online anyway (e.g. the navigation technology in the car, the stocking of supermarket shelves, monitoring in hospitals). Digital trenches will silt up completely on their own because everyone will be born into an online world – in other words, they will be Digital Natives without even being aware of it.

- **From the perspective of decision-makers, we are in the middle of a fundamental transformation in society.** What is at stake here has long since gone beyond technological transformations which affect merely the efficiency of work processes; completely new and different skills demanded for the exercise of a profession have come into being (e.g. the fast meshing of knowledge units, the flexible and repeated familiarisation with new fields, the design or evaluation of a personal or institutional Internet presence and flexible action in global contexts). The need for „classic“ skills is declining, or they have changed almost beyond recognition (e.g. filing, appointment coordination on the phone). Moreover, it is becoming more and more difficult to keep work and professional life apart in many areas because digital applications make it possible to carry out projects even when away from the desk. While this gives rise to new opportunities (home office, „workation“), new challenges are just as common (setting limits in favour of personal life, mistakes caused by information overload).

Security on the Internet is a burning issue – but an illusion

- **Eight out of ten decision-makers view data security as a key thematic complex for themselves personally as well as for society.** Broad subjects such as economic development, education, unemployment, energy supply and social justice are still given a little more weight; but online security is rated as more important than climate change or immigration.

- **Decision-makers are significantly more sensitive to the subject of data security on the Internet than the populace in Germany as a whole.** In comparison to the general public, decision-makers rate the significance of the thematic complex „data security on the Internet“ substantially higher – both for society in general (78 per cent versus 66 per cent) and in the personal sphere (80 per cent versus 64 per cent). The greater importance attached to data security by decision-makers can be explained by their professional environment: decision-makers evaluate the subject from the perspective of potential damage or loss for their company or organisation.

- **The Net is hard to control.** Comprehensive data security on the Internet is a mirage – 68 per cent of the decision-makers are convinced of this. This covers equally the possible loss of data, the uncontrolled distribution of data, the inaccessibility of data and the non-existent „right to forget“ on the Internet. This group is fully aware that (technical) systems can never guarantee more than partial security and that there will always be a residual risk. Logically enough, most decision-makers are of the opinion that we will have to become accustomed to a more liberal handling of data on the Internet (60 per cent).

- **A superordinate codex of values for the Net appears unrealistically utopian.** Technical weaknesses are not the only factors limiting the degree to which data security can be achieved. Considering that the Internet is a global phenomenon, decision-makers believe it will become increasingly difficult to create binding legal provisions of a fundamental nature. 49 per cent are convinced that any one country will hardly be in a position to establish regulations with which „the Internet“ will feel obligated to comply.

Private business runs the Internet

- **The Internet is dominated first and foremost by private business.** The large, globally active Internet service providers such as Google, Apple, Facebook, eBay and Amazon in particular are viewed as the primary actors, who determine to a major degree what basic applications become available.

- **The concentration of the power of global players is regarded as a risk on the Net.** Many decision-makers express their concern that they have become dependent on single companies because there are virtually no alternatives on the Internet for researching, purchasing or networking. As specific services have become more widespread and more tightly intermeshed with one another, monopolies have risen which dictate to the market – and to their own working environment as well.

- **There is almost no perception of the government as a dominant actor on the Internet.** Significant influence on the Internet is attributed to the world of politics by only 15 per cent and to public administration by only eleven per cent.

The sources of risk on the Net are hackers, global Internet service providers and thoughtless users

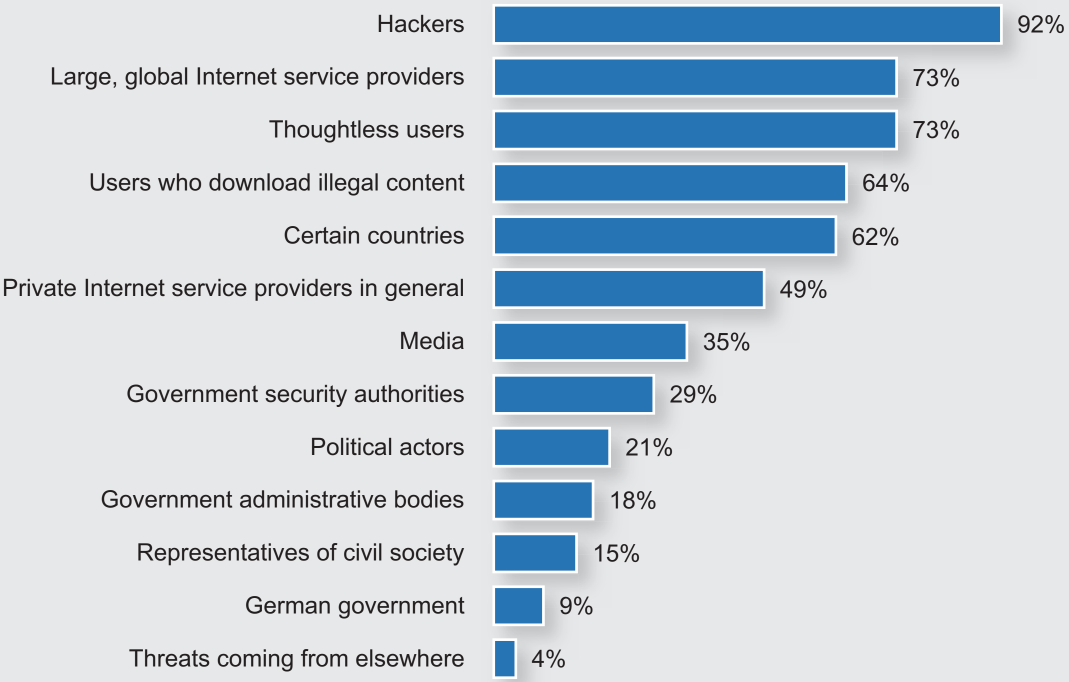
- **Hacker attacks are the greatest risk on the Internet.** Guarantees of protection from hacker attacks are considered completely worthless. Strategies which offer (at most temporary) protection must be regularly reviewed and constantly updated.

- **Large, global Internet service providers have significant potential for risks.** This opinion is shared by 73 per cent of the decision-makers. However, they see the same level of risk from the actions of thoughtless users, who unintentionally jeopardise data security and data protection or who fall into traps because they have not (yet) learned to recognise fraudulent offers.

- **The government poses little threat to the Internet.** Only nine per cent of the surveyed decision-makers discern a high potential for risk in the German government; 18 per cent see such a risk in the government administrative bodies and 21 per cent see the danger coming from political actors. The actions of government security authorities on the Internet are viewed as a risk by 29 per cent.

Decision-makers regard hacker attacks to be the greatest risk on the Internet

„In your opinion, what actors on the Internet pose the greatest threats?“



Sample: 1,220 cases, decision-makers

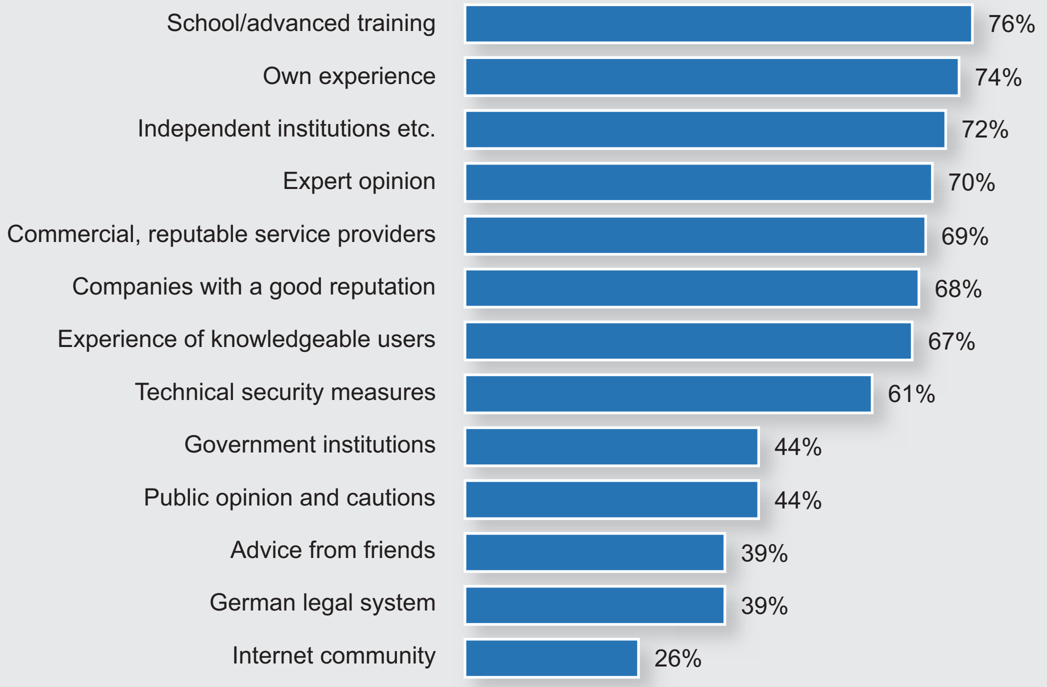
Users bear the primary responsibility, but they lack the necessary knowledge

- **Users clearly bear responsibility for the protection of data.** Security on the Net can only be achieved – if at all – through the media literacy of the populace, according to 69 per cent of the decision-makers. Assuming responsibility for one's own actions is the overriding imperative of the day (73 per cent), which should be heeded by users on the Internet – whether they are aware of this or not.

- **Users bear the greatest responsibility, but too much is being demanded of them.** In the comparison of the various Internet actors, 82 per cent of the decision-makers place responsibility above all on the general populace, but only 27 per cent have any trust in the competence of such users. Consequently, they urge users to depend above all on education and their own experience because no one can assume responsibility in their stead. Decision-makers consider advice from independent institutions and experts to be relevant as well; but people should depend less on government institutions, the German legal system and the Internet community, as shown in the chart below.

From the decision-makers' viewpoint, government institutions and the German legal system tend to be less important for security on the Internet

„Who or what do you believe is most likely to offer dependable support on the Internet for the secure use of the Internet?"



Sample: 1,220 cases, decision-makers

5. What do Decision-Makers „Fight“ About?

Decision-makers in Germany are in agreement on many points: data security and data protection are important issues for which no adequate solutions acceptable to all have been found or which constantly give rise to new challenges which must be mastered. This only makes the need for action all the more urgent. But what must be done – and, above all, who will do what?

The following section will examine the key questions related to trust and security on the Internet from the perspective of the various groups of decision-makers.

Who has the greatest influence on the Net? Who poses the greatest threats?

- **The risk from thoughtless users.** Academics and researchers are joined by civil society in viewing users as the number one risk factor. Representatives from civil society and from academics and research view thoughtless users as a greater threat than professional hackers. In their viewpoint, shopping and socialising in the online world without a moment of concern or thought causes enormous harm on the Internet – usually to the users themselves. Clueless users are a threat to themselves. These two decision-maker groups see a tremendous inequality of opportunity on the Net: a few large players do and know a lot – and a lot of „small players“ know almost nothing.

- **The media criticise the users.** Media representatives also focus overproportionately sharply on users – especially those users downloading illegal content. Media representatives certainly see themselves as victims who suffer harm from the actions of users. This specific viewpoint means that they are less convinced than other actors that users are unable to grasp what is happening on the Net. They suspect that users are deliberately utilising online services subject to charge without paying for them. They criticise the gradual spread of a mindset that expects everything to be free on the Net and emphasise that high-quality services come with a price.

- **Differentiation in the classification of companies as security threats.** Decision-makers from politics, civil service, civil society, media, academics and research are in agreement that companies on the Internet represent a greater threat to security than perceived by the business representatives themselves. Decision-makers from politics and civil service regard the private Internet service providers in general to be a group which threatens security; academics, researchers, media, and civil society focus here above all on the large global corporations. 80 per cent of the decision-makers from academics and research view these corporations as a threat and also express the opinion (more frequently than the average) that the growing market concentration is a key challenge on the Internet (50 per cent versus 36 per cent). The picture business representatives have of themselves deviates sharply from these assessments: only 46 per cent consider private Internet service providers to be a risk on the Net.

- **Academics and researchers as well as media take a critical view of the role of political actors and the government.** 35 per cent of academics and researchers (in contrast to 21 per cent as an average among decision-makers) regard political actors as a group, which is a source of risk. The media fear above all the threat of overregulation in this respect. But academics and researchers also see a threat to security in this context from the lack of opportunities for the political establishment to exercise influence; these decision-makers express their fears that political instruments are unable to keep up with the pace of developments on the Net with the consequence that government institutions are unable to ensure security.

Who should assume responsibility? And how?

- **Responsibility is the „buck“ everyone wants to pass when the question of security on the Internet comes up.** Nobody wants to keep it and everyone passes it on to the next in line. Some hold on to it for a longer period, but others never accept it at all.

- **Decision-makers in the business sector are significantly more reserved in comparison with representatives of all of the other decision-maker groups when it comes to assigning responsibility for security on the Internet.** Their viewpoint is that the capability of specific actors to steer the Internet is restricted and is not a „job“ which anyone will be able to conclude successfully. It is only logical that 74 per cent of the decision-makers from business are of the opinion that every individual is him-/herself responsible for data protection; this opinion is shared by 63 per cent from politics, but by only 52 per cent from academics and research.

- **Business representatives frequently assume that users are naive.** Overall they are less inclined to believe that too much is expected of users – many see demands for protection as an excuse.

- **Politicians are more firmly convinced that users are unable to grasp much of what happens on the Internet and are in need of protection.** This is the attitude of 67 per cent of the politicians in comparison with 54 per cent among decision-makers in business. Political decision-makers view as the greatest necessity the determination of the threshold beyond which users must be protected; like the other groups, they expect the general population to assume a high level of responsibility for their actions.

How should responsibility be assumed?

- **Decision-makers see a number of different ways in which responsibility for security on the Internet can be successfully assumed:** by checking online applications and exercising caution during their use (users), by providing liability (companies/providers, users) or by establishing regulatory measures (politics). Besides the „mature“ use of the Internet by educated citizens, the decision-makers in the qualitative preliminary study addressed above all the issue of regulation because there are obviously substantial differences among the actors in this respect. Business and politics in particular displayed conflicting, in some cases diametrically opposed viewpoints. For example, 40 per cent of the business representatives are convinced that the Internet is a free medium which should not be regimented under any circumstances; this opinion is shared by only 23 per cent of the decision-makers from politics.

- **Decision-makers from business clearly advocate self-regulation ahead of government regulation (60 per cent).** Half of the politicians (50 per cent) agree with this standpoint – evidence that the answer to this question is not simply a decision for the one or the other option. Politicians frequently regard government regulation as the „ultima ratio“. They do not per se consider self-regulation to be inadequate, but they tend to be less euphoric against the backdrop of the empirical reality of the concept: self-regulation sounds great, but it does not work.

- **In comparison with decision-makers from politics, business representatives are less concerned about the need for an active government role to ensure security (70 per cent versus 84 per cent).** The qualitative study revealed that companies think primarily about the security of their own business models (e.g. security of online financial transactions, copyright/trademark violations, other instances of fraud etc.). Nevertheless, the majority of them assume that the government, in view of an Internet spanning the globe, will be unable to create any binding legal frameworks (53 per cent). Politicians are slightly less pessimistic in this case: „only“ 43 per cent believe that this will prove impossible.

- **Academics and researchers as well as civil society call for a legal framework from the government more insistently than the average.** Despite all of the emphasis given to individual media literacy, representatives from academics and research (88 per cent versus 79 per cent of all decision-makers), for example, expect the government to assume major responsibility. Their view is that users can be expected to assume responsibility only if there is a constitutional framework in place.

- **Personal liability of users is differentiated according to circumstances.** The overwhelming majority of all decision-makers – even those from business – say that anyone causing damage or loss should also be liable for the consequences. However, decision-makers disagree as to whether the users should also be personally liable if their computers are not adequately protected. While 46 per cent of business representatives express the opinion that users should be liable, other actors are significantly more reluctant to see things this way (politics 36 per cent, civil society 32 per cent, academics and researchers 25 per cent).

Who and what can you trust on the Net?

- **Decision-makers from civil society see strikingly fewer threats on the Internet than all other groups of decision-makers.** In particular, they dismiss total transparency, mass e-mails or restricted access to one’s own data as posing virtually no risks on the Net.

- **Media, along with academics and research, emphasise especially the social and cultural risks.** Academics and researchers observe above all a rising flood of information and market concentration while the media – as do the political decision-makers – count increasing dependency on online infrastructures and a problematic change in political culture among the threats.

- **Decision-makers recommend differing strategies for more security on the Internet:**

  - Trust in institutions tends to be more pronounced among **political decision-makers and in civil service** – and, in part, in civil society – than among other decision-makers. The latter put more trust in independent institutions (civil society) and government agencies and in the German legal system. Politicians, more than other decision-makers, reject a trial-and-error principle as the basis for action on the Internet – experience and media competence are very important, but there is also a need for general conditions.

  - A look at the various Internet segments within the group of **business representatives** is of interest: the *Digital Vanguard* in particular has significantly less confidence in independent institutions, preferring to rely on education and own experience. The lack of trust in the German legal system is especially great (30 per cent versus 39 per cent).

  - **Decision-makers from the media and from academics and research** rely above all on knowledge based on experience supported by information from independent institutions, experts (especially in the view of academics and researchers), reputable commercial service providers and knowledgeable users or the advice of friends. This means that when a person’s own experience does not suffice, one should trust those who know more about the subject. Trust here means above all trust in people. Technical security measures or „the government“ are less significant. Representatives from academics and research and from the media are the actors pursuing a holistic, systematic concept of trust to which all Net actors (including users) make contributions and in turn profit from others.

6. Conclusion

1. Responsibility and trust do not go hand in hand on the Internet

The decision-makers agree: anyone causing a risk must also bear responsibility for the consequences – but evidently not to the same degree. Although large, global Internet service providers and users are regarded as more or less equally great potential sources of risk (surpassed only by hackers), users are expected to assume significantly greater responsibility. This seeming disparity can be explained by two fundamental assessments:

- It is virtually impossible to control the Internet. Security on the Internet remains an illusion and cannot be created either technically or legally, even if this were desirable. For one, software never offers more than a partial solution. For another, the possibilities for exercising any legal influence are limited because of the global networking of systems and services. Finally, the dominance of some few companies, which has become established, in the meantime leads decision-makers to believe that demanding responsibility from these actors is utopian or irrelevant.

- The Internet is an infrastructure which in the meantime is so widespread that the areas of our everyday lives in which it is not present are becoming few and far between. Despite this growing online omnipresence, decision-makers do not regard an infrastructure itself as dangerous. Threats do not arise until these structures are used improperly. The application of the costs-by-cause principle means that the user bears the onus of the obligation, not the provider of the service.

Decision-makers recommend education and experience as the tools for secure navigation in the online world to users. At the same time, however, they declare that users do not know what they are doing and consequently have little faith in their ability to protect themselves reasonably.

If, therefore, it is not possible to depend on the competence of users at this time, the question as to what other actors can be expected to assume a greater obligation remains. The primary dilemma is the fact that the decision-makers trust the actors who are supposed to assume responsibility even less. The decision-makers in whom they are more likely to place their trust (e .g. public institutions) are seen to have substantially less responsibility.

A majority of the decision-makers believe that a general legal framework on the Internet is absolutely essential – for one thing, to guarantee freedom on the Internet. While the users are considered to bear the (primary) responsibility, decision-makers still see the need for a general framework within which users can move freely and be assured of having adequate security (e.g. from fraud).

2. Digitalisation is entering the consolidation phase

Digitalisation is regarded as one of the so-called mega-trends, right alongside globalisation and demographic transformation. „Mega“ as used in this context describes not only the duration of this trend, but the broad and diverse range of its effects on the most widely varied areas of our lives as well. It is not surprising that the breathtaking evolvement of new technologies has a major impact on our ways of thinking, living and working. For many years, the focus was on the technological discussions or a simple comparison of opportunities and threats: the Internet was either revolution or danger.

However, recent years in particular have demonstrated that digitalisation has launched a fundamental transformation which has long since passed the scope of straightforward technological changes. Short-lived hype about specific technologies or devices which years ago interested only a small part of society has turned into a dense web of fundamental digital behavioural patterns and essential working technologies, becoming a form of background noise to the reality of our work lives.

Digitalisation has substantial cultural implications because it shapes our everyday lives in manifold ways. The concepts of mobility and communication above all have changed extensively and new opportunities have been created which were still unimaginable only a few years ago. Just how people move around the Net, simultaneously creating their own digital value codex, has long since become an integral component of our life style – no less than hobby, profession or favourite music.

3. The Digital Vanguard: the decision-makers of the future?

22 per cent of the decision-makers are classified in the Internet milieu of the *Digital Vanguard*, who consequently represent the largest of the digital milieus in the decision-maker landscape. Moreover, the Internet milieu of the *Digital Vanguard* is the fastest-growing one. It does not require a great leap of faith to assume that the influence of this group within the decision-maker landscape will increase.

The members of the *Digital Vanguard* do not think twice about doing everything on the Internet, and they depend on their personal digital skills to fend off possible threats. Especially the business representatives from this Internet milieu are interested in significantly less „protection“ or influence from institutions and politics. They not only regard the concept of an offline life as obsolete; the one-to-one transfer of principles from the offline to the online world appears just as senseless to them. In their view, many things function completely differently on the Internet which is why new structural systems are arising and continuously evolving. This constant state of flux means that no single actor „can carve [the systems] in stone“.

It is also obvious that responsibility and trust must be redefined and evaluated. Trust is a substantially less relevant category for the *Digital Vanguard* when making decisions for or against an online action than it is for other groups. Efficiency and practicality are more important to this group than the reliability of the source or of the provider.

This is where the evident dilemma stands out especially starkly: if the group of digitally accomplished decision-makers (which will continue to grow in the future) questions trust and, in the case of decision-makers from business, even responsibility as criteria and individualises these characteristics as forms of self-obligation and self-assurance – not only for themselves, but as recommendations to users – we face the question of how Internet security solutions which are effective on people's actions and sustainable can be found.

A look at the entire decision-maker landscape shows that today almost all of them have arrived in the Internet and virtually every single one is online regularly. Almost every other one is a Digital Native; digital everyday life has become established in most of the executive suites. As the Internet has moved into the working world, it has brought with it new technologies, but it has also transformed the fundamental processes of labour organisation and how people see themselves in their professional roles. New requirements for process re-engineering and networking demand management skills in organisations and enterprises, which focus on different areas or are more extensive than those of the past. More and more often, the decisive point is not only to know what is to be done, but also who it is to be done with, i. e. the continuous broadening of networks is becoming more and more significant as a (knowledge) resource – even in professions and generations in which address book changes are still made at greater time intervals.

A key issue of the future will be the development of the relationship of the *Digital Vanguard*, who will represent an increasingly larger share of the group of decision-makers because of demographic developments, to established institutions. This group has an especially sharp perception of the amazing sturdiness and power of the Internet resulting from its features of network orientation and essentially consensual governance and regards these features (along with others) as the harbingers of management methods which are clearly distinct from the 20th century models based on institutional structures. This is also in no small degree the explanation for the ebbing trust of this group in conventional institutions.

The need to determine what role institutions, which have „traditionally" defined general guidelines for infrastructures and ensured compliance with them (e.g. a national system of laws), should and can play on the Internet is becoming urgent, particularly because the Internet has now become an infrastructure for everyone involved in all fields of action and for the populace.

The answer to the question of what balance will be reached between institutions and individuals will be decisive for determining how much room Internet users will retain with respect to the tensions between freedom and security, between trust and control.