Next Generation Internet
Work Programme Preparation 2018-2020
Consultation Report

Rapporteur: Pieter Ballon, iMinds-SMIT, Vrije Universiteit Brussel

Executive Summary

The Next Generation Internet refers to a set of novel architectures and approaches that should enable the evolution of the Internet into a system that is able to **sustain the current explosion** in streaming and mobile traffic, **cope with new demands** caused by the massive proliferation of real-time data generation and exchange throughout the network, **offer major improvements** in terms of reliability, security and trust, and **unleash a wave of opportunities** for service and system innovation and value creation. All of this should happen in a manner that *alleviates the risks of surveillance*, *favours openness and interoperability* and *increases user empowerment and control*.

Future networks require capabilities so as to incorporate mass-market Internet of Things devices as well as large-scale cyberphysical systems including mobility, safety and energy systems of cities, autonomous cars and ubiquitous drones providing massive "data torrents" from mobile, high-bandwidth sensors and actuators.

One major consequence of this is the need for **highly distributed architectures** and approaches. An explosion of massive short-length (often wireless) data exchanges among a multitude of distributed nodes at local level is expected. To support such mass-scale volatile communication patterns, data should be stored, processed and consumed at local level. The *mobile edge cloud* will be supported by micro data centers, providing relief to core networks and core data centres, improving latency bound applications performance and enhancing the user experience.

A second, related evolution is the **virtualization and softwarization** of the network. This refers to the separation between a simple and open hardware data plane and a dissociated programmable control plane. This virtualization will include network components, end-user devices, and eventually sensors. Virtualization enables to transparently use resources, including computing, storage, and networking. The move towards software-defined networking and *cloudnets* thus leads to a single abstraction that provides an application with connectivity, storage, and processing capabilities irrespective of the underlying physical infrastructure.

A third major aspect is the need to achieve **resilience and trust** within a so-called unreliable and trustless Internet context. *Blockchain technologies* offer a distributed architecture that is resilient and able to achieve trust-by-design, with potentially disruptive consequences. Programmable and decentralised blockchain databases open the way for automated and distributed consensus and exchange without the need for a so-called trusted third party. However, this is only part of a more encompassing social, technical, institutional and economic transformation that should lead to more openness, transparency, interoperability and ubiquity of information and services.

The final consequence is the need for **cybersocial and cyberphysical system redesign**. Decentralization, softwarization and distributed trust are expected to

enable a multitude of new services. Highly dynamic platforms will be able to connect and operate cloud and network components as well as end-user and IoT devices as logical resources independent of underlying physical constraints. Services will be powerful, automated, and ubiquitous. They can be related to an end-user, to a machine or to industrial systems and will rely on real-time personalisation, data and resource locality independence, and industry-grade performance. This transformation of the cybersocial and the cyberphysical is impossible without the *activation of experimentation ecosystems* of large companies, SMEs, startups and venture capital funds; regions and cities; knowledge institutions and individuals.

Meeting these challenges will require fundamental research dealing with the formal foundations for reasoning about and programming next generation networks, services and applications, understanding and controlling their dynamics, as well as applied, interdisciplinary work that blends together system prototyping, deployment, testbed operation with use cases and addressing the key contextual roadblocks to service innovation. In particular, a number of areas stand out where European action is required in order to strengthen its competitive position.

The first area is that of **real-time pervasive data analytics**. It appears that a major opportunity for European stakeholders refers to leveraging the power of big data on edge devices. Distributed data analytics are expected to be highly important for the competitiveness of any service or system that is part of, or using, the Next Generation Internet. Research should focus on solving critical issues at hardware and software levels related to low latency data networking, data processing pipelines, ubiquitous access to data, machine learning and decision-making, real-time customisation and personalisation, long-term scalable backups and storage, etc.

The second area is that of **software-defined networking**. The European opportunity is firstly related to the evolution towards software-defined infrastructure and software-defined exchanges. This implies R&D on the integration of software into the network and on the definition and evolution of the Next Generation Internet control plane. Secondly, there is an even broader opportunity related to the performance and security of the Internet. European industry will benefit greatly if R&D in this field leads to an 'industrial-grade Internet' where SLAs can be given related to very complex operational technologies connected to the Internet, as well as from more secure web architectures and standards.

The third area is that of **trust-by-design**. Europe should actively explore the principles and application of trust-by-design related to transparency and accountability, but also to distributed data governance and distributed innovation and collaboration. Application domains include new business ecosystems, the sharing economy, identity and profile management, e-democracy, as well as all sorts of autonomous and critical systems and infrastructures. In addition, research needs to derive ethical frameworks, safeguards and regulation pertaining to the design and management of digital

networks, services, identities and hybrid digital-physical systems (cars, drones, digital implants,…).

Finally, in order to reap the benefits from the technologies mentioned above, it appears paramount that Europe actively creates the right context for these innovations, i.e. by stimulating the set-up and development of **experimentation ecosystems related to the Next Generation Internet.** Next Generation Internet research and development should, in an early stage, consider and include service creation, user experience and user behaviour, business model innovation, incentives to invest, city and regional involvement, open standards and open interfaces, the activation of SMEs, tech startups and creative industries, and so on. For this, a targeted approach is needed, incorporating mechanisms such as co-creation, city-wide living labs and innovative procurement targeted a.o. at starters and SMEs in application domains that are particularly relevant for Europe, including digital fabrication and Industry 4.0, smart cities, mobility and logistics, and hybrid online-offline business and retail.

1. Introduction

As part of drafting the new Work Programme 2018-20, the Experimental Platforms and Net Innovation units are defining their vision for the Next Generation Internet area, identifying key technological challenges and research priorities, and establishing a research agenda for the coming years.

A group of eleven experts was asked to provide input. These experts included Raphael Beaumond, Marco Canini, Primavera De Filippi, Gianlucca Dettori, Christophe Diot, Anja Feldmann, Mikael Grannas, Nectarios Koziris, Michiel Leenaars, Michel Riguidel, and Steven Wilmott. The main objectives of the expert group were to define concepts and activities for Next Generation Internet, and to express ideas that could serve as inputs for Work Programme 2018-20. For this, the expert group addressed a wide range of aspects including technological issues, research challenges, and societal developments.

Each expert submitted a position paper exposing his/her views on Next Generation Internet and the activities to be carried out until 2025. All experts were then invited to a one-day workshop on 16 March 2016 in Brussels to discuss the position papers.

In addition, an open consultation round was organised online, inviting respondents to address 4 main questions:

- What is your assessment of the current status of the Internet and its impact from a European perspective? What are the major trends?
- How do you think the internet will look like in 2025 and beyond?
- What will be the essential functional building blocks of the Internet then?
- Could you indicate where we should focus our activity research in the next 5-10 years to achieve? Are there new fields of research to create/develop?

In total, 317 responses were received to these questions. Respondents also had the opportunity to upload additional documents to further support their arguments. 28 additional documents were sent in this way.

This report contains a synthesis of the 2-page expert inputs, the expert Workshop discussion and the open consultation round.

2. Overall analysis of the consultation

Both the written inputs by the experts and by the broader online Net Innovation and Experimental Platform communities, as well as the oral interventions during the Workshop proved to be rather heterogeneous. The input was therefore quite rich, and impossible to fully do justice to in a summary report.

A number of experts started from a so-called utopian vision of the Next Generation Internet, while others focussed on the problems and 'broken' aspects

of the current Internet; some experts had a mainly technological and/or infrastructure-related outlook, others took on an explicitly business, society and services viewpoint; some inputs focussed on specific research topics, but there were also experts that highlighted approaches, contexts, and regulation; some referred to currently much-discussed trends, some came up with completely new concepts. Still, there were a number of common themes that emerged, a.o.

- Virtualization and move to software-defined networking (SDN) and programmable control planes (Leenaars, Canini, Koziris, Feldmann,…)
- Decentralisation: clouds, edge clouds, micro data centers, cloudnets (Koziris, Diot,…)
- New approaches to trust and security, including blockchain approach, etc. (Leenaars, Koziris, De Filippi, Feldmann,…)
- Over the top-aspects: data and platforms, data flows and data processing planes, IoT Operating Systems, standardisation moving up the stack (Diot, Feldmann,…)
- Ecosystems: Living labs, user-tech interaction and startups (Grannas, Beaumond, Dettori,…)
- Rules and standards for openness: open interfaces, open platforms, digital ethics (Beaumond, Riguidel, Willmott, De Fillippi,…)

The online consultation added a number of complementary and overlapping themes. In general, it showed a great concern for the accessibility and openness of the internet. Net neutrality was often mentioned as a worthy objective, not only in the sense of the absence of control over internet traffic and content by ISPs, but also by other internet players. In this respect, decentralisation was regularly put forward as the preferred architectural principle:

> *"The internet is increasingly centralized onto few nodes of control. This centralization of data and therefore of services, is at the core of the power of Californian oligopolies. (..) So there is a lot of relevance for Europe to massively invest in the decentralization of the internet." (CEO of a 21 people startup founded in 2012, online consultation)*

Another common thread throughout the online consultation replies was the concern for privacy and security. Various respondents stressed that it must be allowed, at all times and for any purpose, to use strong encryption for communication between people, companies, and so on:

> *"Encourage the use of cryptography to establish and maintain various identities per person; one real, some pseudonymous." (Head of IT, University of Technology, online consultation)*

While cryptographic protection was primarily interpreted by respondents as a safeguard against governmental surveillance, they also stressed the importance of consumer privacy vis-à-vis large corporations. As an example, it was repeatedly argued that corporate business models thriving on the commercialisation of data generated by internet users call for research on how to collect and commercialize data in a technically and legally clean way.

> *"[The essential functional building blocks of the Internet should be that] all personal server-based data can be automatically requested by the person to whom the data belongs and a system is plugged in to make a correction of*

someone's personal data in order to avoid mistakes and costs. Everyone is allowed to be the master of his own personal data." (Media Designer, online consultation)

The upcoming permeation of users' daily lives, including their work, life, mobility and health contexts, by internet technologies was another prominent theme. Fast, reliable and omnipresent connectivity using common open standards was called for by many individuals.

"The best investment in the future of the internet and the society that uses it is to standardize and monitor the compliance to standards in communication. Currently, lack of clear and rigid standards holds back innovation because it favors large entrenched players." ("Senior Technical Advisor, expert on document standards, online consultation)

3. Challenges for the Next Generation Internet

An overall 'mission statement' that emerged for the Next Generation Internet is that it should enable the evolution of the Internet into a system that is able to sustain the current explosion in streaming and mobile traffic, cope with new demands caused by the massive proliferation of real-time data generation and exchange throughout the network, offer major improvements in terms of reliability, security and trust, and unleash a wave of opportunities for service and system innovation and value creation.

In 10 to 20 years, it is expected that staggering amounts of data will be available over the Internet, generated and consumed by people as well as by machines, and including public as well as proprietary sources. Moreover, analytic and processing capabilities will have further advanced and will offer intelligent machine learning mechanisms that drive the decision-making and operation of a multitude of systems and services. We will take ubiquitous access to information from everywhere for granted, and will be surrounded by systems that crucially depend on this data infrastructure. As Koziris argues,

"The Internet of everything will allow the smart interaction and pervasive connectivity of real-world physical elements among themselves. The enabling technologies will allow the ad-hoc creation of groups of nodes that can collectively perform sensing, processing, reasoning, communication and actuation tasks. Many domains such health, biology, entertainment, social life etc, but also to the extreme (e.g. Internet of NanoThings for the nanoscale world) will be transformed taking the end users into the driver's seat as active creators of data, content and intelligence."

Also telecommunications companies responding to the online consultation shared this view of a Next Generation Internet of very heterogeneous as well as ultra low-cost networks and devices, in order to enable real worldwide internet access across a multitude of contexts in an economically sustainable way:

"Infrastructure will need to be flexible and versatile to provide services with very different characteristics (e.g. high data rate with low latency for

mobile broadband, very low data rates for massive number of sensors, or highly reliable communications with extremely low latency for factory robots)." (large telecommunications company, online consultation)

As Canini states, this means that future networks require capabilities far beyond today's interconnection of clouds so as to incorporate mass-market Internet of Things devices as well as large-scale cyberphysical systems including mobility, safety and energy systems of cities, autonomous cars and ubiquitous drones providing massive "data torrents" from mobile, high-bandwidth sensors and actuators. Beaumond foresees that:

> "In 2025 the Internet is accompanying most of the day-to-day actions. Interactions with surroundings are done in a smooth and reliable way while the Internet allows for swifter decisions based on instant information available everywhere. The Internet is mainly used to enhance localized economy and activity.
>
> Because Data is open, exact consumption information is known; origin of production, transformation process as well as people involved. Ultimately businesses share their business plans and margins. Swarm data is continuously being collected by the crowd and shared for analysis and forecasts.
>
> On the other hand there is a greater control of personal data, we know what we share and with whom. Aggregated personal data is being used locally for a better self-optimization whilst isolated data is transferred anonymously for big data applications and insight on macro-perspective."

3.1. Highly distributed architectures and approaches

One major consequence of the above is the need for highly distributed architectures and approaches. As the number of network elements and edge devices scales up, there will be an explosion of massive short-length (often wireless) data exchanges among a multitude of distributed nodes at local level. To support such mass-scale volatile communication patterns, data should be stored, processed and consumed at local level. The mobile edge cloud will have become a reality. It is supported by micro data centers, providing relief to core networks and core data centres, improving latency bound applications performance and enhancing the user experience. Feldmann envisions that:

> "scalable data analysis (..) allows us to trace the *data processing pipelines* and enables us to answer questions such as "based on which data elements was this information derived", "did anyone tamper with the data". Indeed, we will have many different interacting data processing pipelines which will have to be mapped to CloudNets and the appropriate network hardware. Hereby, we have novel elements that allow us to sample data, aggregate it, process it, as well as share results in a data privacy preserving manner."

While highly distributed architectures fit well, amongst others, to industrial applications and services, various respondents in the online consultation also link this idea explicitly to our personal environment. Several online

contributions advocate the idea of 'personal clouds' to store and control personal data as

> *"a real and immediately usable replacement of the current services for email, web hosting and social networking. Besides, this "personal server" must be available as soon as possible, because the lock-in to existing walled gardens continues to grow with every month that people put more content and online interactions inside them." (Free Software & Open Data/Hardware/Standards popularizer/trainer , online consultation)*

This personal control is also tightly linked to authentication and the verification of identity, as various respondents argue:

> *"Perhaps the most dangerous development of today's Internet is that the few large players are positioning themselves up as "identity providers" — that is, they confirm whether a person is who they claim to be. This is something that should always remain under personal control, for instance contracted to a hand-picked party, rather than with a party whose earnings derive directly from indexing data and offering personalised advertisements." (Cryptographer, network architect , online consultation)*

The same idea of increased user empowerment and control also extends to the Internet of Things:

> *"Many devices will be connected to the internet. Hopefully, these devices will be under the control of the users, not the manufacturers." (Senior Technical Advisor, online consultation)*

3.2. Network virtualization and softwarization

A second, related evolution is the virtualization and softwarization of the network. As Canini states:

> "innovation in networking (not including transmission technologies) has been historically stagnant during the past couple of decades despite much research efforts. Only recently the emergence of technological trends such as Software-Defined Networking (SDN), Network Function Virtualization (NFV) and Programmable Dataplanes, coupled with the ever-demanding requirements of large data centers have spurred a renaissance of interest into bringing novel ideas for designing radically different networks. In addition, Software-Defined Radios (SDR) have enabled rapid innovation in a domain that used to be dominated by hardware.
>
> It is clear that this process is being enabled by the ability to innovate through loosely coupled, adaptive software components (rather than protocols and their standardization) and by a new generation of programmable hardware (which is far more open than traditional proprietary networking and amenable to experimentation). Thus, the process towards Next Generation Internet appears having to pass through the emergence of Software-Defined Infrastructure (SDI) and eXchanges (SDXes)."

Virtualization and softwarization refer to the separation between a simple and open hardware data plane and a dissociated programmable control plane. This virtualization will be everywhere, including network components, end-user

devices, and eventually even sensors. Virtualization enables us to transparently use resources, including computing, storage, and networking. The move towards software-defined networking and cloudnets thus leads to a single abstraction that provides an application with connectivity, storage, and processing capabilities irrespective of the underlying physical infrastructure.

The crucial role of the research community in designing, trialling and implementing such highly distributed, virtualised network infrastructures was highlighted by many respondents in the online consultation, e.g.:

> *"Like in the early days of the Internet it seems that Research Networks are best positioned to take the lead in this. They can deploy and test new protocols that are developed by researchers and industry. Obviously Governments and the EC must play an important role in facilitating (not determining) the development of this vital new infrastructure." (joint contribution by current and former Research Network CEOs and Internet Hall of Fame inductees, online consultation)*

3.3. Resilience and trust

Both in terms of the present as well as the Next Generation Internet, an overhaul is needed in terms of security. Leenaars, for instance, states that today's innovations are taking place on what is essentially an unsafe *Trojan Horse,* given the increasingly untrustworthy core of the Internet. Related to future architectures, Feldmann argues:

> "Hereby, all services have to operate on a *reliable* and *secure* infrastructure. This means, that not only each component by itself has to be secured and configured appropriately, but also the overall system does not have weaknesses. Thus, security has to make a significant step forward towards *usable security* in the sense that it can actually be used by everyone. Misconfiguration opportunities have to be minimized. Moreover, vigilant security awareness helps in minimizing problems and/or fix them as soon as they are noticed.
>
> While putting an emphasis on reliability we also have to realize that problems and system failures cannot be avoided. Purely, due to scale individual components or even subsystems will fail. Thus, our toolbox will now include scalable methods that let us *debug* this complex Internet infrastructure and its services. We have to be able to trace service misbehavior to the responsible system component. We also need to determine which services are affected if a system component fails."

However, as Driot argues, the goal of a totally secure and managed Internet will not be attained, and is maybe even unwanted because of a number of trade-offs involved. Thus, a third major aspect is the need to achieve resilience and trust within a so-called unreliable and trustless Internet context. Blockchain technologies offer a distributed architecture for timestamping, recording and executing contracts, transactions and services that is resilient and able to achieve trust-by-design, with potentially disruptive consequences. Programmable and decentralised blockchain databases open the way for automated and distributed consensus and exchange without the need for a so-called trusted third party.

However, this is only part of a much more encompassing social, technical, institutional and economic transformation that should lead to more openness, transparency, interoperability and ubiquity of information and services. De Filippi argues that this leads to a situation where 'Intertrust' should supplant the Internet:

> "Beyond financial applications, the blockchain can also be used as a decentralized and tamper-proof registry of titles, such as a land registry (..) or as a way to record any contractual or licensing agreements, such as intellectual property.
>
> In the context of Internet of Things and smart cities initiatives, it is estimated that there will be over 50 billion interconnected devices in 2020, each needing to communicate and transact with one another. Because no central public or private authority could possibly act as the central clearing for all of these transactions, the blockchain provides an efficient and secure solution to govern and execute trillions of transactions in a trustless manner.
>
> Finally, the most recent versions of the blockchain make it possible to execute complex code, in a decentralized and deterministic manner, without relying on any central server.
>
> This allows for the creation of decentralized applications (such as decentralized market places, or decentralized prediction markets), which are neither owned nor controlled by anyone, but simply subsist on the blockchain, and are executed each time someone interacts with them."

These new opportunities are also often highlighted by the respondents to the online consultation. Various solutions to embed data protection in the core design of the next-generation internet are advocated:

> *"Data needs to be encrypted and packaged with a usage policy. When accessed, data should consult its policy and attempt to re-create a secure environment using virtualization and reveal itself only if the environment is verified as trustworthy." (Professor of Telecommunications, online consultation)*

Again, the role of openness and standards is stressed in order to increase trust and avoid centralised control. Several respondents call for the active involvement of the European innovation stakeholders in the creation and implementation of open standards, as a way to enable a more level playing field in which communication and transactions are more secure and competition can thrive.

> *"The European research community should be encouraged to contribute and play a more active role in IoT standardization and IoT interoperability solution design." (foundation promoting international cooperation, online consultation)*

3.4. Cybersocial and cyberphysical system redesign

The final consequence is the need for cybersocial and cyberphysical system redesign. As Leenaars argues:

> "The internet is a complex, heterogeneous system with many different

types of actors and many co-dependencies on different layers and within applications. Even disregarding geo-political and historical aspects, some very large actors have economic interests that are opposite to the interest of European society and democracy. It takes a structured approach and clear vision to tackle the issue. Anyone that wants to change the way the internet works, needs to take not some but *all* the necessary practical aspects into account – creating a proof-of-concept or even a production ready piece of software (no matter how great) or writing some technical specification (no matter how brilliant) is just the beginning of the path to adoption. In virtually all cases there is an orchestration issue where many different mutual dependencies need to be resolved – involving many different applications, devices, services providers, routing infrastructure, DNS registries and registrars. The need for modernisation (security hardening, better scalability, standardisation to disentangle dependencies on specific actors while preserving economy of scale) may be manifest to all, but the actual real world cost of modernisation and its benefits are not equally divided."

In order to realise such wide-ranging redesign and adoption, online respondents argue that systemic solutions for the digital society need to be favoured over "yet another algorithm". Concepts such as user-centric innovation and direct interaction with end users at each stage of innovation are advocated in order to generate a multitude of ubiquitous services enabled by decentralization, softwarization and distributed trust:

> *"We absolutely need to develop ways in which co-creation can be facilitated, including all stakeholders in the process, and learning from current best practices of open source." (CEO, expert in open, online consultation)*

Highly dynamic platforms will be able to connect and operate cloud and network components as well as end-user and IoT devices as logical resources independent of underlying physical constraints. Driot states that the end of data locality renders possible services that are powerful, automated, and ubiquitous. They can be related to an end-user, to a machine or to industrial systems and will rely on real-time personalisation, data and resource locality independence, and industry-grade performance.

As Grannas argues:

> "I see the next generation internet as both a front-end and glue to new and emerging man-machine ecosystems. A next generation internet creates kind of an omnichannel user interface marginalizing the keyboard and increasing the importance of graphics, speech, motion detection and sensing as new means for communicating with technology and between technologies. And intelligent technologies will be merged with virtually all new objects manufactured. This will have a profound impact on the well-being of our citizens in virtually all societal areas, such as new types of preventive health-care opportunities, intelligent mobility, self-alarming city infrastructure maintenance and new ways to develop pedagogics in education."

Some respondents to the online consultation echo this emphasis on citizen involvement and the development of skills and digital literacy:

> *"European citizens need to be educated from a very early age and re-educated throughout their lives on all aspects of the technologies they use. This will allow them to take more control over the digital aspects of their lives and be critical citizens and, on occasion, consumers of technological products/services. Investment in permanent education for all is by far the best investment the EU can make for its citizens." (IT-architect, Cybersecurity & IT-policy advisor to various European governments, online consultation)*

Also, this transformation of the cybersocial and the cyberphysical is impossible without the activation of experimentation ecosystems of large companies, SMEs, startups and venture capital funds; regions and cities; knowledge institutions and individuals. For example, Dettori states that a Single Startup Market, directly connected to technology innovation, is needed:

> "Well connected hubs of tech savvy entrepreneurs coupled with properly skilled and adequately funded venture capitalists, angels and corporate investors are the key ingredients to succeed in company formation and technology transfer.
>
> The European startup ecosystem should be the 'applied research lab' of Europe, and should be strongly connected with all the relevant institutional stakeholders and basic/applied research. It should be the main source of entrepreneurial and managerial talent for our society, a way to access new markets, globalize businesses and feedback all of these values into the corporate world."

Finally, online respondents stressed the importance of smart citizen engagement methods for such systemic redesign:

> *"In user engagement it has become increasingly difficult to involve and engage users since users today are overwhelmed with requests for input, insights and information. It is therefore a great need to develop smart citizen engagement methods by combining technology, human needs and drivers, and societal challenges into innovative and responsible solutions." (Associate professor in Information Systems, online consultation)*

4. Technology areas

In order to realise all the ambitions set out above, a number of critical elements for a future work programme can be identified. This was mainly the topic of the expert workshop and contributions. The experts repeatedly argued that meeting the above challenges will require both fundamental research dealing with the formal foundations for reasoning about and programming next generation networks, services, and applications, understanding and controlling their dynamics, as well as applied, interdisciplinary work that blends together system prototyping, deployment, testbed operation with use cases and addressing the key contextual roadblocks to service innovation.

In particular, a number of areas stand out where European action is required in order to strengthen its competitive position. During the workshop, three technology areas were identified where major opportunities are present, along with a number of key actions needed for large-scale service innovation in a Next Generation Internet context.

4.1 Real-time pervasive data analytics

The first area is that of real-time pervasive data analytics. Current state-of-the-art developments in big data analytics focus mostly on processing-related aspects executed in large, centralised data centers. It appears that a major opportunity for European stakeholders refers to leveraging the power of big data on edge devices, including machines, vehicles, phones, wearables, and so on. Koziris proposes in this respect that:

> "Micro Data Centers are bringing cloud services to the edge; we could refer to this notion as Smart Internet (much like in the same way that Smart Grids should generate and consume energy at local level). To achieve this, a range of technologies should be innovated that will provide support for the flexible, ad-hoc creation of smart clusters, i.e. large groups of self-organised nodes that can collectively perform sensing, processing, reasoning, communication and actuation tasks, taking the concept of fog computing to the next level."

Distributed data analytics dealing with the enormous amounts of data that are going to be generated at the edges of the network, will be highly important for the competitiveness of any service or system that is part of, or using, the Next Generation Internet. Research should focus on approaches that envision the Internet primarily as an infrastructure to process data. This means solving critical issues at hardware and software levels related to low latency data networking, data processing pipelines, ubiquitous access to data, machine learning and decision-making, real-time customisation and personalisation, long-term scalable backups and storage, etc. Feldmann argues that:

> "With regards to the data processing pipelines we also have to address questions of the data processing plane:
> - How to find data that enables us to answer a question?
> - How to combine data in intelligent manner to derive information via novel machine learning mechanisms?
> - How and where to sample data/information?
> - Where to store which data/information?
> - Which access control mechanism should be used?
> - How to keep the data from being misused?
> - How to trace the data processing pipeline?
> - How to provide long term scalable secure backup?
> - How to enable information sharing?
> - How do we price information? How do we price data? What are the resulting pricing models?"

4.2 Software-defined networking

The second area is that of software-defined networking. The European opportunity is firstly related to the evolution towards software-defined infrastructure and software-defined exchanges. As hardware is increasingly commoditised, research and development are needed on the integration of software into the network and on the definition and evolution of the Next Generation Internet control plane in terms of the abstractions of the infrastructure, the distribution of functionalities and control, the way to define and allocate resources to applications, deployment and configuration issues, scalable methods for debugging complex internet infrastructures and services and so on.
For example, Canini states that:

> "Major ongoing trends such as smart grid, smart transportation, smart cities, electronic voting, green economy, online education require better infrastructure as the Internet is ill suited for many new requirements of these technological innovations. Below I suggest that SDXes fit into these themes by giving three examples. I believe that many more exist and that research on next generation networks will be more likely to succeed if the research program is able to "think big" about and connect the research with its potential for enormous impact on our society.
> - SDXes for resource fluidity. Connecting hundreds of networks each, an interconnection of SDXes can become a key enabler for better sharing of bandwidth and other resources.
> - Crowd-sourced SDXes. A global network of SDXes can ensure that independent networks can be quickly constructed and operated when times require it (e.g. natural disasters).
> - SDXvaults. In the IoT era with massive data acquisition capabilities, SDXes stand to act as a neutral common ground providing brokering services for privacy-preserving data aggregation and analysis between producers and consumers of such data."

Secondly, there is an even broader opportunity related to the performance and security of the Internet. European industry will benefit greatly if R&D in this field leads to an 'industrial-grade Internet' where SLAs can be given related to very complex operational technologies connected to the Internet, as well as from more secure web architectures and standards, where the risks of malfunctioning, attacks and unlawful surveillance are strongly diminished. In the view of Canini,

> "Future networks will need to ensure far better security than current Internet. There are security issues that must be addressed in the design of an SDI-based network infrastructure including preventing route hijacks, detecting and mitigating DDoS attacks. Beyond DDoS mitigation, SDXes might enable new architectures that can help by design address network attacks. For example, they provide an opportunity to reconsider the line of research on network capabilities as they might be a way to embed costs into traffic, such that costs can act as a deterrent for attackers."

4.3 Trust-by-design

The third area is that of trust-by-design, as embodied a.o. in blockchain technologies. Presently, this approach is being applied mostly to financial services, and is expected to lead to disruptive effects in this domain. However, Europe should actively explore the principles and application of trust-by-design in a plethora of other areas. These may be related to transparency and accountability, but also to distributed data governance and distributed innovation and collaboration. Application domains include new business ecosystems, the sharing economy, identity and profile management, e-democracy, as well as all sorts of autonomous and critical systems and infrastructures. Besides technology development, Europe should also invest in architectural work that generalises and extends such distributed models for reliability and trust.

In addition, research needs to derive ethical frameworks, safeguards and regulation pertaining to the design and management of digital networks, services, identities and hybrid digital-physical systems (cars, drones, digital implants,…). Riguidel argues in this respect:

> "Engineering in IT ethics will affect the extension of existing computer languages, cryptographic protocols and methods of dissemination services (license agreement) and the trust models, and will allow a better deployment and acceptability of SDN-NFV (Software-defined networking – Network Function Virtualisation).
>
> Industry and research cannot leave this field as alone legal field: the weight of non-consideration of technical reality brings bad solutions. Ignorance of technical induced delays (hence the type of legal decisions made fait accompli), misunderstandings (hence technology development abort, following early hijackings usage). Technologies are often praised by marketing orchestration, or convicted by movements of opinions on social networks: peer-to-peer architecture and illegal downloading, blockchain technology and virtual currency managed in the dark (bitcoin), social networking and use of personal data.
>
> (..) The obligation of reciprocity between actors (users, suppliers, etc.) for effective dialogue between stakeholders (commitment and response to some questions, in the form of computer probes) may be a way out of the rut in which the today's interconnected world has weakened. A whole set of methodologies, models and tools could be developed to design and implement digital ethics as a new engineering domain, taking account European values: privacy, dignity and sovereignty of citizens."

4.4 Experimentation ecosystems for the Next Generation Internet

In order to reap the benefits from the technologies mentioned above, it appears paramount that Europe actively creates the right context for these innovations, i.e. by stimulating the set-up and development of experimentation ecosystems related to the Next Generation Internet. Since hybrid digital-physical-social transformations are involved, it cannot be expected that solely new IPR development will be sufficient to propel Europe into a leading position. The key

to success seems the organisation of European ecosystems of all relevant stakeholders that are willing to evolve and take risk jointly. Grannas argues that, as the usability of our physical environment itself will be altered deeply, citizens need to be involved in the redesign. Also, in such a transition to an 'Omninet', or omnipresent Internet, an experimenting culture, which is not only limited to e.g. big companies and big cities, but also encompasses small cities and small companies, is not just a nice-to-have, but a need-to-have.

Therefore, many experts stressed that Next Generation Internet research and development should, in an early stage, consider and include service creation, user experience and user behaviour, business model innovation, incentives to invest, city and regional involvement, open standards and open interfaces, the activation of SMEs, tech startups and creative industries, and so on. For example, Wilmott claims that:

> "While it may seem obvious that interfaces are valuable, the arenas they make sense in may not all be obvious. Traditionally standards have been applied to low level areas of the technology stack (network protocols, encryption etc.). However, innovation has moved "up the stack" into applications, web systems and higher level systems. This means there are now huge benefits possible from:
>
> 1. Standardizing higher level technical infrastructure such as identity systems, rights management, security, location etc.
> 2. Developing standards for specific domains. (..) Such specifications are an enormously valuable resource. Especially if evolved over time and deployed widely. They:
>
> - create the ability for compatible platform software and app software to be developed
> - act as an attractor for an ecosystem of commercial and open source implementations
> - drive down costs for buyers (…) since vendors conform to a public standard, making them compete without interface lock-in
> - spur innovation by reducing to learning curve across users for access to systems for developers of new applications
>
> The effect of such higher level, domain specific interfaces cannot be under-estimated. Evolving these would provide Europe which huge leverage in European and global markets."

For this, a targeted approach is needed, incorporating mechanisms such as co-creation, city-wide living labs and innovative procurement targeted a.o. at startups and SMEs. Grannas recommends therefore the following points to be taken into future work programmes: "

1. Projects furthering omnichannel man-machine interaction
2. An experimental iterative approach for project execution using an open platform for innovation together with methodologies such as co-creation, living labs and innovative procurement
3. Incentive for getting small and mid-size front-runner cities involved in the co-creation of next generation internet as a network or jointly with larger cities. This because most European citizens live in small

> and mid-size cities, large size is no more required for creating permanent impact and because these cities work best together with SMEs."

Other potential mechanisms are mentioned by Beaumond:

> "Instead of highly bureaucratic grants, collaborative voting platforms can act as venture capital to allocate budget into start-up companies. Stimulating project based learning in incubators and makerspaces while not rejecting failure could help access to IT education for all."

Encouraging or even mandating open source developments in areas like distributed data analytics, in order to boost the opportunities for SMEs to develop applications and services, was also put forward as a valuable instrument. Leenaars argues that more budgets should be allocated to European frontrunners in open source developments related to the Next Generation Internet. He claims in this respect:

> "At the heart of a new strategy for Future Internet lies a recognition of the Commons, and a willingness to contribute to cleaning up technical debt, as well as maintenance and future development. The focus on 'innovation' is a mismatch. Open source and open standards are what really drove the internet as a decentralised enabler, and moving the mass of the current internet involves a structural investment. The strong European open source ecosystem has had tremendous impact on the growth of the internet: it produced its dominant operating system (Linux) and leading distributions such as Debian), the first public domain webserver, key open source programming languages (PHP, Python) and databases (MySQL, MariaDB). Each of those technologies became part of the fabric of the internet, and both the strategy (open source enables the creation of a Commons to power permissiveless innovation) and the wider ecosystem itself are essential to any upgrade and the future of the internet."

Related to regulation, Riguidel argues the need to combine technological R&D with the engineering of regulation, to aim at a 'New Deal' with the digital world that embeds ethics into the design. While the EU currently does a lot of work on data protection, the realm of software is left as dark and obscure, and we lack a body of basic rules and guidelines related to algorithms. Canini agrees on the need to regain control of software developments, i.e. through a 'democratisation of software'.

Finally, in terms of application domains, efforts need to be concentrated in areas that are particularly relevant for Europe, including digital fabrication and Industry 4.0, smart cities (not just large cities but also small and medium-sized ones), mobility and logistics, and hybrid online-offline business and retail. Several workshop participants conclude that it would be useful to envisage further iterations, focussing on the increasing interdependence of these domains with the virtualised infrastructure underneath.