



**ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS
DEPARTMENT OF INFORMATICS**

Information Security and Critical Infrastructure Protection Research Group

Director: Dimitris A. Gritzalis, Associate Professor (ICT Security)

**Ambient Intelligence:
The Promise, the Price, and the Social Disruption**
A Review of Security and Privacy Strategies in Leading Economies

Dimitris **Gritzalis**, Marianthi **Theoharidou**
Stelios **Dritsas**, Giannis **Marias**

**Review Report Series
No. 1 (2006)**

Report code: AUEB-CIS/REV-0106/v.2.9/19.03.06

March 2006



Athens University of Economics and Business, Dept. of Informatics
Information Security and Critical Infrastructure Protection
Research Group
76 Patission Ave., Athens GR-10434, Greece
Tel.: (+30) 210.8203505, 210.8203157, Website: www.cis.aueb.gr

The Vision...

“...Inspired by the social scientists, philosophers, and anthropologists, we have been trying to take a radical look at what computing and networking ought to be like. We believe that people live through their practices and tacit knowledge so that the most powerful things are those that are effectively invisible in use. This is a challenge that affects all of computer science. Our preliminary approach: Activate the world. Provide hundreds of wireless computing devices per person per office, of all scales This has required new work in operating systems, user interfaces, networks, wireless, displays, and many other areas. We call our work "Ubiquitous Computing". It is invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere...

...For thirty years most interface design, and most computer design, has been headed down the path of the "dramatic" machine. Its highest ideal is to make a computer so exciting, so wonderful, so interesting, that we never want to be without it. A less travelled path I call the "invisible"; its highest ideal is to make a computer so imbedded, so fitting, so natural, that we use it without even thinking about it. I have also called this notion "Ubiquitous Computing", and have placed its origins in post-modernism. I believe that in the next twenty years the second path will come to dominate. But this will not be easy; very little of our current systems infrastructure will survive...”.

Mark Wieser, 1996

*There is more information available at our fingertips
during a walk in the woods than in any computer system,
yet people find a walk among trees relaxing and computers frustrating.*

Mark Wieser, 1991

Abstract: In his seminal papers of early 90s, Wieser introduced the concept of ubiquitous computing as that describing the new paradigm of the Information and Communication Technologies of the 21st century, a paradigm to follow and replace network computing. Wieser indicated that the most profound technologies are those that disappear and weave themselves into the fabric of everyday life until they are indistinguishable from it. He envisioned that in the context of ubiquitous computing anyone would be able to be connected to anything, from anyplace and at any time. Nowadays, ubiquitous computing is perceived as an enabling technology of Ambient Intelligence (AmI), a more abstract and generic concept, referring to the emerging ICT paradigm. AmI implies a seamless environment of computing, advanced networking technology and specific interfaces, which is aware of the specific characteristics of human presence and personalities, takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire, and even can engage in intelligent dialogue. One of the most important characteristics of this paradigm is the fundamentally new security and privacy threats and vulnerabilities that appear in this context. In this report, we comparatively review the AmI paradigm, as it emerges in three of the currently leading economies, namely: European Union, United States and Japan. The review is performed with an eye towards the security and privacy protection strategies, policies, and priorities, which are adopted and put in practice by each of these economies and governments. We identify agonies and trends of the local governments and industries, we discuss the way this new concepts is perceived in each national context, we describe the strategic plans under development and their cornerstones, and we review the strategies adopted by the local governments in order to deal with the rising security and privacy risks. Finally, we provide the reader with a consolidated review of the strategies, which are currently adopted and those which under development, for protecting privacy and strengthening security in these three economies.

Key words: Ambient Assisted Living, Ambient Intelligence, Confidence, European Union, Information and Communications Technologies, Japan, Pervasive Computing, Privacy, Security, Trust, Ubiquitous Computing, Ubiquitous Network, United States.

Acknowledgments: A brief version of this review was presented at the *Safeguards in a World of Ambient Intelligence (SWAMI) Conference*, European Commission (JRC/IPTS), Brussels, 21-22 March, 2006. D. Gritzalis would like to thank the organizers of the event for their invitation and sponsoring. Furthermore, the authors wish to thank Vassilis Tsoumas for his useful comments and suggestions.

Table of contents

0	Introduction	5
1	European Union	7
1.1	Agonies and Trends	7
1.2	Envisioning the Emerging ICT Paradigm	8
1.3	Cornerstones and Strategic Planning	10
1.4	Security and Privacy Strategies	12
2	United States	15
2.1	Agonies and Trends	15
2.2	Envisioning the Emerging ICT Paradigm	17
2.3	Cornerstones and Strategic Planning	19
2.4	Security and Privacy Strategies	24
3	Japan	30
3.1	Agonies and Trends	30
3.2	Envisioning the Emerging ICT Paradigm	32
3.3	Cornerstones and Strategic Planning	35
3.4	Security and Privacy Strategies	38
4	Towards a Consolidated View	43
4.1	The Strategic Situation	43
4.2	The Vision and the New ICT Paradigm	50
4.3	Security and Privacy	51
4.4	Social Disruption	52
	References	54
	Short CV of the authors	57

0 INTRODUCTION

Anthropologists teach that the people of Fertile Crescent invented the first information technology, i.e. that of capturing words on flat surfaces by using abstract symbols. This invention, this technology, is called literacy. Long after this invention, literacy was expensive, tightly controlled, and precious. In the rise of the 21st century, this invention effortlessly and unobtrusively surrounds us. Anthropological studies of work life teach that people primarily work in a world of shared situations and unexamined technological skills [Suc-85, Lav-91]. Weiser argued that “the most profound technologies are those that disappear and weave themselves into the fabric of everyday life until they are indistinguishable from it” [Wei-91].

Nowadays, computers in the workplace or information appliances at home can be as effortlessly and ubiquitous (the English word “ubiquitous” came from the Latin and means “existing everywhere”) as that. In late 80’s visionaries argued that “PC and workstation will wither because computing access will be everywhere: in the walls, on wrists, and in scrap computing, lying about to be grabbed as needed” [Wei-93b]. Wieser called this situation “ubiquitous computing” (UbiComp). What differentiates the existing network computing paradigm from the emerging UbiComp paradigm is the centre of attention. In specific, in network computing the computer - rather than being a tool through, which we work and which disappears from our awareness - usually remains the focus of attention. On the other hand, ubiquitous computing aims at enhancing computer use by making computers available through the physical environment, but making them effectively invisible to the user, and keeping the user at the centre of attention. Weiser argued that such a disappearance is a fundamental consequence not of technology, but of human psychology, as whenever people learn something sufficiently well, they cease to be aware of it.

The shift from the existing to the emerging paradigm requires advanced research in numerous areas of computer science and engineering, including hardware devices (i.e., sensors, actuators, etc.), network protocols and technologies, interaction substrates (i.e., software for screens, pens, etc.), security and privacy technologies, etc. Considerable work has already been done, and much research is still in progress (particularly in view of the 4G technology), regarding the development of a robust mobile infrastructure for wireless networking (Fig. 1).

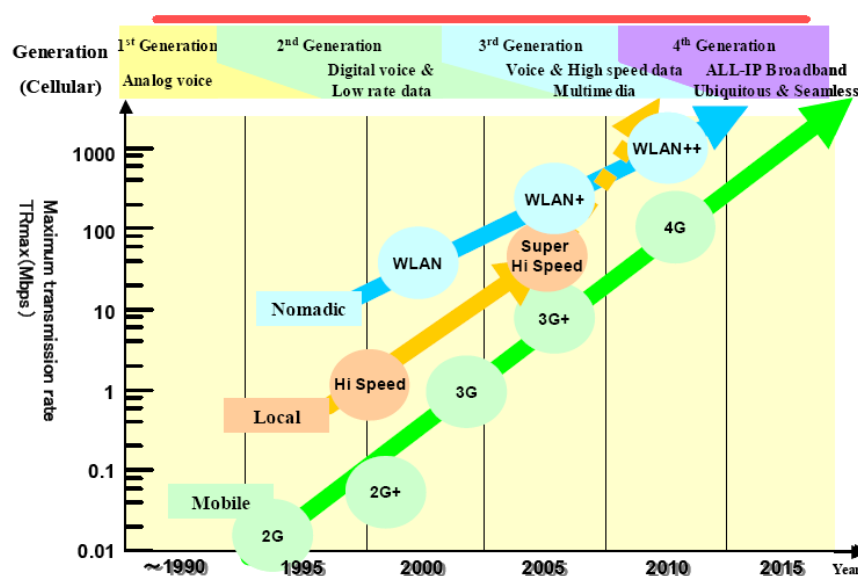


Fig. 1: Transmission rate enhancements toward 4G mobile systems [MITF-04]

As a result of this rapidly developing market, the penetration of the mobile and the broadband market in China, Japan, Russia, Korea, United States, and in some of the leading EU economies grows fast (Table 1). An overview of the recent history (2001-04) of the broadband penetration rate for the G7 countries appears on Fig. 2 [ITU-05, J&P-05, OECD-05].

Table 1. Mobile and Broadband Market (as of 31.12.2004)

Economy	Mobile Market			Broadband Market		
	Subscr's (M)	Penetration (%)	As % Internet subscr's (M)	Subscr's (M)	Penetration (%)	3G ¹ mobile subscr's (M)
China	334.8	25.5	8.71	² 1.51	² 21.30	² 60.3
Japan	91.5	71.6	25.70	19.10	14.90	56.4
Korea (Rep.)	36.6	76.1	27.51	11.92	24.90	99.1
Russia	74.4	51.6	0.18	1.24	0.87	*
United States	181.1	61.0	49.50	37.89	12.80	59.5
European Union	France	44.6	73.7	0.04	6.75	56.6
	Germany	71.3	86.4	0.25	6.90	*
	UK	61.1	102.8	2.83	6.26	39.6

¹ 3G mobile refers to services using CDMA 2000 1x, CDMA 1x EV-DO and W-CDMA standards. ² Data refer to Hong Kong (China). * Not referred to in the reviewed ITU and OECD reports.

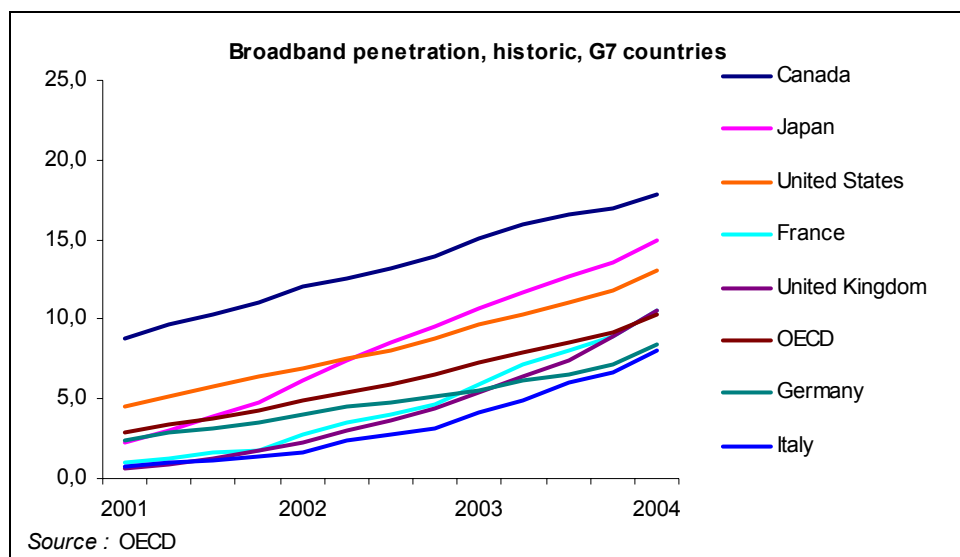


Fig. 2: G7 Countries - Broadband Penetration [OECD-05]

A diametrically opposed to the UbiComp vision is “virtual reality”, which attempts to make “a world inside the computer”. Virtual reality focuses an enormous apparatus on simulating the world, rather than on invisibly enhancing the world that already exists. The opposition seems so strong that the term UbiComp may be replaced by “embodied virtuality”, which refers to the process of drawing computers out of their electronic shells. By pushing computing devices in the background, UbiComp may make individuals more aware of the people on the other end of their computing links and reverse the centripetal forces that the conventional PC introduced. Wieser argued that UbiComp may mean the decline of the computer addict and help overcome the information overload problem [Wie-91].

1 EUROPEAN UNION

1.1 Agonies and Trends

In the European Union (EU), the emerging ICT paradigm is cultured under the notion of Ambient Intelligence (AmI). The European vision of AmI is introduced by the Information Society Technology Advisory Group (ISTAG), which advises the European Commission's Information Society Directorate General. ISTAG has published several reports, which identify the European vision, agonies, considerations, and plans [IST-03].

EU adopted the term "Ambient Intelligence" (AmI) and considers it different from such concepts, as "Pervasive Computing", "Ubiquitous Computing", etc. According to [IST-01], AmI implies a "seamless environment of computing, advanced networking technology and specific interfaces, which is aware of the specific characteristics of human presence and personalities, takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire, and even can engage in intelligent dialogue". AmI should also be unobtrusive, often invisible: everywhere and yet in our consciousness - nowhere unless we need it. Interaction should be relaxing and enjoyable for the citizen, and not involve a steep learning curve" [IST-01]. ISTAG envisions *humans* who will be surrounded by *intelligent interfaces* supported by computing and networking technology which is *everywhere, embedded in everyday objects*, such as furniture, clothes, vehicles, roads and smart materials, even particles of decorative substances like paint. Such an environment is sensitive to the presence of living creatures (persons, groups of persons and maybe even animals) in it, it remembers and anticipates behavior, and supports their activities [IST-02b].

AmI is considered to stem from the convergence of three key technologies: Ubiquitous Computing, Ubiquitous Communication, and Intelligent User Friendly Interfaces. Therefore, EU considers AmI as a superset of these technologies/terms and as a broader concept. AmI does not associate with a specific technological framework but focus on the use of the technology - by the individual, by business, and by the public sector.

ISTAG claims that Europe should adopt a holistic view of AmI, considering "not just the technology, but the whole of the innovation supply-chain from science to end-user, and also the various features of the academic, industrial and administrative environment that facilitate or hinder realisation of the AmI vision". It promotes cooperation between academia and industry regarding ICT and co-evolution of the technology and the market; thus, adopting a business-oriented perspective.

The holistic EU AmI vision also includes societal agonies and interests. Its goal is "to enable and facilitate participation by the individual - in society, in a multiplicity of social and business communities, and in the administration and management of all aspects of their lives, from entertainment to governance" [IST-03]. ISTAG emphasizes on the need to advance towards a more holistic understanding of AmI and how it can be applied within a social context. The scenarios described in the Grand Challenges for IST report [IST-04] envision a society where people live in and navigate between (both physically and virtually) different interconnected social settings (the home, workplace, school, hospital, social care facilities, cultural institutions etc.), within which they may adopt multiple roles and may have different needs that depend on both the physical context and the mood of the individual. In each described scenario, societal and ethical challenges are highlighted.

Lately, formal European Union documents regarding the 7th Framework Programme of the Union introduced the term "Ambient Assisted Living" (AAL) [EU-05a, EU-05b, EU-05c,

EU-05d]. In the given context, AAL seems to refer to an emerging context, where AmI is expected and envisioned to act as a kind of abstract guidance.

1.2 Envisioning the Emerging ICT Paradigm

The EU, as US and Japan, works towards a new ICT paradigm, which will implement the Ideas of Ambient Intelligence, which were described above. The EU vision places emphasis on the adoption of a holistic view that associates the technological, societal and economic aspects of AmI. This is described in ISTAG ‘3-layer’ model presented in Fig. 3. Societal and economic challenges (Fig. 4) are placed at the top layer, technologies at the bottom layer, and a “middle layer” is introduced, which is called the *AmI Space* [IST-02b].

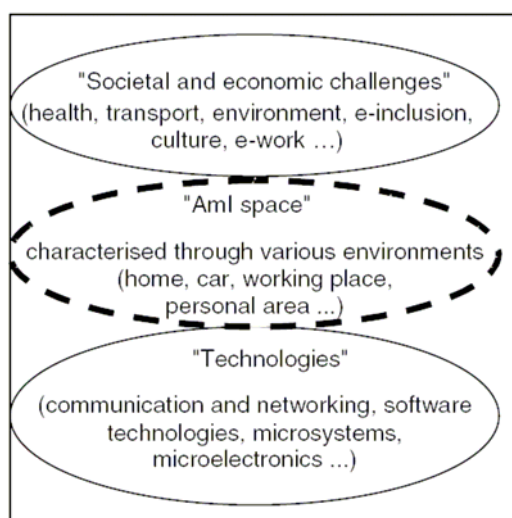


Fig. 3: The AmI Space [IST-02b]

The notion of AmI Space is not constructed as a physical layer of infrastructures, hardware, platforms, services, or applications, but a combination of the above. Originally, AmI Space was an abstraction, with properties, which could be presumed to be available to specific environments. However, later it became apparent to the ISTAG that instantiation of an actual AmI Space will be crucial to the realisation of the Ambient Intelligence vision [IST-02b].

The humans and physical entities - or their cyber-representatives - together with services share this new space, which encompasses the physical and virtual world, the AmI Space. This space needs to be engineered so it has predictable behaviours, so that services can be offered through it, and so it can manage complicated many-to-many relationships. The AmI Space could be seen as the integration of functions at the local level across the various environments, enabling the direct natural and intuitive dialogue of the user with applications and services spanning collections of environments, as well as at the cyberspace level, enabling knowledge and content organisation and processing [IST-02b].

Accordingly, the AmI Space is composed of collaborative (location or social based) sub-spaces, of devices (including sensor and actuator systems), services (including their interfaces) and the connecting networks [IST-02b]. Its characteristics include: (a) openness, to allow evolution and extendibility with autonomously developed components, (b) dynamism, to allow constant reconfiguration, and (c) trustworthiness, to handle issues of safety, reliability, security, privacy and usability.

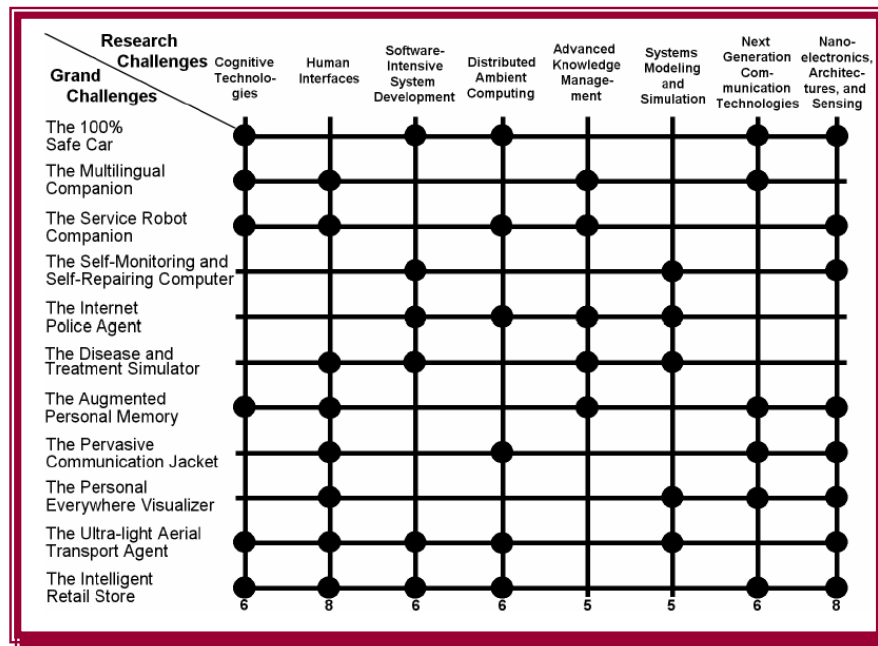


Fig. 4: Grand Challenges and Research Challenges in the EU [IST-04]

This new form of *system* is composed of *networked* (using a changing collection of heterogeneous network) *embedded systems*, which host *services* that which can be viewed as dynamically configured distributed *components* (autonomously developed, loosely coupled). This system must:

- "know itself" - and its components must also possess a system identity,
- configure and reconfigure itself under varying (and, in the future, even unpredictable) conditions,
- never settle for the status quo - it always looks for ways to optimise its workings,
- be able to recover from routine and extraordinary events that might cause some of its parts to malfunction,
- be an expert in self-protection, since a virtual world is no less dangerous than the physical one,
- know its environment and the context surrounding its activity, and act accordingly. It will find and generate rules for how best to interact with neighbouring systems,
- not exist in a hermetic environment. While independent in its ability to manage itself, it must function in a heterogeneous world and implement open standards,
- anticipate the optimised resources needed while keeping its complexity hidden.

As described in [IST-02b], the *Ami Space* should be able to:

- *Interact with the user* by taking into account her preferences. Natural interaction with the user replaces the keyboard and windows interface with a more natural interface like speech, touch, or gestures.
- *Model the user behavior* to keep track of all the relevant information concerning a user, automatically builds the user preferences from his past interactions and eventually abstracts the user profile to more general community profiles.

- *Model the environment and sensors available to perceive it*, to take care of the world model. This essentially deals with the list of authorized users, available devices, active devices, state of the system, etc.
- *Control security aspects* to ensure the privacy and security of the transferred personal data and deal with authorization, key and rights management.
- *Ensure the quality of services* as perceived by the user.

To accomplish this across different physical (home, private and public vehicles, private and public buildings, on the road) and social (family, clubs, enterprises...) spaces is not a trivial exercise and it is certainly not only technical. Examples of related issues include availability and protection (Digital Rights Management, DRM) of content, ownership, control, and access of personal data, regulations on network services, allocation of licensed and unlicensed radio frequencies for wireless networks, standardization of APIs, protocols and ontologies, and operational and business models on network infrastructures, etc. The multiplicity of AmI Space and its requirements are pointed out by [IST-02b] in Fig. 5.

ISTAG considers the home, car, the person and enterprise environments from the perspective of both the technological requirements in those environments, in order to realise the Ambient Intelligence vision, and the demands they make on Ami Space [IST-02b].

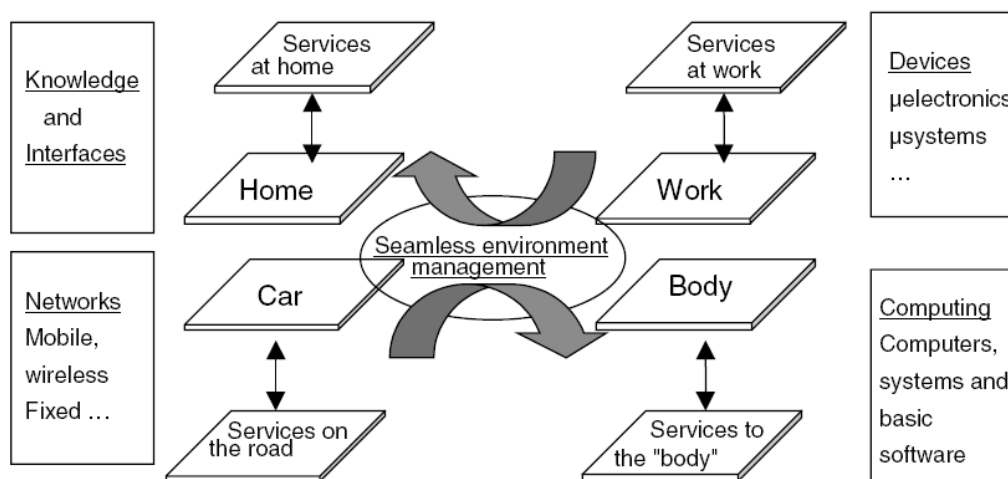


Fig. 5: Requirements to realise the AmI vision [IST02]

1.3 Cornerstones and Strategic Planning

A report that describes Europe's strategy in relation to AmI and ICT, was the "Strategic Orientations and Priorities for IST in FP6" report, which was published by ISTAG (2002). The report defines and describes the concept of Ambient Intelligence and provides guiding principles for the Information Society aspects of Framework Programme 6. During 2001-02, ISTAG recognised that the EU strengths in ICT lie primarily in mobile and wireless systems, in consumer electronics, in sectors such as automotive or aerospace, that deploy embedded ICT extensively, and in application sectors such as banking and manufacturing, and software suppliers to these sectors. ISTAG further recognised that promotion of the concept of AmI would build on these European strengths, facilitating the establishment of markets, thereby enabling more suppliers to grow and especially to gain critical mass for long-term viability.

This will strengthen the role of European industry in shaping the development of next-generation ICT.

ISTAG sees “significant opportunities” for AmI in relation to:

- Modernising the European social model particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services.
- Improving Europe’s economy in terms of: supporting new business processes; increasing the opportunities for teleworking in the networked home; enhancing mobility and improving all forms of transport; supporting new approaches to sustainable development [IST-03].

The following technology requirements for AmI could be identified: Req-1: Very unobtrusive hardware, Req-2: A seamless mobile/fixed communications infrastructure, Req-3: Dynamic and massively distributed device networks, Req-4: Natural feeling human interfaces, and Req-5: Dependability and security. On top of these generic technology requirements the following list of major research clusters emerged from the work of the scenario-building group:

- AmI compatible enabling hardware, including fully optical networks, nano-micro electronics, power and display technologies.
- AmI open platforms: for interoperating networks based upon a corporate effort to define a “service control platform”.
- Intuitive technologies involving efforts to create natural human interfaces.
- AmI developments in support of personal and community development, including socio-technical design factors, support for human-to-human interaction and the analysis of societal and political development.
- Metacontent services developments to improve information handling, knowledge management and community memory, involving techniques such as smart tagging systems, semantic web technologies, and search technologies.
- Security and trust technologies in support of privacy safety and dependability.

Technological requirements and research areas are also expressed by The Wireless World Research Forum (WWRF), which was founded in 2001 by Alcatel, Ericsson, Motorola, Nokia and Siemens and represents the European industrial perspective in AmI. The forum cooperates with and welcomes all interested parties (e.g. manufacturers, network operators and service providers, R&D centres, universities, and small and medium enterprises). The WWRF main reference remains *The Book of Visions* [WWRF-01], as its working groups and special interest groups have, as of today, not published new material. The vision expressed by this forum is the one of a Wireless World, as depicted in Fig. 6.

As [Fri-06] describes, Europe funds several actions in order to promote its AmI Vision. It uses the following methods and planning tools:

- *Scenarios* offer glimpses to the future and enable one to elaborate on the new situations and consequences of a new technology. A characteristic report is the AmI Scenarios created by ISTAG [IST-01, IST-04].
- *Roadmaps* are created in order to realise scenarios. They provide an overview of current developments and highlight barriers, gaps and bottlenecks that need to be overcome. Several European roadmaps related to AmI include Biovision, RAPID, PAMPAS, ACIP, etc.



Fig. 6: Building blocks of the Wireless World (in the Book of Visions)

- *Research agendas* follow roadmaps as they are designed in order to realise vision into reality by clearly indicating specific research areas. Research agendas are included in the e-Mobility and the ARTEMIS platforms.
- *Platforms* are a result of the cooperation between industry, academia, research institutions, governmental authorities etc., in order to implement a particular research agenda. These include the Wireless World Research Forum, ARTEMIS, eMobility, etc.
- *Projects* enable the implementation of AmI vision, as they focus in the deployment of a specific module that forms part of the greater vision. The European projects are numerous. Examples include PISA, PRIME, FIDIS, GUIDE, etc. [Fri-06].

One of the main European technology vehicles, the 7th Framework Programme, has as one of its major priorities *Cooperation*. Under this umbrella, EU will provide support to a wide range of research activities carried out in trans-national scientific and technological cooperation. Among them, *security* is defined as one out of nine major pylons for the *Cooperation* priority. The main objective of the Security pylon is “to develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism and crime, while respecting fundamental human rights; to ensure optimal and concerted use of available technologies to the benefit of European security, and to stimulate the co-operation of providers and users for security solutions” [EU-05e].

1.4 Security and Privacy Strategies

As already mentioned, ISTAG scenarios [IST-01, IST-04] provided insights regarding the societal, ethical and political aspects of AmI and their role in the realisation of the vision. The societal acceptance of AmI is based on the following factors: (a) facilitation of human contact, (b) orientation towards community and cultural enhancement, (c) building knowledge and skills for work, better quality of work, citizenship and consumer choice, (d) trust and confidence, (e) long term sustainability - personal, societal and environmental- and life-long learning, (f) “convivial technologies” that are easy to live with, and (g) controllable technolo-

gy by ordinary people. Therefore, any future scenario should take into account the future users' opinion, needs and anxieties about choices of systems, services and interfaces (Fig. 7).

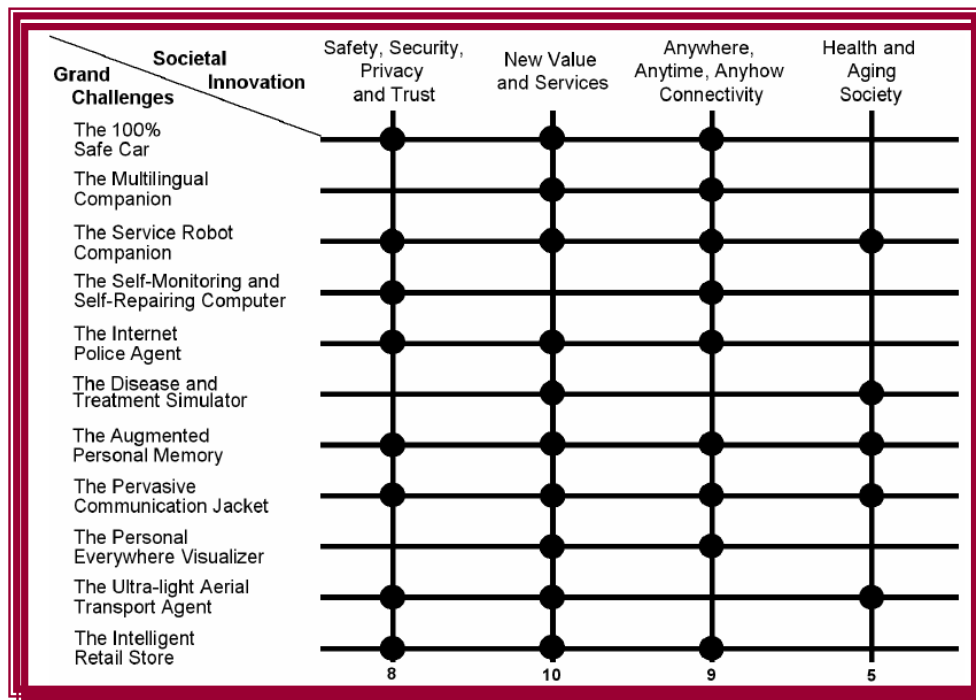


Fig. 7: Grand Challenges and Societal Innovation in the EU [IST-04]

The holistic view of AmI adopted by EU is reflected by the fact that the chosen scenarios include in their description societal, ethical, and political concerns. These include privacy, control and social acceptance issues. They also take into account the multi-cultural character of Europe by creating scenarios (e.g. the multilingual companion) that will allow cooperation of people in a diverse social, cultural and even political environment. The view of AmI is rather optimistic; however, it doesn't disregard the potential threats in this new environment. [IST-02a] recognises that the emerging ICT paradigm will require new security solutions, as it states that in order for Europe to acquire a leading position in security, it must focus research on the new security paradigm, which will address threats and risks within the AmI Space. Such a threat may be the fact that, despite the obvious benefits of AmI, one must not disregard the possibility of using AmI to enable or facilitate monitoring, surveillance, data searches and mining. This is an issue that doesn't concern only the civil rights and liberties of citizens but it concerns governments and industry as well.

In this context, people will participate “in a multiplicity of parallel, overlapping, inter-leaved and evolving one-to-one, one-to-many, and many-to-many relationships, some of which will be very short-lived, and some of them established temporarily and (apparently) instantaneously. Much of the communication between participants in these relationships will be asynchronous (as it is now): this means that 'virtually' applies to time as well as space” [IST-02a]. The current security solutions will probably prove to be insufficient in the new environment, because they are designed based on specific conditions which will not further apply, such as relatively *stable, well-defined, consistent* configurations, contexts, and participants to the security arrangements [IST-02a].

The emerging paradigm introduces the notion of “conformable” security, that is the degree and nature of security associated with any particular type of action will change over time and with changing circumstances and with changing available information so as to suit the con-

text. The security challenges posed by ISTAG are numerous and these are related to personal data protection and anonymity in a new highly personalised environment, to security management when the user adopts multiple roles and engaged in diverse relationships, to dependability and trustworthiness, to security awareness in a diverse group of users, to issues of emergent behaviour by an intelligent environment with unknown results, and more.

However, this is not only recognised as a potential gap or threat but as an opportunity for EU to increase its industry's competitiveness by exploiting this change in paradigm. It is also viewed as a necessary precondition in order to maintain an independent capability in the field of security for Europe [ISTAG-02a]. Europe is oriented towards user-friendly, acceptable and usable security that enables the use of the AmI products and not hinders their exploitation. It also aims to address different security aspects, such as security related to the individual, to communities and social groups, to the industry or to critical infrastructures. It also directs research to security for the evolving technological frameworks (e.g. mobile computing, grid computing, etc.).

The ISTAG vision is similar to the one described in the *Book of Visions* [WWRF-01], which suggests that end users/customers should be able to decide their security policies in a simple way and on their own. The concept is that they are provided with the means to achieve it without much complexity. ISTAG also says that any security rules must be "simple, user-understandable, user-friendly, intuitively usable, socially acceptable and based on co-operation". WWRF includes security and privacy in its building blocks needed in order to achieve a wireless world and establishes a Special Interest Group (SIG 2), which is addressing threats to privacy and security and what industry should do about them. One can conclude that the new paradigm's privacy and security issues are already raising consideration in Europe, both on a strategic and a technological level.

Further, and in the context of the AmI vision in the European Union, the concepts of *trust* and *confidence* are top horizontal ICT priorities, along with security and privacy [IST-03, IST-04]. Trust is recognized as a *resource* for social and business cooperation, whilst security is a *condition* for their enduring existence [IST-04]. Building citizens' confidence in AmI spaces should involve privacy issues, unfair or illegal commercial practices, unsolicited communications, and harmful content distribution. In this respect, specific new tools and methodologies are essential to improve technology and infrastructure dependability - in terms of self-testing, self-repairing, and fault tolerant - and thus enabling a trustworthiness AmI space, as failures in reliability, survivability, or adaptability will impact users' confidence in the Information Society.

2 UNITED STATES

2.1 Agonies and Trends

In US, current advances in ICT are enabling a new technology paradigm, which is cultured under the notion of Ambient Intelligence. According to the National Institute of Standards and Technology (NIST) [NIST-01], pervasive computing denotes the strongly emerging trend toward “numerous, casually accessible, often invisible, computing devices, frequently mobile or embedded in the environment, connected to an increasingly ubiquitous network infrastructure composed of a wired core and wireless edges”.

The challenges and agonies introduced by this paradigm are currently under thorough study by many academic and research institutes, as well industrial laboratories in US. A first comprehensive review on this issue has been prepared by the National Academy of Sciences [NRC-03]. More specifically, the Defense Advanced Research Projects Agency and the National Institute of Standards and Technology (NIST) invited the Computer Science and Telecommunications Board of the National Research Council to conduct a study on Ubiquitous Systems. The outcome of this effort was a report that identified agonies and opportunities for the use of UbiComp, examined the ways that these systems differ from traditional systems, and defined the most important research topics that need to be addressed, in view of the 11.09 attacks. The main aim of the report to help developing a research agenda, which could guide federal programs related to computing research, inform the research community (private sector, universities, government) about the challenging needs of this emerging research area, and propose specific actions that should be conducted in order that the UbiComp paradigm becomes a reality.

The definition of UbiComp shows that US analysts consider that the new paradigm will introduce new ways of thinking, regarding computing and communications issues and trends. In addition, analysts consider that new ways will be needed to ensure that the systems which compose the UbiComp will operate in a reliable, safely and predictably manner; that they provide their users with the necessary information about their current operating state and that they can accommodate changes in the overall system configurations or in their operating environments. Moreover, UbiComp presents new opportunities for pervasive, transparent, monitoring, and information aggregation, while at the same time it generates many challenges regarding security, privacy, and ethical issues.

Analysts argue that the characteristics of UbiComp are unique and different from current distributed systems, not only in their underlying and enabling technologies, but in their very nature, as well. They argue that, while several of the solutions and approaches of the current technology paradigm (Internet/network computing) may also apply in UbiComp, there exist new threats and vulnerabilities, which current security approaches cannot cope with effectively.

However, although the recognized advantages and benefits introduced by UbiComp paradigm, nowadays US have a significant pressure for holding their ICT leadership across the world. It is emphasized that US should have a technological boost analogous to the boost given by the first satellite being into orbit by Soviets four decades ago. The specific fact motivated a flurry of private discussions and public actions that opened a new era of national attention to US research and education in science, engineering, and technology.

US strategists argue that while the information technology-powered revolution is accelerating, US have not yet awakened to the central role played by computational science and high-

end computing in advanced scientific, social science, biomedical, and engineering research; defense and national security; and industrial innovation. Computational science has a central role in many scientific fields, ranging from network and communications to biology and infrastructure protection (Fig. 8). However, only a small fraction of the potential of computational science is being realized, thereby compromising US preeminence in science and engineering.

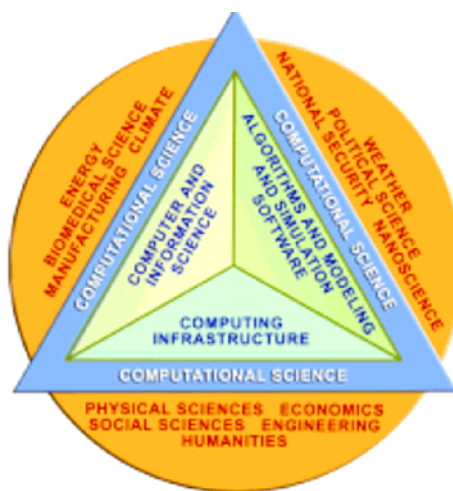


Fig. 8: Visualization of Computational Science Definition [PITAC-05a]

The aforementioned situation is enhanced from some indicators that exhibit the US competitive situation today [PITAC-05a]:

- US ICT manufacturing has declined significantly since the 70s, with the decline accelerating after 2000.
- Some of the computing systems, which are critical for US national defense and national security, have not improved substantially in a decade, and today's commercial high-end systems perform more poorly on some key metrics than older, custom-designed systems.
- US is currently producing a declining proportion of the world's scientists and engineers.
- In 2002, 58% of Science and Engineering postdoctoral positions at US universities were held by temporary visa holders.
- In 2002, only 849 PhD degrees in computer science and computer engineering awarded by US institutions; it was the lowest number since 1989 (Computing Research Association).
- Since 1988, Western Europe has produced more science and engineering journal articles than the US; the total growth in research papers is highest in East Asia (492%), followed by Japan (67%) and Europe (59%), compared with 13% for the United States.
- Worldwide, the share of US citations in scientific papers is shrinking from 38% (1988) to 31% (2001).

Therefore, the challenge for US of preserving their technological competitiveness is far more diffuse, complex, and long-term than it was 15-20 years ago. In the 21st century global economy, science and engineering capabilities of countries around the world (i.e., China) are increasingly testing US preeminence in advanced scientific R&D and in science [PITAC-05a]. Moreover, the rise of these global competitors is spurred by the very computing and networking technologies that were pioneered in the US and have been the engine of US scientific discoveries, revolutionary advances in commerce and communications, and unprecedented productivity.

In general, US analysts argue that United States led the world in developing the advanced information technologies that are transforming research, commerce, and communications. These capabilities place the notion on the threshold of revolutionary discoveries, such as in the treatment of disease, atom-by-atom construction of materials with previously unimaginable properties, miniaturization of devices down to the quantum level, and new energy sources and fuel technologies [PITAC-05a].

So, in the case of UbiComp, which introduces exciting new challenges and poses fundamental research questions US analysts expect that this new technology paradigm will fundamentally change the way in which people interact with and control their physical environment. They consider that UbiComp will have severe implications to most aspects of our society, from national defense and government applications, to wide-ranging commercial concerns to systems that private individuals will use in everyday life.

2.2 Envisioning the Emerging ICT Paradigm

US analysts recognize that ICT is on the verge of another revolution. Driven by the increasing capabilities and ever declining costs of computing and communications devices, ICT is being embedded into a growing range of physical devices linked together through networks and will become ever more pervasive, as the underlying technology components become more smaller, faster and cheaper. These networked systems of embedded computers, which are referred as Ambient Intelligence or Ubiquitous Computing, have the potential to change dramatically the way people interact with their environment. On the other hand, the range of applications continues to expand, while offering new and more sophisticated end user services.

Realizing the great promise of UbiComp requires more than only the advance of individual technologies. It also requires holistic perspective, including technologies as well as societal issues and it will rely on numerous subsystems working together in an efficient, unattended, comprehensible, and trustworthy manner. Many aspects of the needed research are highly interdisciplinary because of the complicated ways in which UbiComp systems interact with the physical world. In the absence of programs aimed at solving some of the basic research problems, it is likely that many of the benefits of UbiComp will simply not be realized.

Therefore, US analysts argue that meeting the challenges posed by UbiComp paradigm will require to dramatically extending the frontiers of knowledge in science and engineering. But they also require thinking more coherently about the proper role for business and government, the development of public/private partnerships, and the reconciliation of different priorities and points of view. The definitions of specific and clear policies on such issues will help to realize the full promise that UbiComp can deliver. In this context, the key areas of research [NRC-03] that will help US to achieve the full potential of UbiComp are referred to in the sequel.

Self configuration and Adaptive Coordination. Given the expected pervasive nature of UbiComp, it will be necessary for these systems to be able to configure themselves and adapt to their environments in an automate and dynamic way. Self-configuration and adaptive coordination comprise a set of changes that a system makes to itself in response to occurrences both internal to it and external. Current work in distributed systems has not solved this problem. Especially due to many constraints introduced by the UbiComp paradigm, this problem becomes more difficult to solve. Research issues related to service discovery include the scaling of discovery protocols, security, and the development of adequate failure models for automatically configured networks. Adaptive coordination involves changes in the behaviour of a system as it responds to changes in the environment or system resources. To obtain neces-

sary adaptability in UbiComp, research is needed in three areas: (a) exploiting massive redundancy to achieve system robustness and longevity, (b) decentralized control, and (c) collaborative processing.

Building Trustworthy UbiComp Systems. UbiComp will be deployed in large number and will become a part of the fabric of everyday life. Therefore, its success and the degree of its acceptance will depend on how much trustworthy these systems are. The most important issues regarding trustworthiness of UbiComp are reliability, safety, security, privacy, and usability. Reliability is the quality of a system that is satisfying its behavioural specifications under a given set of conditions and within defined time periods. Current techniques are not readily applicable to UbiComp because of the large number of elements, highly distributed nature, and environmental dynamics. Research is needed on fault models and recovery techniques for UbiComp, monitoring and performance-checking techniques, and verification tools and approaches. Safety refers to the ability of a system to operate without causing an accident or unacceptable loss. It is distinct from reliability and poses another set of research problems for UbiComp. UbiComp increase the number of possible behaviours and the complexity of the possible interactions within the system. Further, UbiComp systems operate in real time and with limited human intervention and are likely to exhibit emergent or unintended behaviours. Several safety topics deserve further research effort, including hazard analysis for UbiComp, validating requirements, designing for and verifying safety, and ensuring safety in upgraded hardware. The networking of embedded devices (e.g. sensors and actuators) will greatly increase the number of possible points of failure, making security analysis even more difficult. Defining and then protecting system boundaries where physical boundaries are likely to be nonexistent and where nodes can automatically move in and out of the system will be a serious challenge. UbiComp will be able to gather more information than current systems and will do so in a much more passive manner. Achieving consensus on privacy and confidentiality policies will be exacerbated by the pervasiveness and interconnectedness of UbiComp systems. Determining how to handle the vast amounts of personal information that will be collected is a large area for research. UbiComp will need to be usable by persons with little or no formal training. Unfortunately, usability and safety often conflict, and decisions on trade-offs will need to be made. Understanding the way people create mental models of the systems they use and interact with is a good way for designers to begin to address the issues of usability and manageability. In particular, more research is needed in designing for a range of persons and in enhancing mental models and user training.

Models of Computation. New models of computation are needed to describe, understand, construct, and reason about UbiComp effectively. UbiComp tight coupling to the physical world, the heterogeneity of its underlying components, the multitude of elements, and timing and resource constraints, among other things, exhibit the need for a much richer computing model. Computational models for UbiComp will need to incorporate resource constraints, failures, new data models, trust, concurrency, and location.

Enabling Technologies. The development and deployment of UbiComp systems will be supported in general by advances in the enabling information technologies. In this context research is needed on specific aspects of communications, geolocation, software and operating systems, and MEMS. Work is needed to understand how to create network architectures and designs for low-power, short-range wireless systems. Many UbiComp systems will therefore require ready access to absolute or relative geographic information. New methods of software development may be needed in order to ensure that complex UbiComp software is up to coping with the constraints placed on it.

Although the aforementioned research challenges present problems that are already in the focus of research, in addition they set goals that move far beyond what has been demonstrated by today's research. In most cases, it is precisely the scale of the vision of UbiComp that makes them challenging. Each challenge requires at least many years of concentrated research in order to make substantive progress. Each is deserving of considerable investment by government and private sector because each challenge, if successfully fulfilled, will materially improve the capabilities and the civilized conduct of society.

It is worthwhile remembering that while individual components may be elegantly and effectively modelled by mathematics, complex systems that serve society are inherently messy. They must adapt to human habits and procedures, understand verbal and nonverbal cues, and present an interface that seems intuitive to human users, among other criteria [CRA-02]. In other words, they must be efficient for human use, even if not computationally efficient. Accordingly, these research challenges require the collaboration of experts from many fields in a generalizing research framework that provides an overriding context for coordinating and motivating this needed research effort.

2.3 Cornerstones and Strategic Planning

The characteristic of human beings to find solutions to challenges go far beyond just mere intellectual curiosity. It is embedded in humanity's very nature to conquer new frontiers for social, economic, and political advancement. Information technology has an important role in conquering these frontiers. Recognizing this role, analysts argue that the US Government makes critical decisions about appropriate investments in ICT R&D to help society forward both socially and economically. For this reason specific committees have been organized in order to recognize the challenges that should be addressed in order the US nation to preserve its leadership in ICT domain. While keeping the longer-term grand challenge in perspective, certain aspects of the challenge have been identified for focused attention in the next ten years. Some of these focus areas were selected because they are particularly difficult and need to be handled right away. For others, the knowledge and resources needed to address them are available today. Focus on these component challenges in the near term helps sustain focus on the longer-term grand challenge.

The recognized challenges can generate a vast array of social, economic, political, scientific, and technology benefits as their solutions are found. Common threads permeating these benefits include finding answers to complex questions that have long perplexed humanity, creating new disciplines of human inquiry and areas of multidisciplinary collaboration, and developing and using new technologies. The list of challenges that should be solved according to Networking and Information Technology R&D (NITRD) are [NITRD-04]:

- Knowledge Environments for Science and Engineering
- Clean Energy Production Through Improved Combustion
- High Confidence Infrastructure Control Systems
- Improved Patient Safety and Health Quality
- Informed Strategic Planning for Long-Term Regional Climate Change
- Nanoscale S&T: Explore and Exploit the Behaviour of Ensembles of Atoms and Molecules
- Predicting Pathways and Health Effects of Pollutants
- Real-Time Detection, Assessment, and Response to Natural or Man-Made Threats
- Safer, More Secure, More Efficient, Higher-Capacity, Multi-Modal Transportation System

- Participation in a Digital Society
- Collaborative Intelligence: Integrating Humans with Intelligent Technologies
- Generating Insights From Information at Your Fingertips
- Managing Knowledge-Intensive Dynamic Systems
- Rapidly Acquiring Proficiency in Natural Language
- SimUniverse: Learning by Exploring
- Virtual Lifetime Tutor for All

ILLUSTRATIVE GRAND CHALLENGES	NATIONAL PRIORITIES					
	LEADERSHIP IN SCIENCE AND TECHNOLOGY	NATIONAL AND ECONOMIC SECURITY	HEALTH AND ENVIRONMENT	ECONOMIC PROSPERITY	A WELL-EDUCATED POPULATION	A VIBRANT CIVIL SOCIETY
Knowledge Environments for Science and Engineering						
Clean Energy Production Through Improved Combustion						
High Confidence Infrastructure Control Systems						
Improved Patient Safety and Health Quality						
Informed Strategic Planning for Long-Term Regional Climate Change						
Nanoscale Science and Technology: Explore and Exploit the Behavior of Ensembles of Atoms and Molecules						
Predicting Pathways and Health Effects of Pollutants						
Real-Time Detection, Assessment, and Response to Natural or Man-Made Threats						
Safer, More Secure, More Efficient, Higher-Capacity Multi-Modal Transportation System						
Anticipate Consequences of Universal Participation in a Digital Society						
Collaborative Intelligence: Integrating Humans with Intelligent Technologies						
Generating Insights From Information at Your Fingertips						
Managing Knowledge-Intensive Organizations in Dynamic Environments						
Rapidly Acquiring Proficiency in Natural Languages						
SimUniverse: Learning by Exploring						
Virtual Lifetime Tutor for All						

Table 2: Grand Challenges and US National Priorities relationships [NITRD-04]

The aforementioned challenges are in strong relationship with the US national priorities that reflect the country’s broad-based scientific, military, social, economic, and political values and goals. Each of the grand challenges strongly contributes to one or more of these national priorities [NITRD-04]: a) Leadership in Science and Technology, b) Homeland and National Security, c) Health and Environment, d) Economic Prosperity, e) A Well-Educated Populace, and f) A Vibrant Civil Society. Table 2 depicts how the aforementioned grand challenges are correlated with the US national priorities and goals.

ILLUSTRATIVE GRAND CHALLENGES	IT HARD PROBLEM AREAS													
	ALGORITHMS AND APPLICATIONS	COMPLEX HETEROGENEOUS SYSTEMS	HANDHELD TECHNOLOGIES	HIGH CAPABILITY HIGH CONFORMANCE IT	HIGH-END COMPUTING IT	HUMAN-COMPUTING SYSTEMS	INFORMATION TECHNOLOGY INNOVATION	INFORMATION MANAGEMENT	INTELLIGENT SYSTEMS	IT SYSTEM DESIGN	IT USABILITY	IT WORKFORCE	MANAGEMENT OF IT NETWORKS	SOFTWARE TECHNOLOGIES
Knowledge Environments for Science and Engineering														
Clean Energy Production Through Improved Combustion														
High Confidence Infrastructure Control Systems														
Improved Patient Safety and Health Quality														
Informed Strategic Planning for Long-Term Regional Climate Change														
Nanoscale Science and Technology: Explore and Exploit the Behavior of Ensembles of Atoms and Molecules														
Predicting Pathways and Health Effects of Pollutants														
Real-Time Detection, Assessment, and Response to Natural or Man-Made Threats														
Safer, More Secure, More Efficient, Higher-Capacity Multi-Modal Transportation System														
Anticipate Consequences of Universal Participation in a Digital Society														
Collaborative Intelligence: Integrating Humans with Intelligent Technologies														
Generating Insights From Information at Your Fingertips														
Managing Knowledge-Intensive Organizations in Dynamic Environments														
Rapidly Acquiring Proficiency in Natural Languages														
SimUniverse: Learning by Exploring														
Virtual Lifetime Tutor for All														

Table 3: Relationships between the Grand Challenges and IT hard problems [NITRD-04]

Furthermore, in order the aforementioned grand challenges to be efficiently addressed many technological issues should be examined. The NITRD task force identified several ICT hard

problems, which might influence the satisfaction of Grand Challenges [NITRD-04]. These problems are: Algorithms and Applications, Complex Heterogeneous Systems, Hardware Technologies, High Confidence, High-End Computing Systems, Human Augmentation, Information Management, Intelligent Systems, System Design, Usability, Workforce, Management of IT, Networks and Software Technologies. Table 3 summarizes the relationships between grand challenges and ICT hard problems.

Besides, the general open issues regarding US grand challenges, there are also many open issues regarding Ubiquitous Computing paradigm in the US nation. Analysts believe that an important step towards ensuring US competitiveness advantage is how the research regarding UbiComp is organized and conducted [NRC-03]. They underline that it is unlikely that such a broad-based and widely applicable research effort will be undertaken by industry alone. The note that, while systems can be built individually, the accumulated understanding will be insufficient without fundamental work promoted and supported by federal funding agencies and organizations. They argue that long-term, forward-thinking, and broad-ranging research programs are crucial to achieve a deep understanding of UbiComp impacts on society, as well as of how to design and develop the new ICT technologies and systems. More specifically, according to PITAC, US must come to grips with both the broad science and technology challenge they face and the reality that the 21st century scientific and engineering enterprise is computational and multidisciplinary, requiring the collaborative scientific skills of diverse disciplines [PITAC-05a].

Abstractly, the most important research challenges introduced by UbiComp were identified to be [NRC-03]:

- *Predictability and manageability.* Methodologies and mechanisms for designing predictable, safe, reliable, manageable UbiComp systems.
- *Adaptive self-configuration.* Techniques to allow adaptive self-configuration of UbiComp in order to respond dynamically to environmental changes and participating (underlying) system resources.
- *Monitoring and system health.* A complete conceptual framework to help achieve robust operation through self-monitoring, continuous self-testing, and reporting of system health in the face of extreme constraints on nodes and elements of the system.
- *Computational models.* New abstractions and computational models for designing, analyzing, and describing the collective behavior and information organization of massive UbiComp systems.
- *Network geometry.* Ways to support and incorporate network geometry (as opposed to just network topology) into UbiComp environments.
- *Interoperability.* Techniques and design methods for constructing long-lived, heterogeneous systems that evolve over time and space while remaining interoperable.
- *Integration of technical, social, ethical, and public policy issues.* Fundamental research into the non-technical issues of UbiComp, especially those having to do with the ethical and public policy issues surrounding privacy, security, reliability, usability, and safety.
- *Enabling technologies.* Ongoing research into the various component and enabling technologies of UbiComp.

Fig. 9 depicts schematically the research issues that should be fulfilled because of the transition and shift to the UbiComp paradigm.

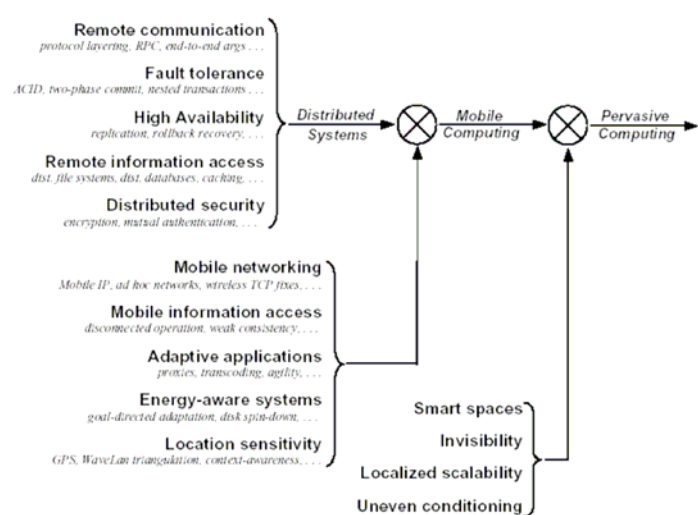


Fig. 9: Transition to UbiComp - Challenges introduced [Sat-01]

In general, according to many analysts ensuring that the right kinds of research are conducted to advance the state of the art in UbiComp will require changes in the way the nation's research is organized. Academia and industry will both have important roles to play. Effective collaboration will be needed not only among industry, universities, and government, but also between IT researchers and researchers in other areas. Explicit efforts will need to be made to put mechanisms in place for ensuring such collaboration. While past attempts to achieve similar goals met with mixed results, the pressing needs of UbiComp demand redoubled efforts, drawing upon the lessons of history.

Mechanisms will be needed, also, to promote interdisciplinary approaches to research on UbiComp, which tie computer science to other sciences and other disciplines in general. Domain expertise found in disciplines such as Biology, Geophysics, Chemistry, and Medicine will allow the application of UbiComp in a variety of areas. These disciplines and others can provide models that couple the world of the networked computer and the physical world and can help in investigations of the wider implications of UbiComp society.

On the other hand, the federal government has long been a strong supporter of broad ranging research in IT domain through specific funding programs. Such funding, in general, can cause industry to take a broader perspective and produce more flexible technology for users in the federal government and elsewhere than it would if left strictly to market forces. More specifically, in the next paragraphs we present the specific actions that should be adopted by two grand research organizations in Unites States, DARPA and NIST respectively [NRC-03].

DARPA has already invested in UbiComp-related technologies, but it has only scratched the surface of what will be necessary to advance this critical technology. Publicly funded research is needed to drive innovation that is of sufficient scope and addresses externalities such as interoperability, safety, and upgradeability. The development of robust UbiComp technology will require the research community to rethink the fundamentals of information technology and the design of computer and communications systems. Therefore, DARPA is advised to aggressively pursue multiple programs that build upon and interact with one another and with some of the seed programs that have already begun to explore related areas. To truly harness the power of UbiComp systems, DARPA should manage these programs in a way that fosters their interaction and creates and builds on conceptual overlaps.

On the other hand, NIST is in an excellent position to foster interaction by devising the appropriate metrics for measuring the effectiveness of UbiComp elements as well as the requi-

rements for performance and quality of service for the more abstract services that will be built upon those elements. In addition to metrics, NIST can also act as a collector of and repository for experimental data. There is a growing gap in access to critical evaluation data. Many analysts believe that NIST also has a particularly critical role to play in this realm as the agency that establishes confidence in information systems. NIST is seen as an outside observer that can provide objective services and analysis. It has an important role in the standards development process, allowing the work done in industry to be illuminated in a fair and open fashion.

2.4 Security and Privacy Strategies

After 11.09, US analysts recognize that for the national economy - particularly its information technology industry component - the dearth of trusted, reliable, secure information systems presents a barrier to future growth (Fig. 10 depicts the US framework regarding Homeland Security). Much of the potential for economic growth made possible by the information technology revolution has yet to be realized - deterred in part by cyberspace security risks. Cyberspace vulnerabilities place more than transactions at risk; they jeopardize intellectual property, business operations, infrastructure services, and consumer trust. As US take steps to improve the security of current systems, it should also ensure that future cyber-systems and infrastructure are built to be secure. This will become more important, as more and more of US citizens' daily economic and physical lives come to depend on cyber-infrastructure.

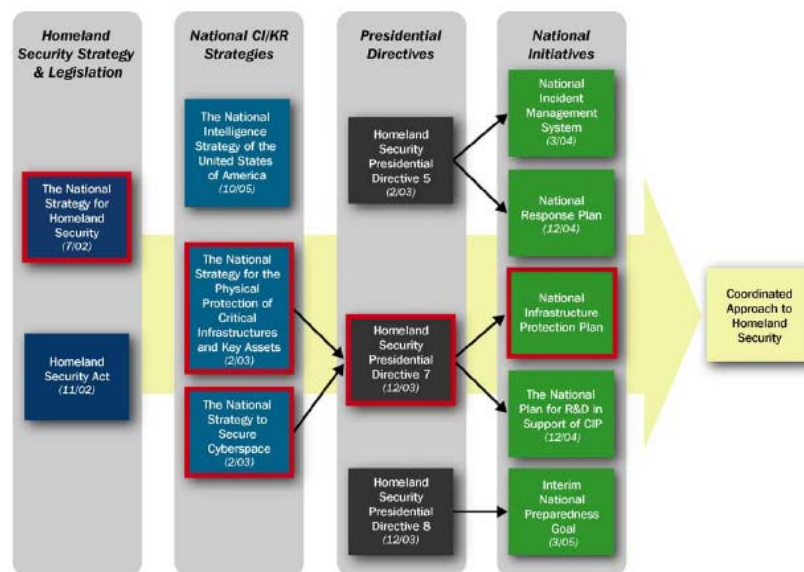


Fig. 10: US Framework Regarding Homeland Security [DHS-06]

According to reports published by several federal committees, the US IT infrastructure is highly vulnerable to deliberate attacks with potentially disastrous effects. The IT infrastructure encompasses not only the best-known uses of the public Internet - e-commerce, communication and Web services - but also the less visible systems and connections of US critical infrastructures such as power grids, air traffic control systems, financial systems, and military and intelligence systems. The growing dependence of these critical infrastructures on the IT infrastructure means that the former cannot be secure if the latter is not (Fig. 11).

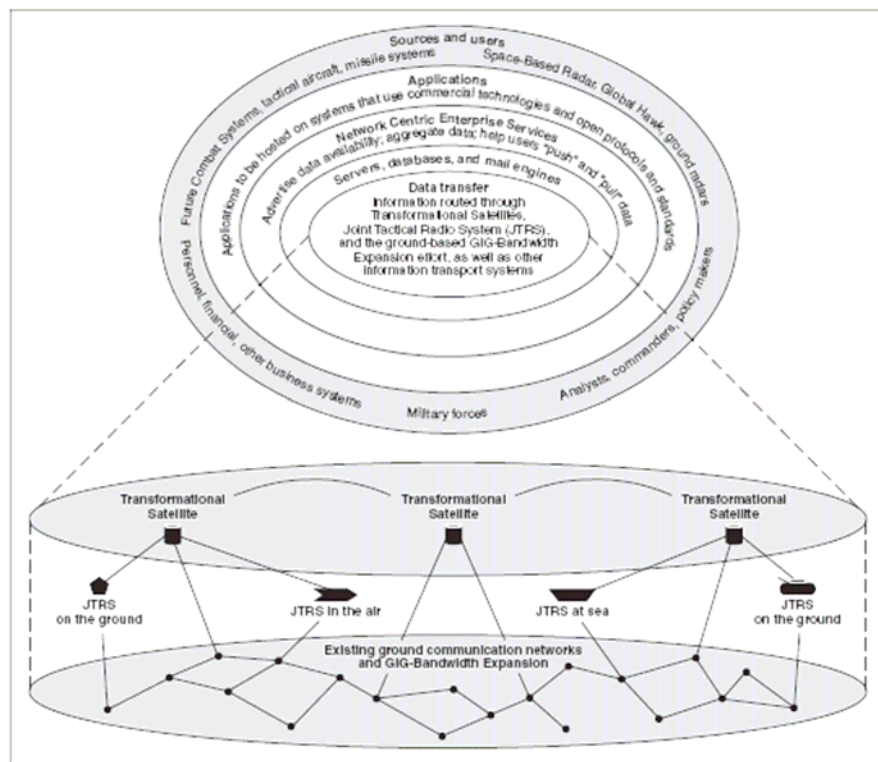


Fig. 11: Technologies composing ICT infrastructure and their relationships

Beyond economic effects, the risks to US nation's security are described as clear. In addition to the potential for attacks on critical targets within US borders, the national defence systems are at risk as well, because the military increasingly relies on ubiquitous communication and the networks that support it. The Global Information Grid, which is projected to cost \$100 billion and is intended to improve military communications by linking weapons, intelligence, and military personnel to each other, represents one such critical network [GAO-04]. Since military networks interconnect with those in the civilian sector or use similar hardware or software, they are susceptible to any vulnerability in these other networks or technologies. Thus cyber security in the civilian and military sectors is intrinsically linked.

Analysts suggest that the main findings, regarding US cyber security, which highlight the need to adopt new approaches for secure their nation, are:

- The federal R&D budget provides inadequate funding for fundamental research in civilian cyber security.
- The nation's cyber-security research community is too small to efficiently support the cyber-security research and education programs.
- Current cyber-security technology transfer efforts are not adequate to successfully transition federal research investments into civilian sector best practices and products.
- The overall federal cyber-security R&D effort is currently unfocused and inefficient because of inadequate coordination and oversight.

Therefore, US strategists argue that US need to expand their focus on short-term patching to also include longer-term development of new methods for designing and engineering secure systems. Addressing cyber-security for the longer term requires a dynamic ongoing program of fundamental research to explore the science and develop the technologies necessary to design security into computing and networking systems and software from the ground up. Fun-

damental research is characterized by its potential for broad application and includes farsighted, high-payoff research that provides the basis for technological progress.

Besides the technological issues regarding US national security, there are social, as well as ethical issues, which should also be considered. The other facets of cyber-security, which are considered to require societal attention include:

- *Domestic and international law enforcement.* A hostile party using an Internet-connected computer thousands of miles away can attack an Internet connected computer in the US as easily as if he or she were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.
- *Education.* US analysts argue that they need to educate citizens that if they are going to use the Internet, they need to continually maintain and update the security on their systems so that they cannot be compromised. They, also, need to educate corporations and organizations in best practices for effective security management.
- *Information security.* Information security refers to measures taken to protect or preserve information on a network as well as the network itself. Thus it also involves physical security, personnel security, criminal law and investigation, economics, and other issues. These factors need to be included in the curriculum for cyber security practitioners, and supporting law and technologies need to be made available.
- *Sociological issues.* There are several areas relating to cyber security in which there may be conflicting interests and needs, and such tensions will need to be addressed as part on any comprehensive approach to cyber security. Such areas involve ethics, law, and societal concerns as much as they do technology and these non-technology issues make the cyber security problem even more challenging.

The above security issues are key challenges in the case of the UbiComp paradigm as well. More specifically, in open and uncontrolled environments such as UbiComp, crammed with devices and objects that may invisibly sense and collect private and sensitive information and invisibly communicate with other systems, the issue of security and privacy is of obviously major importance. In general, this ubiquitous interconnectivity provides the primary conduit for exploiting vulnerabilities on a widespread basis. So far, despite the efforts, the existing security and privacy protection technologies are not sufficient or appropriate in order to fulfil the unique security and privacy requirements of UbiComp.

The analysts consider that purely technical approaches will be insufficient for the protection of privacy and security. They suggest that policy and technical aspects should be also coordinated, in order to address the problems appearing in UbiComp environments. They stress the point that privacy, security, and ethical considerations need to be considered and incorporated early, i.e. during the design and development phases of these systems. These are areas in which inter- and multidisciplinary research efforts could pay large dividends. Furthermore, the ethical concerns related to security and privacy - which drive legal and policy activity - require a fundamental research agenda. Some of that research will relate to technical mechanisms that can help to ensure authenticated use and proper accountability, while safeguarding privacy. Perhaps more importantly, it may be necessary to develop a new calculus of privacy to be able to evaluate how interactions between new elements (e.g. objects-to-objects) will impinge on security and privacy. As a result, research strategists suggest that security refers strongly to controlled access to the sub-networks, the information stores, the devices that are interconnected, and the computing and communication resources of a given network. In heterogeneous, diffuse, fluid networks, traditional network security methods will not be effective.

Rather, trust management and security policies and methods will be the responsibility of individual nodes and applications. In this context the most important security research topics, according to US strategists, are: (a) the definition of specific and standard based network access policies and controls, (b) the definition and the enforcement of specific security policies, (c) critical infrastructure self-defence, and (d) energy scarcity.

In the case of privacy protection, strategists recognize that consideration of the privacy implications of UbiComp cannot be limited to these systems alone, but must extend to the larger networks of more powerful computers to which UbiComp systems connect. A related issue that will need to be resolved is how (and sometimes whether) to advise people when their actions are being monitored. As a result, many privacy questions will need to be rethought in a world of increasing automation and instantaneous wireless communication. Both privacy expectations and case law are evolving and it will be necessary to clearly understand the trade-offs involved. UbiComp has more of a propensity to be ubiquitous and enveloping, unavoidable in our environment, where individuals are not in control of their interaction. In these cases, privacy issues cannot be addressed by education and personal policies alone. Rather, they become (even more) a matter of public policy. In this context, the most important research topics regarding privacy protection are: (a) the development of a calculus of privacy and the definitions of specific ways to enable flexible, configurable privacy policies in systems, so that as external situations or policies change, the system can be easily adjusted to reflect that, (b) the implementation of specific techniques in terms of informed consent about the privacy issues, (c) research into possible legal requirements for the protection of personal information in order to ensure adequate accountability, and (d) the development of specific anonymity mechanisms that should protect users' identities through appropriate identity management procedures. What is actually needed is a technology that supports a range of preferences, which may vary with users and contexts, and enhances privacy, accountability, and other values and assets.

Emerging areas of research on other domains can also produce unforeseen consequences for security. The US strategists argue that US must be at the leading edge in understanding these technologies and their implications for security. In this context the guiding principles regarding security and privacy in the US should include and focus on: (a) A national effort, i.e. protecting the widely distributed assets of cyberspace requires the efforts of many Americans, (b) protect privacy and civil liberties, i.e. avoid the abuse of cyberspace infringes on citizens privacy and liberty. Analysts argue that it is incumbent on the federal government to avoid such abuse and infringement. Cyber-security and personal privacy need not be opposing goals. The federal government will lead by example in implementing strong privacy policies and practices in the agencies. As part of this process, the federal government will consult regularly with privacy advocates and experts, (c) regulation and market forces, i.e. the market itself is expected to provide the major impetus to improve cyber-security, (d) accountability and responsibility, (e) ensure flexibility, and (f) multi-year planning.

Another relevant and important issue, regarding UbiComp and its underlying technologies in the US, is safety and reliability. This dimension of UbiComp, which is not considered as such an important issue in the case of neither Europe nor Japan, refers to the ability of the systems to operate without causing an accident or an unacceptable loss. Safety constraints need to be identified early on in the design process so that the system can be designed to satisfy them. Testing and measurement simply provide assurance on how effectively the design incorporates already-specified safety considerations. The process involves identifying system hazards, using them as the basis for writing system safety requirements and constraints, designing the system to eliminate the hazards and their effects, tracing any residual safety-related requirements and constraints that cannot be eliminated at the system level down to re-

quirements and constraints on the behavior of individual system components (including software), and verifying that the efforts were successful. In the case of UbiComp, its technology components introduce added difficulties to the aforementioned. UbiComp complicate the process of error reduction simply because of their increased complexity and the opacity of system design and operation. In this context important research topics regarding safety are: (a) safety must be designed into a system, including the human-computer interface and interaction, (b) the deficiencies in existing hazard analysis techniques when applied to UbiComp need to be identified, (c) designers of UbiComp systems who may not necessarily be familiar with such techniques will need to understand them, (d) improved specification and analysis techniques are needed to deal with the challenges posed by UbiComp and take into account that user needs and therefore specifications will evolve, and (e) ensuring safety in upgraded software even if the software is designed and assured to be safe in the original system context.

Another important prerequisite, regarding security and privacy issues in the US, is that there must be a strong and viable relationship between government and private sector. This relationship should be bi-directional and efficient in terms of information sharing. The information sharing can enable government and private sector to accurately assess events, formulate risk assessments, and determine appropriate actions. Fig. 12 presents an example of how this information sharing is suggested to take place [DHS-06].

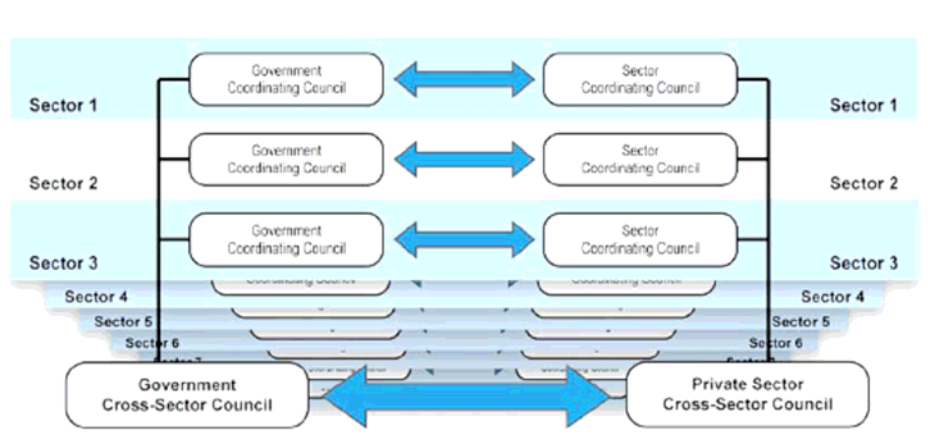


Fig. 12: Security-related information sharing in the US [DHS-06]

Concluding, the ICT infrastructure in the US, which is vital for communication, commerce, and control of US physical infrastructure, is highly vulnerable to terrorist and criminal attacks. In this respect, strategists consider that the private sector has an important role in securing the nation's IT infrastructure by deploying sound security products and adopting good security practices. But the federal government has also a key role to play by supporting the discovery and development of cyber-security technologies that underpin these products and practices. Therefore, the most important actions for the near future, regarding the protection of US cyber-security, are considered to be:

- Increase federal support for fundamental research in civilian cyber security by 90B\$ annually at NSF and by substantial amounts at agencies such as DARPA and DHS
- Intensify federal efforts to promote recruitment and retention of cyber security researchers and students at research universities, with an aim of doubling this profession's numbers by the end of the decade.
- Provide increased support for the rapid transfer of federally developed cutting-edge cyber-security technologies to the private sector.

- Strengthen the coordination of the Interagency Working Group on Critical Information Infrastructure Protection and integrate it under the Networking and Information Technology Research and Development (NITRD) Program.

3 JAPAN

3.1 Agonies and Trends

The competitiveness and strength of specific Japanese industries (automobiles and home appliances) is being lost due to the progress of globalisation in the 90's. Analysts consider that if no measures are taken, the advanced component and material industrial cluster, that is now competitive in Japan, may also be lost. For Japan, the 90's were a kind of a lost decade, in which Japanese companies were cleaning up the mess, after the asset boom of the 80's turned to bust. At the end of the 90's, Japanese companies were reported to be a few years behind the US companies, which have established a formidable lead in the ICT field. In particular, Japanese companies had some catching up to do in the field of network computing, especially as it relates to Internet and e-commerce [Fuj-00].

Under the circumstances, Japan industries turned to focus at developing strategic superiority in terms of "being different" rather than "being fast". The underlying approach of the Japanese strategists was to make Japan's own ICT "paradigm" different than that of any other country. During the 90's Sakamura (Univ. of Tokyo) advocated a new concept, a potential basis for a new ICT paradigm, which he called "computer anywhere". Japanese analysts considered that this concept could actually give birth to the new ICT paradigm in Japan, which they call the Ubiquitous Network (UbiNet). The term ubiquitous have been used in the ICT field after Weiser (Zerox Palo Alto Research Centre) advocated a concept called "Ubiquitous Computing" (UbiComp) (see Fig. 13) [Mur-03, Mur-05, Wie-91, Wie-93a, Wie-93b].

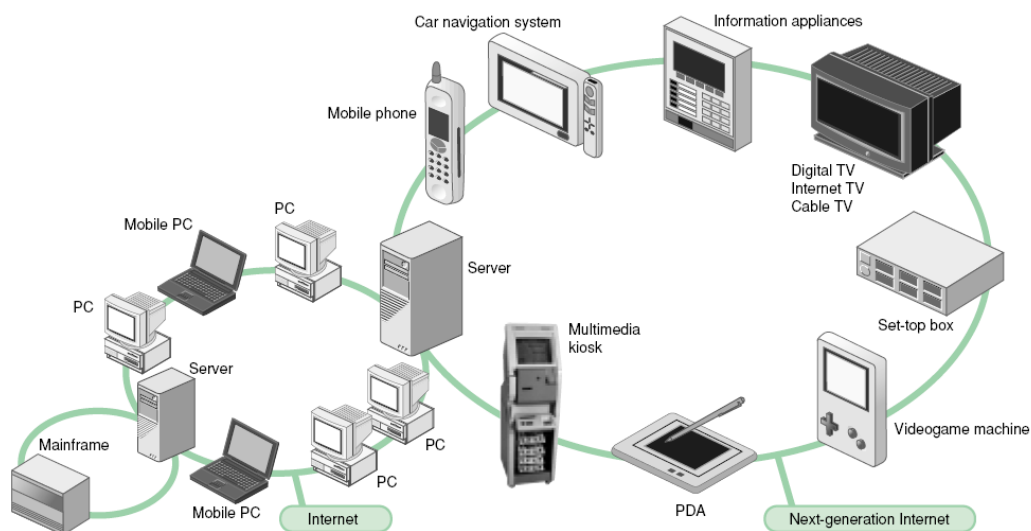


Fig. 13: Ubiquitous Computing [Mur-00]

Terminologically speaking, the term "ubiquitous computing" originated in the US, while the term "ubiquitous network" was given birth in Japan, where more than one alternative to this term is officially used. For example, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) called it the "ubiquitous network"; the Ministry of Economy, Trade and Industry (METI) pursued the "ubiquitous information society"; the Ministry of Land, Infrastructure and Transport (MLIT) called it a "ubiquitous information network" and the Ministry of Education, Culture, Sports, Science and Technology (MEXT) named it "ubiquitous computing".

The situation in Japan, regarding the UbiNet, could be abstractly seen as a kind of a short term race, or agony, to transform Japan into a “ubiquitous island”, in just the same way as Silicon Valley received its name in the era of network computing [Fuj-00]. The agony was visible when Japanese strategists commented upon newspapers articles (Wall Street Journal, Jan. 2004) on the UbiComp boom in Japan, reporting that “the Japanese are again immersed in gadgetry” [Mur-04]. Furthermore, strategists’ agony was also visible in their trend to differentiate UbiComp and UbiNet, underlining that “the ubiquitous network is an ICT paradigm that was rediscovered in Japan, i.e. Japan did not imported the technologies born in the US called ubiquitous computing” [Mur-04].

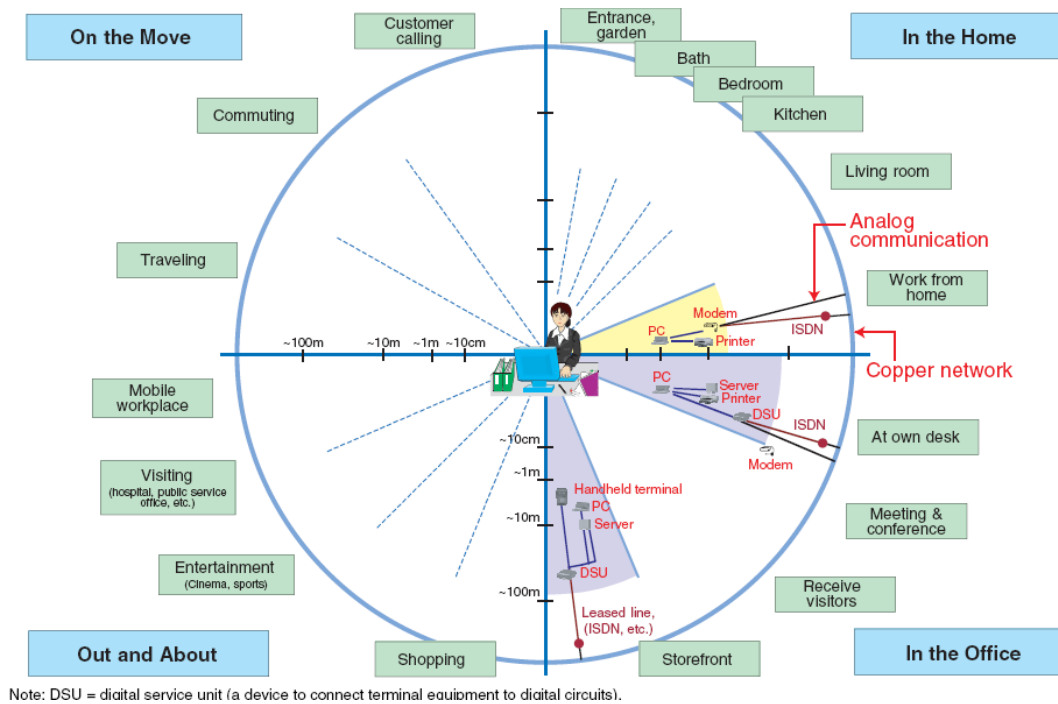


Fig. 14: Network Computing [Mur-04]

Provided that US companies are clearly ahead in the ICT field, Japanese strategists believe that if they: (a) transfer the competition to a new paradigm, i.e., from the network computing (Fig. 14) to the ubiquitous network (Fig. 15), (b) make the most of their own know-how, and (c) create a new ubiquitous industry, this would probably stand a better chance of catching up with and overtaking their US rivals. Their plans are also based on their belief that “consumers in Japan probably have the most sophisticated and mature consumption behaviour in the world, with respect to digital information equipment” [Fuj-00].

In Japan, it is believed that progress in shifting only towards modern network technologies (i.e., broadband) may establish this country as the leading broadband nation, but this will not necessarily make Japan the leading ICT nation. In order to do so, Japan needs new strategies capable of leading Japanese industries to comprehensive innovation throughout an entirely new ICT paradigm. Concluding, the focus is on ensuring Japan’s industrial lead through the establishment of “the world’s (a) first, (b) only, and (c) best ICT environment, an environment allowing industries to connect to consumers anywhere and at any time via broadband networks” [Mur-03].

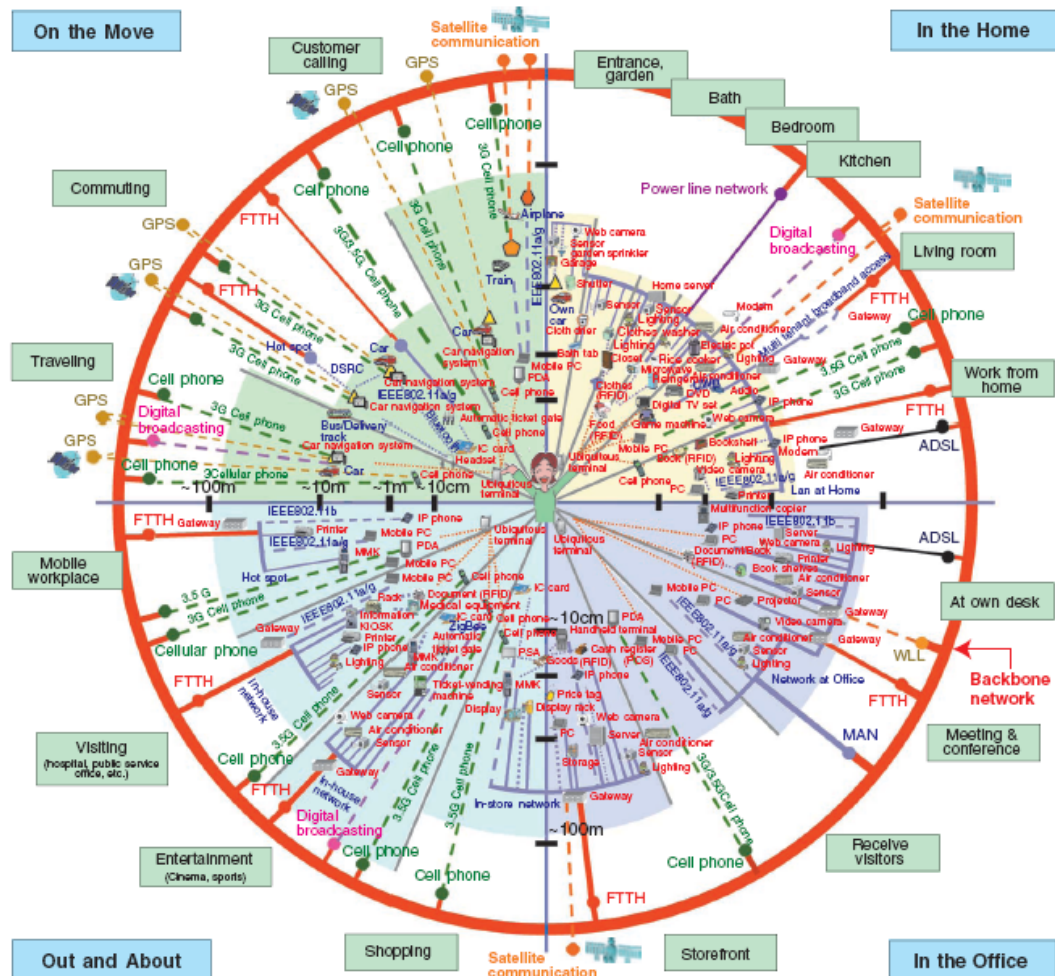


Fig. 15: Ubiquitous Network [Mur-04]

3.2 Envisioning the Emerging ICT Paradigm

Weiser was the one who advocated UbiComp as a new computing paradigm, consisting of context-aware concepts (i.e. the system itself can make a decision based on the circumstances), in which computing capabilities are incorporated everywhere and are linked to automatically generate an optimal status. UbiComp relies not only on devices to be developed (i.e., paper computers and wearable computers, envisioned by MIT Media Lab, etc.), but also on existing ones (i.e., mobile telephones, multimedia kiosks, videogame machines, digital TV, car navigation systems, information appliances, etc.). All these devices will be linked to a network that will include wireless communications and broadcasting and offer greater bandwidth than the public telephone lines and trunk lines on which the Internet currently depends. UbiComp has added a new dimension to the world of ICT: From anytime, any place connectivity for anyone, we will now have connectivity for anything (Fig. 16) [ITU-05]. In this respect, the three operational stages in the use of computing are: (a) Mainframes: One computer - many people, (b) Personal computers: One person - one computer, and (c) UbiComp: One person - many computers.

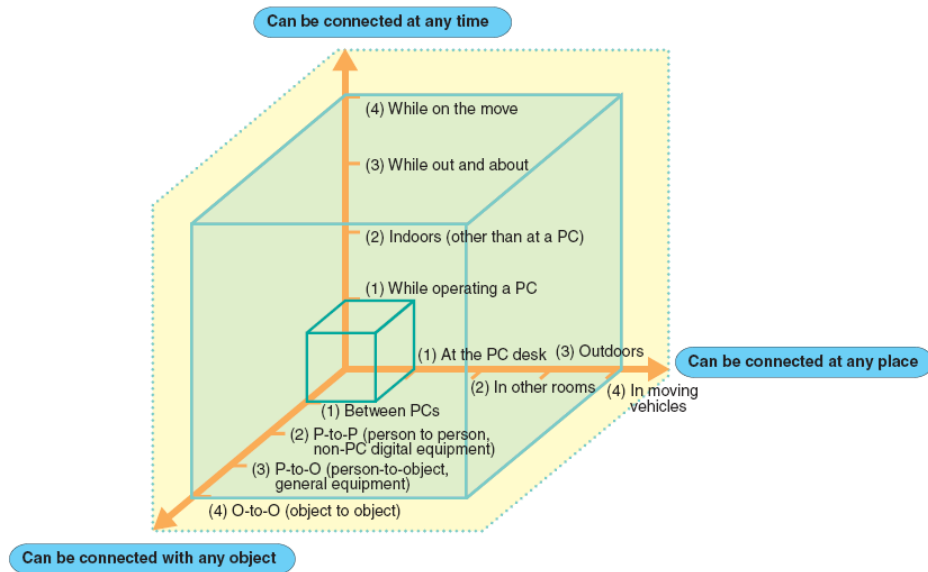


Fig. 16: A new ICT paradigm and its new dimension [ITU-05]

UbiNet is the Japan's term for the new ICT paradigm. The UbiNet is something that pursues the ubiquity of network connections, not the ubiquity of computing capabilities. Furthermore, the UbiNet positions the user at the centre of the ICT environment. From this viewpoint, network-enabled connections appear in three types: Person-to-Person (P2P), Person-to-Object (P2O) and Object-to-Object (O2O). The notion of O2O gave birth the concept of the "Internet of Things", which in turn leads to a new market (Fig. 17) [ITU-05].

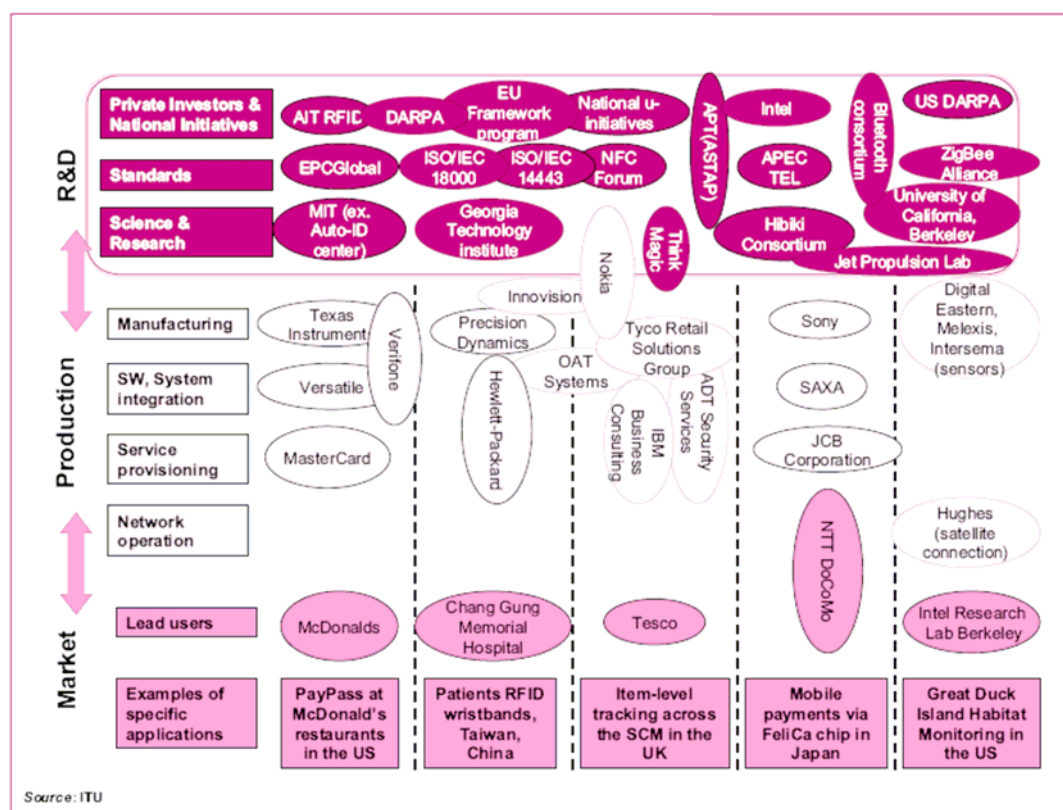


Fig. 17: The Internet of Things: From idea to market

The user sees the UbiNet as an ICT usage environment that provides access to a broadband network from literally everywhere. For the user, the UbiNet would provide constant access. On the UbiNet, the user could handle all types of content. For the supplier the UbiNet is an ICT environment that meets the following requirements [ITU-05, Mur-03]:

- (a) it provides broadband network access with the mobility to allow for always-on connections, regardless of the place of usage, and incorporating such models, as fixed, mobile, wired, and wireless systems, or communications and broadcasting,
- (b) it allows for connecting not only large-scale general-purpose computers and PC, but also mobile phones, PDA, game machines, car navigation systems, digital TVs, home information appliances, web cameras, RFID¹ tags, and other information equipment and sensors to this network, via IP and similar protocols,
- (c) it enables the utilization of content that involves not only text, data, and still images, but also the transmission of animated images and sound, as well as the utilization of platforms that enable secure exchanges of information and the implementation of commercial transactions.

For Japanese strategists, the UbiNet is - as the Internet also is - a single integrated ICT paradigm that covers a full range of key elements from network infrastructure, digital equipment with communication capabilities and digital platforms, to solutions. UbiNet represents the environment for ICT utilization, as well as a “major change that involves the entire social system, ranging from legal frameworks and usage practices, to value judgements” [Mur-04]. On the other hand, UbiNet is an ICT environment that can potentially create a new huge market (ubiquitous electronics and ubiquitous services), in which diverse and profuse digital content is exchanged through connections to broadband networks. For Japanese officials, the “realization of the ubiquitous society will bring about sustainable economic growth and a safe and secure society” [Mur-03].

The envisioned ubiquitous services can be divided into five levels: (a) the “communications” level, where the UbiNet is used simply as an information transmission route, (b) the “information providing” level, that provides information as needed in response to user requests, (c) the “notification” level, which automatically notifies users of information they need, when they need it, (d) the “proposal” level, that proposes certain choices to users, in dealing with specific situations, and (e) the “automated” level, in which all necessary actions are executed in accordance with a given set of circumstances.

Japan’s vision on the emerging ICT paradigm is also based on the existing economic condition in Japan, which is due to the full-scale self-supporting revitalization by industry. In Japan, historically, this kind of autonomous revitalization was supported by specific groups of products, usually referred to as “the three sacred treasures of digital home appliances”. In detail, in the 50’s, black and white TV, electric washing machines, and electric refrigerators were these three treasures. In the 60’s and 70’s, colour TV, cars, and coolers replaced them. In the 90’s, PC, cellular phones, and email addresses were the new three treasures. In the beginning of the 21st century, digital cameras, Plasma Display Panel (PDP) and Liquid Crystal Display (LCD), and DVD are today’s treasures. In the emerging UbiNet environment, ubiquitous home appliances, ubiquitous cars, and ubiquitous offices are expected to be the new sacred treasures [Mur-04].

¹ Researchers in Europe developed plastic RFID prototypes that operate at the industry-standard frequency of 13.56 MHz. At the 2006 IEEE International Solid-State Circuits Conference, researchers from Philips (NL) presented an all-plastic device that responded with an 8-bit code when queried via RW by a nearby reader.

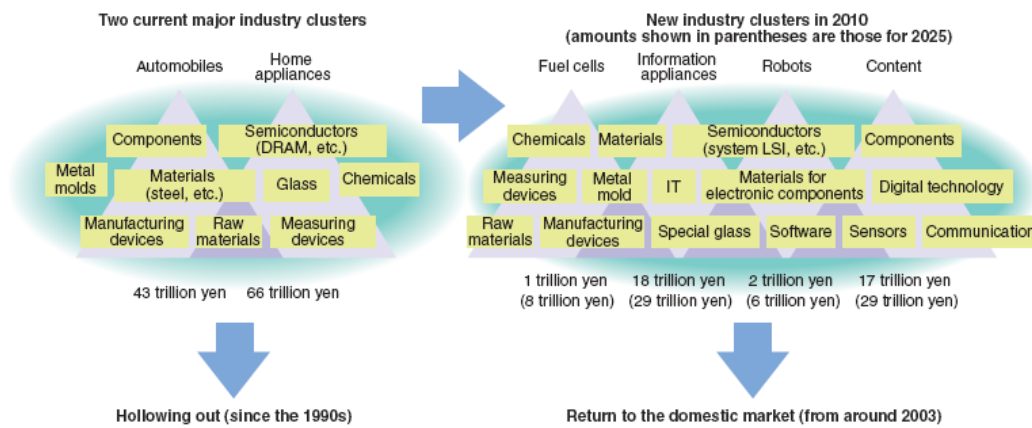


Fig. 18: Expected new industry clusters [Mur-05]

As mentioned above, the competitiveness and strength of the Japanese automobiles and home appliances industries are being lost. In addition, the advanced component and material industrial clusters, that are still competitive in Japan, may also be lost. As a plan of overcoming this situation, Japanese strategists expect that the establishment of the leading-edge industrial fields of fuel cells, digital home appliances, robots, digital content, and the fulfilment of the needs of three key-markets (health and welfare, environment and energy, business support in the domestic market) has become essential (Fig. 18) [Mur-05].

3.3 Cornerstones and Strategic Planning

The UbiNet, as Japan's emerging ICT paradigm, is expected to utilize the strength of the country's ICT environment. In specific, Japan is said to have become (2004) the world's largest ADSL country and the only country where >1M ordinary customers are enjoying optical fibre Internet access service at 100 Mbps (Table 4). Also, Japan is the world's largest market of car navigation systems. Moreover, Japan is one of the most advanced broadband nations in the world, if the situation is viewed in terms of absolute penetration numbers and progress in the development of super high-speed Internet access at >30 Mbps. Currently, Japan - in addition to ADSL and CATV - is also building upon 3G mobile phones, low-priced household optical fibre access service, wireless LAN and hot-spot applications [Mur-03, Mur-04].

Table 4: Annual velocity of broadband penetration (2004) [Mur-04]

(Unit: Million persons)

	Broadband	March 2004	March 2003	Annual velocity of penetration	Rate of population penetration (Rate of household penetration)
South Korea	ADSL	6.58	6.07	0.70	22.2% (92.3%)
	CATV	3.91	3.72		
	Total	10.49	9.79		
US	ADSL	7.68	5.10	7.09	7.6% (22.2%)
	CATV	13.68	9.17		
	Total	21.36	14.27		
Japan	ADSL	10.90	6.59	5.61 (4.83)	11.4% (31.0%)
	CATV	2.55	2.03		
	FTTH	1.04	0.26		
	Total	14.49	8.88		

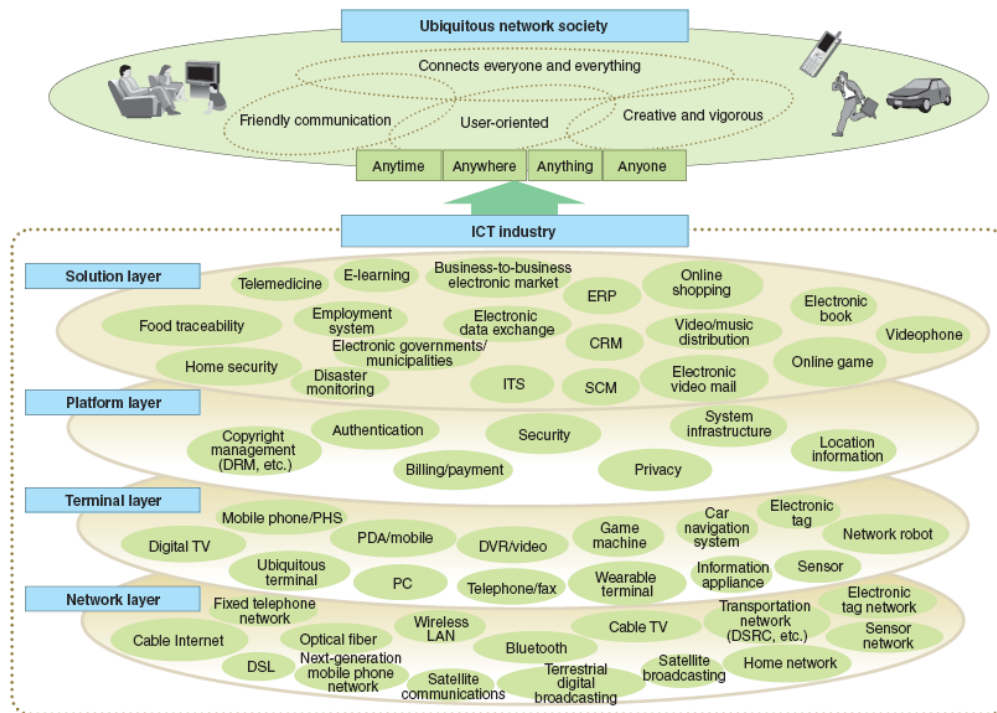


Fig. 19: The structure of the UbiNet Industry [Mur-05]

The ICT industry of the UbiNet environment is expected to consist of four or six layers (see Fig. 19). In the first case, the four layers are: the network layer, the terminal layer, the platform layer, and the application layer. In the latter, the six layers would be: the UbiNet infrastructure layer, the ubiquitous terminal layer, the ubiquitous platform layer, the ubiquitous content layer, the ubiquitous electronics layer and the ubiquitous service layer [Mur-05].

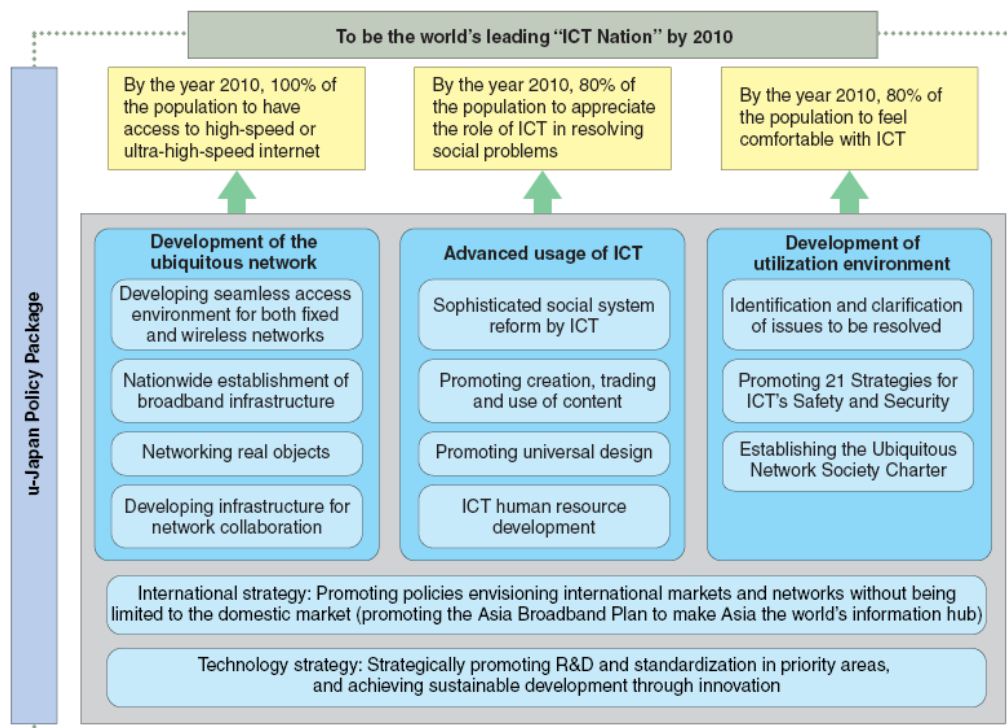


Fig. 20: Japan's ICT strategy and policy for 2010 [Mur-05]

The current Japanese national ICT policy (e-Japan II) is based on five strategies: (a) Development of the world's most advanced ICT infrastructure for the UbiNet, at an early stage, (b) construction of an Asian-wide platform for electronic bulletin board systems and content distribution, (c) concentrated investment on security and privacy protection, in order to make the network space in Japan the safest and most secure business spaces in the world, (d) establishment of business platform that connects ICT and services as new players, and (e) realization of four types of solutions, i.e. those for everyday life, business, government, and social systems. The emerging ICT strategy is called u-Japan and is still under development (Figs. 20 and 21) [Mur-05].

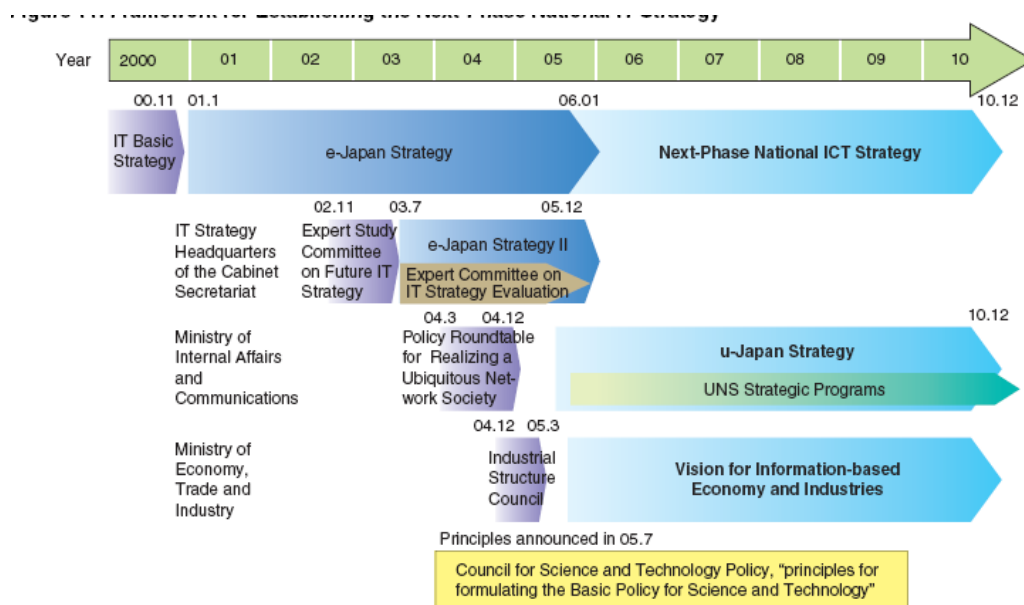


Fig. 21: Development of the next-phase Japan's National ICT Strategy [Mur-05]

As a result, Japanese strategists suggest that the country should [Mur-03, Mur-04]:

- (a) Construct a brand-new UbiNet infrastructure, originating in the country and not yet existing anywhere else in the world.
- (b) Utilize the UbiNet infrastructure, by means of: (a) building a ubiquitous terminal, (b) developing a ubiquitous platform where terminals are connected, and (c) providing a secure authentication, charging and settlement functionalities. Unless high-performance ubiquitous terminals continue to be marketed and unless users choose to pay network usage fees by making their own investment, the process of UbiNet will not move forward.
- (c) Promote the use and utilization of the UbiNet, by means of: (i) creating digital content, (ii) producing a panoply of ubiquitous electronics equipment and (iii) creating a group of services that utilize ubiquitous electronics. Three means for supporting the development of such content are suggested: first, the establishment of an evaluation system by Japanese people for digital content created in the country, and the transmission of easy-to-understand information about this worldwide; second, Japan should establish a global award for digital content that is equivalent to the Academy Awards² in the field of animation, electronic games and computer graphics; third, a symbolic core city, equivalent to Hollywood or Cannes, that has a series of functional clusters, such as core facilities, support industry complex, educational organizations, and accreditation organizations is established.

² Note the conflict between the Japanese strategists desire to adopt their own country's UbiNet paradigm, and their suggestion of mimically adopting specific practices followed by the European (i.e., Cannes Festival) and North American (i.e., Oscar Awards, City of Hollywood) culture industry.

In addition to the above cornerstones, basic R&TD in the UbiNet area should be carried out, on a co-operative basis that jointly involves the industrial, academic and public sectors, rather than being carried out separately by individual companies. The UNS (Ubiquitous Network Society) Strategy program (2005) represents the three pillars for R&D in Japan, namely: (a) Universal communication, (b) New-generation network, and (c) Security and safety. Also, strategists suggest that Japan has to play an active role in developing protocols for UbiNet, since Japanese companies were left largely behind during the 60's and only begun to try to catch up once the de facto standards had already been established. Finally, it is suggested that Japanese companies device business models at the same time they develop technical standards, otherwise they risk becoming merely suppliers of commodities [Mur-03, Mur-05].

3.4 Security and Privacy Strategies

Along with significant convenience and prospect, UbiNet is at the same time highly vulnerable from the viewpoint of security. The UbiNet is expected to bring about ultimate network convenience and, at the same time, it has the possibility of bringing ultimate vulnerability. In UbiNet, the routes for potential security breaches are many and diverse. Constant-access networks present a high risk of instantaneous spread of viruses and worms. Also, it is very difficult to monitor and trace the new threats that appear. In this respect, UbiNet should set up a reasonable range of controls to face the arising threats and vulnerabilities, thus ensuring secure information distribution. Only after overcoming this vulnerability can the UbiNet truly become a useful tool for business, as well as for administrative activities involving personal data. Therefore, as the UbiNet, which is accessible by diverse information equipment, is vulnerable to attack, the security issue could be the most serious bottleneck in promoting its penetration [Gri-04, ITU-05]. In this respect, the emerging Japanese national policy (u-Japan) adopts measures to appeal to the value judgment of users, in addition to these institutional and technical measures. For this purpose, a UbiNet Social Charter was proposed, in order to stipulate the basic stance of users living in the UbiNet (Fig. 22).

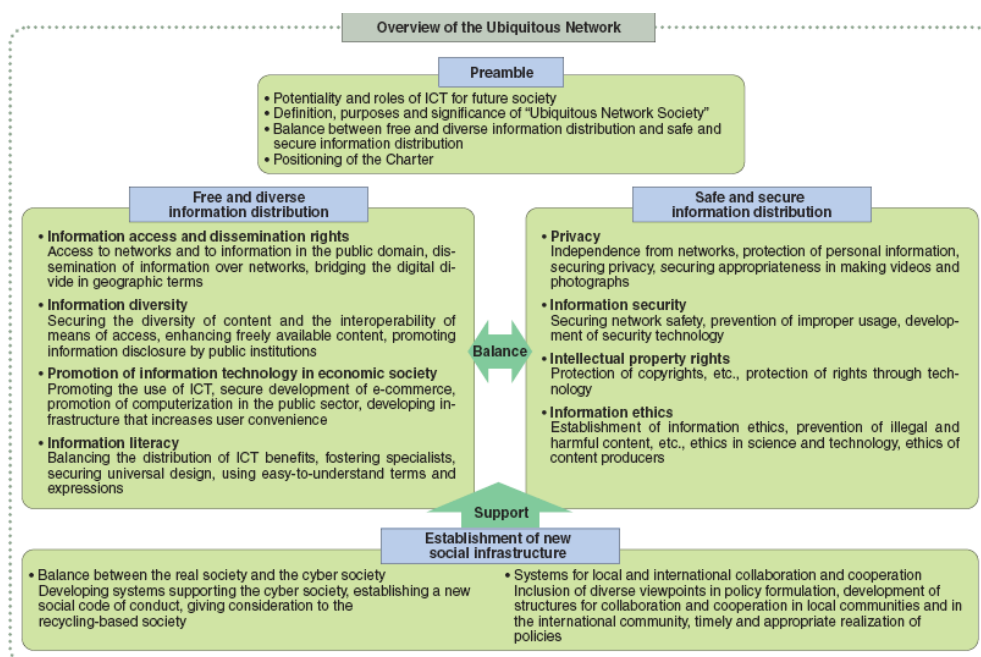


Fig. 22: UNS Charter Overview [Mur-05]

In UbiNet, there will be a plenty of networks of physical objects. These networks will include RFID, sensors and actuators, network robots, GPS networks, etc. This type of network actively approaches objects and directly incorporates them into part of the network. In terms of privacy and security, the full-scale realization of this type of network will essentially involve difficulties, at a level far different from that encountered in the previous paradigm. In Japan, it is considered important to deal with the security and privacy issues in the early stage of their development, so as to give proper solutions and answers to the problems and concerns expressed by the users. In that sense, it is suggested that the government encourages and supports R&D in the field of security, especially with respect to security in the individual and household sectors. The UbiNet Society (UNS) Programme represents the three pillars of Japan's current R&D strategy. These pillars are: (a) Universal communication, (b) New-generation network, and (c) Security and safety. According to UNS, the security and safety technology pillar focuses on realizing a safe and secure society by establishing an ICT infrastructure that is not interrupted by cyber-attacks or large-scale disasters, and by overcoming social problems (i.e. global environment issues, declining birth rate, aging society, etc.) by means of ICT (Fig. 23).

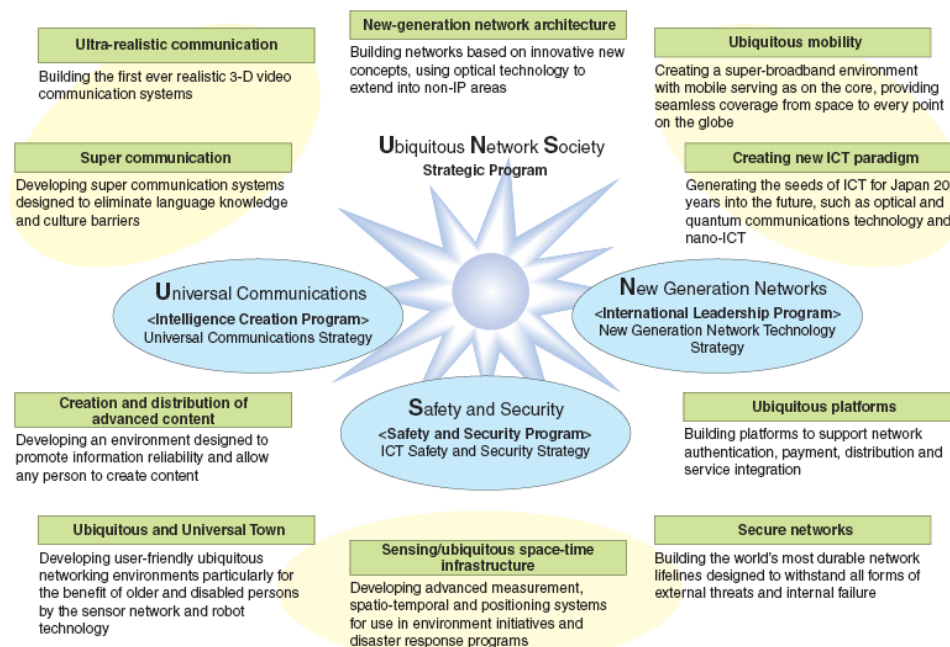


Fig. 23: The UNS Strategic Program [Mur-05]

The Japan's Council for Science and Technology Policy described six policy goals (see Fig. 24) to be achieved within the next few years. One of these goals is to establish a "nation able to be proud of its security, or, in other words, to realize the safest country in the world, in terms of securing safety in country, society, and everyday life" [Mur-05].

Japanese strategists argue that it is simply impossible to formulate any national ICT strategy in the UbiNet environment, without dealing with the "negative aspects" that can be "collectively called the security and privacy issues". Therefore, although the e-Japan I national strategy was initially started without having a priority area devoted to security, during its (current) phase (e-Japan II), security was added to its priority areas of concern.

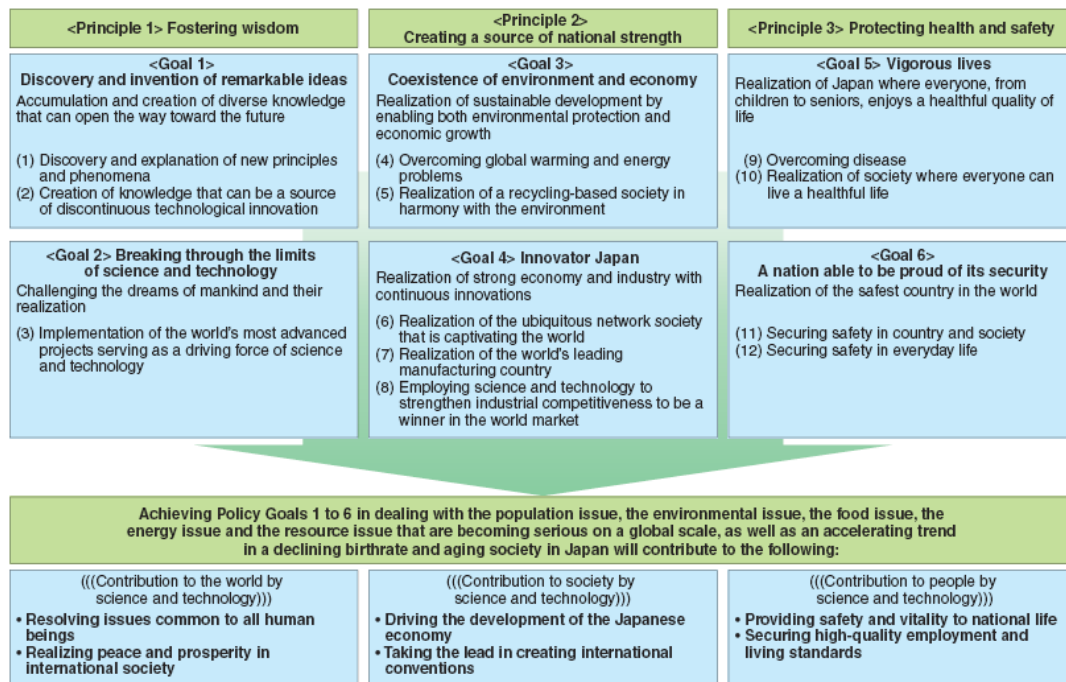


Fig. 24: Japan's Science and Technology Policy goals [Mur-05]

Furthermore, the Personal Data Protection Law (2005) forced privacy to be added to the priority areas (see Fig. 25). On the other hand, the technology protecting user privacy has also the potential of not preventing the expansion of the more shadowy aspects of anonymity (i.e., stalking, slander and defamation, money laundering, cyber-terrorism, etc.) [Gri-04, Mur-03, Mur-05].

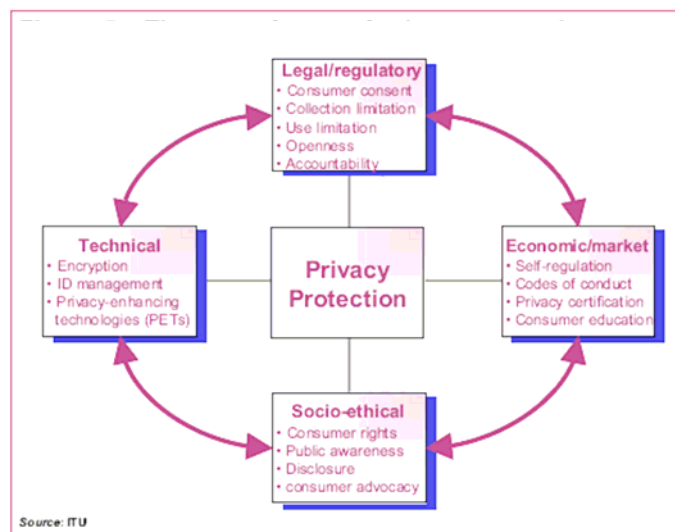


Fig. 25: Facets of privacy protection [ITU-05]

In view of UbiNet, analysts feel that the growth of the digital industry infrastructure will depend on how some security-specific processes (i.e., authentication, billing, payment settlement, etc.) will take place, because these processes make network transactions work smoothly, for both providers and users. Nowadays, although online transactions in Japan have gained a certain degree of support from users, a vague anxiety about the privacy of online transactions does exist. Regarding specific functionalities and technologies, Japanese analysts

suggest that the essential digital platform requires functions, such as: (a) authentication, (b) charging, (c) payment, (d) copyright management, (e) security, and (f) privacy management, as well as a system infrastructure that integrates these functions. Specific attention is given to the so-called “authentication module”, which is expected to utilize authentication technology, biometrics (bio-authentication), UIM (User Identity Management), in order to contact individual authentication. It is also argued that the security of the UbiNet can only be dealt with by mobilizing all the technologies available [Mur-03, Mur-04].

The development of privacy technologies is of particular importance in Japan. At present, the mainstream of R&D on individual identities on the network emphasizes the aspect of how to associate an ID with an ID. Not much research has been done on how to separate network-based ID and real personal data. Japanese analysts do realize that this is a subject that would not get much attention if left to company-side initiatives. This is also an important topic for governmental organizations, provided that they most frequently use personal data [Mur-03].

Security is an issue that should be also addressed by: (a) establishing a legal framework and (b) making use of cultural approaches, such as the development of a security culture [Gri-04]. Assets such the trust between suppliers and users often constitute a company’s largest invisible asset. At present, tampering with websites and unauthorized access are, among others, crimes subject to penalty. Japanese strategists argue that what is important in the social systems is “not to press victims to take appropriate preventive measures, but to punish perpetrators of such acts”. As a result, it is suggested that the focus should be shifted to the prosecution of offenders, as well as to the establishment of a framework that enables: “detering” an offender from committing the crime in the first place, “arresting” offenders without fail through thorough investigation, once a crime is committed, and “meeting out appropriate punishment”. In this sense, security, privacy, and network crime prevention measures should be established as “core areas”, in order to make clear that network attacks are serious crimes, resulting in strong punishment [Mur-05].

Under the current circumstances, Japanese strategists claim that there is much they can learn from the “advanced and comprehensive” security-related approaches taken in the US. They argue that, after 11.09 attacks, the US has been allocating substantial resources not only to national security and public order, but also to advanced security measures for the electronic networks. In this respect, they suggest³ that Japan’s next-phase national ICT strategy on security and privacy should learn from “the extensive experience accumulated in the US and by keeping in step with that country” [Mur-05].

Regarding security and privacy, the emerging u-Japan policy framework - expected to follow e-Japan (Fig. 26) - is suggested to adopt measures to also appeal to the value judgment of users, in addition to the institutional and technical measures [Mur-05].

³ Note another conflict, as the vision of Japan’s independent path to UbiNet contradicts with the Japanese analysts suggestions for blindly adopting specific practices, which are followed in other countries (e.g., the US).

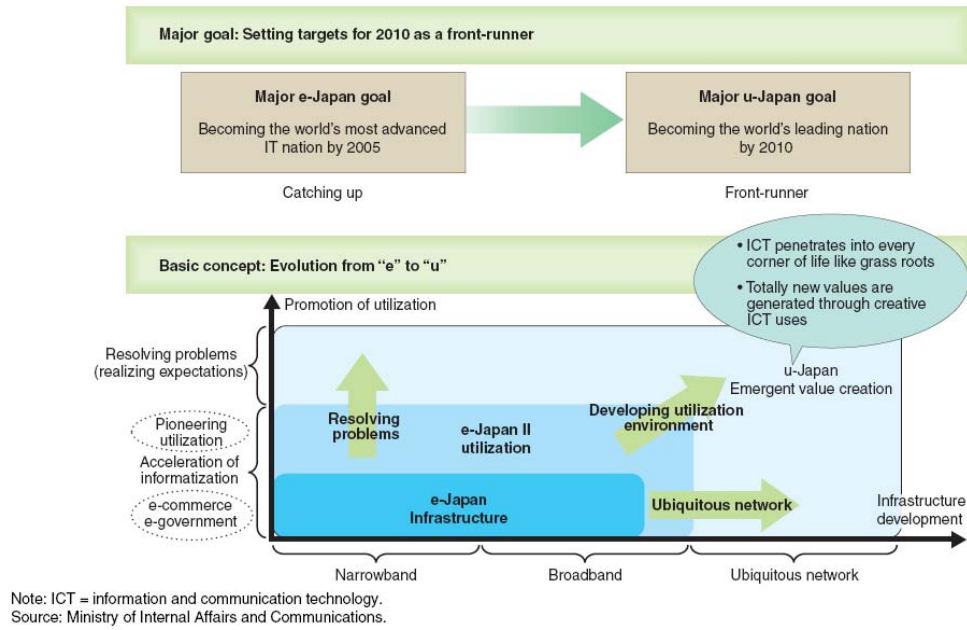


Fig. 26: Framework of a u-Japan Policy [Mur-05]

4 Towards a Consolidated View

4.1 The Strategic Situation

European Union

The European Union (EU) holds an advantage in the wireless and mobile domain (e.g. developing the Digital Enhanced Cordless Telecommunications (DECT), and Global System for Mobile Communication (GSM) standards). It is also in a strong position because of technological progress in the fields of broadband and multi-platform access, in particular digital television and 3G mobile communication systems. One of its goals is to play a leading role in the emerging market of new services which exploit the full potential of existing fixed networks (xDSL technologies), the local radio loop (BLR or high-speed wireless access), and satellites, which are essential for serving zones with low or no network coverage. Wireless systems, whether UMTS (3G mobile telephony), Wi-Fi or WiMax, also offer potential for developing novel applications and new services.

In the EU, the emerging ICT paradigm is cultured under the notion of Ambient Intelligence (AmI). AmI implies a “seamless environment of computing, advanced networking technology and specific interfaces, which is aware of the specific characteristics of human presence and personalities, takes care of needs and is capable of responding intelligently to spoken or gestured indications of desire, and even can engage in intelligent dialogue. AmI should also be unobtrusive, often invisible: everywhere and yet in our consciousness - nowhere unless we need it. Interaction should be relaxing and enjoyable for the citizen, and not involve a steep learning curve”. Lately, the term “Ambient Assisted Living” (AAL) is also introduced. In the given context, AAL seems to refer to an emerging context, where AmI is expected and envisioned to act as the major abstract guidance. AmI is considered to stem from the convergence of three key technologies: Ubiquitous Computing, Ubiquitous Communication, and Intelligent User Friendly Interfaces. The emphasis is placed on greater user-friendliness, more efficient services support, user-empowerment, and support for human interactions.

EU wishes to adopt a holistic view of AmI, considering “not just the technology, but the whole of the innovation supply-chain from science to end-user, and also the various features of the academic, industrial and administrative environment that facilitate or hinder realisation of the AmI vision”. It promotes cooperation between academia and industry regarding ICT and co-evolution of the technology and the market; thus, adopting a business-oriented perspective. It envisions a society where people live in and navigate between (both physically and virtually) different interconnected social settings (the home, workplace, school, hospital, social care facilities, cultural institutions etc.), within which they may adopt multiple roles and have different needs that depend on both the physical context and the mood of the individual.

The humans and physical entities - or their cyber-representatives - together with services share this new AmI space, which encompasses the physical and virtual world. The Ami Space could be seen as the integration of functions at the local level across the various environments, enabling the direct natural and intuitive dialogue of the user with applications and services spanning collections of environments, as well as at the cyberspace level, enabling knowledge and content organisation and processing. To accomplish this across different physical (home, private and public vehicles, private and public buildings, on the road) and social (family, enterprises, etc.) spaces is not a trivial exercise and it is certainly not only technical.

ISTAG sees “significant opportunities” for AmI in relation to:

- Modernising the European social model particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services.
- Improving Europe's economy in terms of: supporting new business processes; increasing the opportunities for teleworking in the networked home; enhancing mobility and improving all forms of transport; supporting new approaches to sustainable development.

The technology requirements for AmI that Europe identifies are: Req-1: Very unobtrusive hardware, Req-2: A seamless mobile/fixed communications infrastructure, Req-3: Dynamic and massively distributed device networks, Req-4: Natural feeling human interfaces, and Req-5: Dependability and security. On top of these generic technology requirements the following list of major research domains emerge:

- AmI compatible enabling hardware, including fully optical networks, nano- or micro electronics, power and display technologies.
- AmI open platforms: for interoperating networks based upon a corporate effort to define a "service control platform".
- Intuitive technologies involving efforts to create natural human interfaces.
- AmI developments in support of personal and community development, including socio-technical design factors, support for human-to-human interaction and the analysis of societal and political development.
- Metacontent services developments to improve information handling, knowledge management and community memory, involving techniques such as smart tagging systems, semantic web technologies, and search technologies.
- Security and trust technologies in support of privacy safety and dependability.

EU also shares societal, ethical, cultural and political concerns. These include privacy, control and social acceptance issues. The view of AmI is rather optimistic; however, it doesn't disregard the potential threats in this new environment. In this new context, people will participate "in a multiplicity of parallel, overlapping, inter-leaved and evolving one-to-one, one-to-many, and many-to-many relationships, some of which will be very short-lived, and some of them established temporarily and (apparently) instantaneously. Much of the communication between participants in these relationships will be asynchronous (as it is now): this means that 'virtually' applies to time as well as space". The current security solutions will probably prove to be insufficient in the new environment, because they are designed based on specific conditions, which will not further apply, such as relatively stable, well-defined, consistent configurations, contexts, and participants to the security arrangements.

The emerging paradigm introduces the notion of "conformable" security, that is the degree and nature of security associated with any particular type of action will change over time and with changing circumstances and with changing available information so as to suit the context. The security challenges posed by ISTAG are numerous and these are related to personal data protection and anonymity in a new highly personalised environment, to security management when the user adopts multiple roles and engaged in diverse relationships, to dependability and trustworthiness, to security awareness in a diverse group of users, to issues of emergent behaviour by an intelligent environment with unknown results, and more. However, this is not only recognised as a potential gap or threat but as an opportunity for EU to increase its industry's competitiveness by exploiting this change in paradigm. It is also viewed as a necessary precondition in order to maintain an independent capability in the field of security for Europe. Europe is oriented towards user-friendly, acceptable and usable security that enables the use of the AmI products and not hinders their exploitation. It also aims to

address different security aspects, such as security related to the individual, to communities and social groups, to the industry or to critical infrastructures. It also directs research to security for the evolving technological frameworks (e.g. mobile computing, grid computing, etc.).

Further, and in the context of the AmI vision in the European Union, the concepts of trust and confidence are top horizontal ICT priorities, along with security and privacy. Trust is recognized as a resource for social and business cooperation, whilst security is a condition for their enduring existence. Building citizens' confidence in AmI spaces should involve privacy issues, unfair or illegal commercial practices, unsolicited communications, and harmful content distribution. In this respect, specific new tools and methodologies are essential to improve technology and infrastructure dependability - in terms of self-testing, self-repairing, and fault tolerant - and thus enabling a trustworthiness AmI space, as failures in reliability, survivability, or adaptability will impact users' confidence in the Information Society.

Concluding, Europe has adopted AmI as its emerging ICT paradigm and aims to exploit its leading position in wireless and mobile technology. The goal is to create a new market of user-oriented services based on an existing or evolving communications infrastructure and sustain European economic growth. The Vision of AmI is highly oriented in improving the life of European citizens and many of the projects, research agendas, roadmaps and scenarios are oriented towards new services for elderly, disabled or working citizens. Europe also highlights the need for a new security paradigm that will address the risks and threats raised by the emerging environment. It is oriented towards user-friendly, acceptable and usable security that enables the use of the AmI products and not hinders their exploitation. Issues of trust and confidence are top horizontal ICT priorities, along with security and privacy. However, although Europe has a clear vision and strategic planning, its weakness lies in the slower rates of implementing the envisioned Information Society.

United States

After a long time of scientific and technology leadership, USA has a significant pressure for holding and preserving it. Nowadays, the economic situations in other economies, such as in the European Union, Japan and China, in accordance with their technology advances motivate in USA a flurry of discussions and public actions with an eye towards US pre-eminence in advanced scientific research and development.

In the context of ICT, the challenge of preserving US technological competitiveness is more diffuse, complex and long-term. Advances to ICT have the potential to offer more sophisticated services to end-users and engender new business models for many organizations. These new benefits will be facilitated by geometric advances in semiconductor and magnetic storage as well as in electronic and optical communications. In this context the recognized technology challenges that can generate social, economic, political, scientific and technology benefits if specific actions take place by public and private sector are, inter alia: Knowledge Environments, High Confidence Infrastructure Control Systems, Improved Patient Safety and Health Quality, Nanoscale Science and Technology, Predicting Pathways and Health Effects of Pollutants, Real-Time Detection, Assessment and Response to Natural or Man-Made Threats, Safer - More Secure - More Efficient - Higher-Capacity - Multi-Modal Transportation System, Anticipate Consequences of Universal Participation in a Digital Society, Collaborative Intelligence, Generating Insights From Information at Fingertips, Managing Knowledge-Intensive Dynamic Systems, and Rapidly Acquiring Proficiency in Natural Languages.

The emerging ICT paradigm adopted in USA is usually called Ubiquitous/Pervasive Computing or Embedded systems, respectively. UbiComp refers to numerous, often invisible, computing devices, mobile and embedded into the environment, connected through wired or

wireless network infrastructures. The benefits of UbiComp will be tremendous and will introduce new ways of thinking, regarding computing and communications trends and will be tightly coupled to the physical world through miniature sensors and actuators. On the other hand, UbiComp is expected to change the way the humans interact with computational devices in a way similar to how Internet changes our lives.

However, in order to meet the challenges introduced by UbiComp and to fully exploit the benefits of the new paradigm a holistic view of UbiComp is essential. It is important to analyze not only technological issues but social, as well as ethical issues. UbiComp is expected to change the frontiers of well-know practices adopted in science and engineering while a more detailed analysis about the role of government and private sector partnership is needed. Thus, the US policy regarding research priorities in the UbiComp domain are: (a) Predictability and manageability, (b) Adaptive self-configuration, (c) Monitoring and system health, (d) Computational models, (e) Network geometry, (f) Interoperability, (g) Integration of technical, social, ethical, and public policy issues, and (h) Enabling technologies.

In terms of action priorities, USA aims at promoting interdisciplinary approaches to research on UbiComp, which tie computer science to other sciences and disciplines. Furthermore, USA desire to change the way research is organized. Academia and industry will both have important roles to play in accordance with the government and federal agencies. Explicit efforts will need to put mechanisms in place for ensuring such collaboration, ignoring lessons-learned and the history.

UbiComp, due to its dynamic and pervasive nature, introduces many security and privacy challenges. Analysts believe that UbiComp introduces a new security paradigm regarding how we can deal with novel and sophisticated security and privacy requirements. In this context, and in accordance with the priorities posed by USA in terms of security, after 11.09 attacks, US analysts argue that new security practices are important in the case of UbiComp and in relation with US national security priorities. Addressing UbiComp security issues requires a dynamic ongoing effort in order to develop the technologies necessary to design secure, reliable and trustworthy UbiComp systems.

USA recognizes that technical approaches alone will be insufficient for the protection of privacy and security in the UbiComp context. The overall approach is that specific policies and technical initiatives should be also adopted in order to adequately address the emerging security issues. In this respect, the most important security research issues regarding UbiComp are considered to be: (a) the definition of specific and standard based network access policies and controls, (b) the definition and the enforcement of security policies, (c) critical infrastructure self-defence, and (d) energy scarcity.

Regarding privacy, the implications introduced by UbiComp are quite sophisticated and more difficult to deal with. An open issue is how to advise people when their actions are monitored and when their personal data are disclosed in a way that is not noticeable and evident. Thus, embedded mechanisms that enhance the control of the users over their personal information in a way that does not hamper the evolution of UbiComp are crucial. In this context, the most important research priorities regarding privacy issues in UbiComp are: (a) enabling flexible, configurable privacy policies in systems, so that as external situations or policies change, this can be reflected seamlessly to the system, (b) the implementation of specific techniques in terms of informed consent about the privacy issues, (c) research into possible legal requirements for the protection of personal information in order to ensure adequate accountability, and (d) the development of specific anonymity mechanisms that should protect users' identities through appropriate identity management procedures.

From national security perspective, USA is the most organized nation in terms of strategies adopted and actions taken. US recognize, especially after 11.09 attacks, the importance of its critical infrastructures and their reliance in the underlying information technologies. Cyber-space vulnerabilities put the whole national infrastructure at risk, as they may jeopardize intellectual property, business operations, and consumer trust. In this context the future actions of US regarding the protection of critical infrastructure and cyberspace are: (a) the enlargement of the federal R&D funding in civilian cyber security, (b) the broadening of the nation's cybersecurity research community, (c) the organized transition of current cybersecurity technology efforts from federal investments into civilian best practices and products, and (d) the description of specific coordination practices regarding federal cybersecurity R&D efforts.

Concluding, in the case of US the UbiComp paradigm is expected to offer serious benefits to end-users, as well as to organizations. The overall effort of USA is to keep their leadership in the ICT sector, while preserving the national security. In order to achieve those goals, specific R&D areas have been recognized that should be accomplished through the harmonic interaction and cooperation of the government, academia and private sector. USA exploits a strategic roadmap towards security and privacy in UbiComp. Whilst this plan is associated with national security issues a potential deployment weakness is exhibited, since civilians' privacy and infrastructures' safety require almost controversial research, social, economical and legal initiatives and policies.

Japan

The competitiveness and strength of specific Japanese industries is being lost due to the progress of globalisation in the 90's. Japan is economically surrounded by: (a) the US, which seems to be pursuing a principle of one-nation prosperity, supported by strong military power, (b) South Korea, which is repeating strategic reorganizations with the ability to make decisions far more quickly and boldly than Japan, and (c) China, with its really huge potential. As a result, the Japanese industry should survive and grow under the situation defined by: (a) the US, which continues to be the champion of the world's economy, (b) the EU and the other European countries, which have steadily expanded their economic scale and (c) the Asian nations, including China, which has an enormous economic scale, strong price competitiveness and power to promote business operations, and (d) Korea, which has the ability to make decisions quickly and implement strategies. The available options for competitive strategies, which are left for Japanese industries to choose, are limited. The existing economic condition in the country is mainly based on the full-scale, self-supporting revitalization by industry. This kind of autonomous revitalization was supported by specific groups of products, usually referred to as "the three sacred treasures of digital home appliances".

Under the circumstances, Japan industries wish to focus at developing strategic superiority in terms of "being different" rather than "being fast". Their underlying approach is to be based on ICT and make Japan's own ICT "paradigm" different than that of any other country. As a result, Japan plans to transfer the competition to a new ICT paradigm, to make the most of its own know-how, and to create a new ubiquitous industry. A problem with this is that Japan's ICT strategies have always followed ICT paradigms pioneered by other countries (e.g. the Silicon Valley in the US in the 90's, and the Korea's fast shift towards broadband in the 21st century). Until today, Japan's real progress towards this goal remains hardly visible. On the other hand, Japan has succeeded in operating well the industrial information systems and in ensuring that this situation is steadily been improved by: (a) utilizing Chinese resources, as bases for outsourcing and system development, (b) responding to frequent consolidations and company break-ups, and (c) ensuring business continuity in an emergency.

The emerging ICT paradigm, adopted by Japan, is called Ubiquitous Network. UbiNet is something that pursues the ubiquity of network connections, not the ubiquity of computing capabilities. UbiNet positions the user at the centre of the ICT environment. Also, UbiNet represents both, the environment for ICT utilization, as well as a major change that involves the entire social system, ranging from legal frameworks and usage practices, to value judgements. Japanese consider that UbiNet is an ICT environment that can potentially create a new huge market, in which diverse and profuse digital content is exchanged through connections to broadband networks. For Japanese, the realization of the UbiNet will bring about sustainable economic growth, and a safe and secure society.

However, progress in shifting only towards modern network technologies may establish Japan as the leading broadband nation, but will not necessarily make Japan the leading ICT nation. For doing so, Japan needs new strategies capable of leading its industries to comprehensive innovation throughout UbiNet. Thus, the focus is on ensuring Japan's industrial lead through the establishment of the world's first, only, and best ICT environment, an environment allowing industries to connect to consumers anywhere and at any time via broadband networks. It is worth noticing that the local consumers are expected to play a central role, as they are call themselves the consumers with the most sophisticated and mature consumption behaviour in the world, with respect to digital information equipment. Towards these goals, the current national ICT policy (e-Japan II), is based on five strategies: (a) Development of the world's most advanced ICT infrastructure for the UbiNet, at an early stage, (b) construction of an Asian-wide platform for electronic bulletin board systems and content distribution, (c) concentrated investment on security and privacy protection, in order to make the network space in Japan the safest and most secure business spaces in the world, (d) establishment of business platform that connects ICT and services as new players, and (e) realization of four types of solutions (everyday life, business, government, and social systems). In connection to this, the establishment of the leading-edge industrial fields of fuel cells, digital home appliances, robots, digital content, and the fulfilment of the needs of three key-markets (health and welfare, environment and energy, business support in the domestic market) are considered essential

In terms of action lines, Japan aims at: (a) constructing a brand-new UbiNet infrastructure, originating in the country and not yet existing anywhere else in the world, (b) utilizing the UbiNet infrastructure, by means of building a ubiquitous terminal, developing a ubiquitous platform where terminals are connected, and providing a secure authentication, charging and settlement functionalities, (c) promoting the use and utilization of the UbiNet, by means of creating digital content, producing a panoply of ubiquitous electronics equipment and creating a group of services that utilize ubiquitous electronics. Development of such content can be supported by: first, the establishment of an evaluation system by Japanese people for digital content created in the country and the transmission of easy-to-understand information about this worldwide; second, the establishment of a global award for digital content in the field of animation, electronic games and computer graphics; third, a symbolic show-business core city that has a series of functional clusters.

In UbiNet, there will be a plenty of networks of physical objects. These networks will include RFID, sensors and actuators, network robots, GPS networks, etc. This type of network actively approaches objects and directly incorporates them into part of the network. In terms of privacy and security, the full-scale realization of this type of network will essentially involve difficulties, at a level far different from that encountered in the previous paradigm. In UbiNet, the routes for potential security breaches are many and diverse. Constant-access networks present a high risk of instantaneous spread of viruses and worms. Also, it is very difficult to monitor and trace the new threats that appear. In this respect, UbiNet should set up a

reasonable range of controls to face the arising threats and vulnerabilities, thus ensuring secure information distribution. Only after overcoming this vulnerability can the UbiNet truly become a useful tool for business, or for administrative activities involving personal data. Therefore, as the UbiNet is highly vulnerable to attacks, the security issue could be the most serious bottleneck in promoting its penetration.

Japan wishes to deal with the security and privacy issues in the early stage of their development, so as to give proper solutions and answers to the problems and concerns expressed by the users. In that sense, government encourages and supports R&D in the field of security, especially with respect to security in the individual and household sectors. The UbiNet Society (UNS) Programme represents the three pillars of the country's current R&D strategy. These pillars are universal communication, new-generation network, and security and safety. The third pillar focuses on realizing a safe and secure society by establishing an ICT infrastructure that is not interrupted by cyber-attacks or large-scale disasters, as well as by overcoming social problems (e.g. environment issues, declining birth rate, aging society, etc.) by means of ICT.

UbiNet will be based on a new digital platform, which requires some major functions, such as: (a) authentication, (b) charging, (c) payment, (d) copyright management, (e) security, and (f) privacy management. It also requires a system infrastructure that integrates these functions. Among these functions, specific attention is paid to the so-called "authentication module", which is expected to utilize authentication technology, biometrics (bio-authentication), UIM (User Identity Management), in order to contact individual authentication. In addition, security and privacy are two issues that should be also addressed by: (a) establishing a legal framework and (b) making use of cultural approaches, such as the development of a security culture. Assets such the trust between suppliers and users often constitute a company's largest invisible asset. In Japan, tampering with websites and unauthorized access are, among others, crimes subject to penalty. Strategists suggest not to press victims to take appropriate preventive measures, but to punish perpetrators of such acts. Thus, the focus should be shifted to the prosecution of offenders and to the establishment of a framework that enables: deterring an offender from committing the crime in the first place, arresting offenders without fail through thorough investigation, once a crime is committed, and meeting out appropriate punishment. Thus, security, privacy, and network crime prevention measures should be established as core areas, in order to make clear that network attacks result in strong punishment.

Regarding national security, Japan expects to learn much from the "advanced and comprehensive" security-related approaches taken in the US. They argue that after 11.09 attacks the US have been allocating substantial resources not only to national security and public order, but also to advanced security measures for the electronic networks. In this respect, they suggest that Japan's next-phase national ICT strategy on security and privacy should learn from the extensive experience accumulated in the US and by keeping in step with that country.

Concluding, Japan has adopted UbiNet not only as its emerging ICT paradigm, but also as a main means for making the country the leading ICT nation in the world. For Japan, the realization of the UbiNet will bring about sustainable economic growth and a safe and secure society. However, as UbiNet is highly vulnerable to attacks, the security issue could be the most serious bottleneck in promoting its penetration. To face this, Japan supports R&D, as well as other targeted initiatives, on issues such as authentication, ID management, copyright management, secure payment, and privacy technologies. From the legal point of view, the strong punishment of offenders is suggested, instead of the adoption of preventive measures by the users. In the area of national security Japan tends to keep in step with the US, thus de-

monstrating once more the inherent conflict of a nation, which wishes to be different and to mimic other nations strategies, at the same time. The same conflict appears also in Japan's strategy to promote the domestically developed digital content. Finally, Japan keeps on adopting traditional approaches on how to turn fast new technologies into short-term financial benefit.

4.2 The Vision and the New ICT Paradigm

The new ICT paradigms, which are emerging all over the world, such as ambient intelligence, pervasive computing, ubiquitous networking, ubiquitous computing, nomadic computing, always-best-connected service etc., are generally pursuing actually similar, or even the same, goals. The term "ubiquitous computing" originated in the US, while the term "ubiquitous network" was given birth in Japan, where more than one alternative to this term is officially used (ubiquitous network, ubiquitous information society, ubiquitous information network, ubiquitous computing). UbiNet is the Japan's term for the new ICT paradigm. In the US the terms of Ubiquitous Computing, Pervasive Computing, or Embedded Networks seem to prevail, as opposed to Europe, where their use is currently limited. The European Union is promoting R&D activities under the theme of AmI and, at present, the EU seems unlikely to replace the theme of AmI with that of UbiNet. Instead, the term Ambient Assisted Living (AAL) appeared in recent EU documents.

Europe clearly refers to a new ICT emerging paradigm and so does Japan by recognizing three eras in ICT: (a) Mainframes: One computer - many people, (b) Personal computers: One person - one computer, and (c) UbiComp: One person - many computers. USA researchers and analysts don't apply the term "paradigm", however US analysts recognize that ICT is on the verge of another revolution and they predict that the established practises in science and engineering will change dramatically. One can assume that all the three leading economies believe that ICT is transforming to a new paradigm or era of computing and communicating.

Examining the way each economy views the new ICT paradigm, one can recognise a core of similar ideas. EU envisions humans who will be surrounded by intelligent interfaces supported by miniature computing and networking technology which is everywhere, embedded in everyday objects and is considered capable of recognising and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way. US envisions ICT being embedded into a growing range of physical devices linked together through self-configured networks and will become ever more pervasive, as the underlying technology components become more smaller, faster, cheaper, and autonomous and change dramatically the way people interact with their environment. Japan adopts Weiser's vision and describes the new paradigm as connectivity anytime, any place, for anything (as opposed to the previous paradigm of connectivity anytime, any place, for anyone). From this viewpoint, network-enabled connections appear in three types: Person-to-Person (P2P), Person-to-Object (P2O) and Object-to-Object (O2O).

Analysts in all three reviewed economies agree on the strengths and benefits that will be introduced by the new paradigm. However, each country views AmI under its own perspective and in accordance with each one's technological advantages. Therefore, the European Union wishes to exploit its advantage in the wireless and mobile domain, while Japan aims at exploiting its expertise in gadgetry and services industry. Both adopt a business-oriented approach that aim to provide users with new services. From their point of view, USA, based on their current technological advantages and leadership in many sections, aim at preserving this status, as well as their national security, which is the ultimate target for this nation. Their st-

strategy is based in the cooperation between the government and the industry, with the government playing an important role.

4.3 Security and Privacy

AmI postulates a new security paradigm, characterised by "conformable" security in which the degree and nature of security associated with any particular type of action will change over time, space and situation. An important aspect regarding this paradigm is how leading economies consider and understand the security and privacy issues. While the "umbrella" term often used for security and privacy is trust, the way these economies realize these issues differs according to each country's technological and societal context and internalities.

EU promotes the idea of a new security paradigm that will address the new threats and vulnerabilities that dwell into the emerging paradigm. Security and privacy issues, which are prioritized, reflect the European culture, as issues of high importance are liberties of citizens and the protection of personal data and anonymity. Europe views AmI as an enabler and facilitator of the individual's participation in society, in a multiplicity of social and business communities, and in the administration and management of all aspects of their lives, from entertainment to governance. Thus the security concerns reflect such a perspective and focus on user's privacy, trust and security.

In USA, there are specific and clear goals regarding security and privacy, especially after 09.11. Thus, the focus of technological development in ICT currently leans towards critical infrastructure protection and cyberspace security. Their ICT strategy is expected to remain neither too close, nor too remote from national security. US analysts recognise that future ICT has more of a propensity to be ubiquitous and enveloping, unavoidable in the environment, where individuals are not in control of their interaction. In these cases, privacy issues cannot be addressed by education and personal policies alone. As opposed to EU, privacy issues are not addressed in the user level, but they become (even more) a matter of public policy and the responsibility for addressing these issues is a federal one.

Another relevant and important issue, regarding UbiComp and its underlying technologies in the US, is safety and reliability. This dimension of UbiComp, which is not considered as such an important issue in the case of neither Europe nor Japan, refers to the ability of the systems to operate without causing an accident or an unacceptable loss. Most national initiatives are directed in Critical Infrastructure Protection, as a top priority. Another important prerequisite, regarding security and privacy issues in the US, is that there must be a strong and viable relationship between government and private sector. Furthermore, US interests are also focused on promoting security and privacy issues beyond their borders, as they desire to be ready to lead global efforts, working with governments and industry alike, in order to secure cyberspace.

Japan recognizes the importance of security and privacy issues, but their approach is somewhat unclear, as Japan has just now turned to a security-focused strategic plan. Via this plan Japan aims at becoming the safest country in the world. In Japan, under the pretext of improving the security level and/or protecting privacy, user convenience has frequently been sacrificed, and there has been a tendency to neglect user-side features. Not surprisingly, Japan's next-phase national ICT strategy on security and privacy is expected to learn from the experience accumulated in the US and by keeping in step with US.

Japan's new security paradigm seems immature; Europe and US adopt new security paradigms in this new era. However, there is a major difference in perspective, which dwells in their cultural differences. Europe regards this new security paradigm as a necessary outco-

me of the new ICT paradigm. It includes trust, security and privacy in its requirements so as to promote AmI. Focus is placed primarily on the end-user and its protection. The culture in the US towards security issues, mainly formulated by the 09.11 events, gives first priority to security and then ubiquitous computing. In the US, security is a starting point not a necessary prerequisite. And the term is broader, it not only includes privacy issues, but its key priorities remain public and national safety. The initiative for such is a responsibility of the US government, as opposed to the European perspective, where initiative is placed in industry and academia and EU adopts a strategic and regulatory role.

Addressing the balance between privacy and security will be a core challenge for the future, related to the fundamental but complex interrelationship between what constitutes the private and the public space of an AmI-aware citizen. Harmonizing privacy and security policies achieves digital dignity.

4.4 Social Disruption

The overall success of this new technology paradigm will depend on its acceptability by citizens and by taking steps to mitigate, or even minimize, their concerns with regard to how it might lead to further encroachments upon their privacy, safety, and security. Realising any of these visions will require more than just technology and, as has happened throughout history, significant technological advances almost always raise policy issues. In this context, the formulation of adequate social and policy options would be proved to be essential. AmI is also regarded in many cases as an enabler of social changes.

Japan in its ubiquitous society vision includes the idea of ubiquitous metropolis. AmI is viewed as a mean to create user-friendly ubiquitous networking environments for the benefit of elderly or disabled persons, children or parents. The Japanese strategy shows a particular sensitivity in social issues and considers UbiNet as beneficiary in several social problems the Japanese society faces. For example, it is believed to contribute to issues, such as declining birth rate and aging society, medical and welfare services, employment of young people, working women and mothers, education and training, environmental issues etc.

The holistic EU AmI vision also includes societal agonies and interests. Its goal is to enable and facilitate participation by the individual - in society, in a multiplicity of social and business communities, and in the administration and management of all aspects of their lives, from entertainment to governance. The scenarios described in the Grand Challenges for IST report aim at addressing social issues, such as transport safety (The 100% Safe Car), European linguistic and cultural diversity (The Multilingual Companion), elderly and disabled citizens (the Service Robot Companion), as well as market and industry issues (The Intelligent Retail Store) [IST-04].

One of AmI goals are modernising the European social model particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services.

In the US challenges, some social and environmental issues are also included, such as knowledge environments, improved patient safety and health quality, predicting pathways and health effects of pollutants, participation in a digital society, etc. In several documents there is an indication that privacy and trust issues are not merely technical ones, however there is not a clear description of strategic planning, actions or projects for addressing the social and ethical issues that rise. These issues are mainly addressed by federal initiatives, with a prime fo-

cus in the public and national safety, outlining emphasis in critical infrastructure protection, and a secondary focus on civilians' privacy. No priority to such issues is really visible, in the existing strategic documents and initiatives.

References

- [CRA-02] Computing Research Association, *Grand Research Challenges in Information Systems*, USA, June 2002.
- [DHS-06] Dept. of Homeland Security, *National Infrastructure Protection Base Plan (draft 2)*, January 2006.
- [EU-05a] European Union, Call for proposals for indirect RTD actions under the specific programme for research, technological development and demonstration: “*Integrating and strengthening the European Research Area*”, Call identifier: FP6-2005-IST-6 (2005/C325/13).
- [EU-05b] European Union, Proposal for a Council Decision concerning the specific programme “*Cooperation*” implementing the 7th Framework Programme (2007-13) of the European Community for research, technological development and demonstration activities, Brussels, 21.9.2005, COM(2005)440.
- [EU-05c] European Union, Proposal for a Council Decision concerning the specific programme: “*Ideas*” implementing the 7th Framework Programme (2007-13) of the European Community for research, technological development and demonstration activities, Brussels, 21.9.2005, COM(2005)441.
- [EU-05d] European Union, Proposal for a Council Decision concerning the specific programme “*People*” implementing the 7th Framework Programme (2007-13) of the European Community for research, technological development and demonstration activities, Brussels, 21.9.2005, COM(2005)442.
- [EU-05e] European Union, Proposal for a Council Decision concerning the 7th framework programme of the European Community for research, technological development and demonstration activities (2007-13), Brussels, 6.4.2005, COM(2005)119 final.
- [Fri-06] Friedewald M., Vildjiounaite E., Wright D. (Eds.), *The brave world of Ambient Intelligence: A state-of-the-art-review*, SWAMI Project Consortium, Deliverable 1, January 2006.
- [Fri-05] Friedewald M., Wright D., Vildjiounaite E. (Eds.), *Safeguards in a World of Ambient Intelligence: Scenario Analysis and Legal Framework*, Report to the 1st SWAMI Expert Workshop, Brussels, June 2005.
- [Fuj-00] Fujinuma A., Murakami T., “Ubiquitous Networking: Towards a new paradigm”, *NRI Papers*, Paper no. 2, Nomura Research Institute, Japan, April 2000.
- [GAO-04] US Government Accountability Office, *Defense Acquisitions. The Global Information Grid and Challenges Facing Its Implementation*, Report to the Subcommittee on Terrorism, Unconventional Threats, and Capabilities, House of Representatives, USA, July 2004.
- [Gri-04] Gritzalis D., *Autonomy and Civic Disobedience in Cyberspace*, Papassotiriou Publ., Athens 2004 (in Greek).

- [IST-01] IST Advisory Group; Ducatel, K., et al., *Scenarios for Ambient Intelligence in 2010*, Joint Research Centre, Institute for Prospective Technological Studies, 2001 (<http://www.cordis.lu/ist/istag-reports.html>).
- [IST-02a] IST Advisory Group, *Trust, dependability, security and privacy for IST in FP6*, Office for Official Publications of the European Communities, 2002 (www.cordis.lu/ist/istag-reports.html).
- [IST-02b] IST Advisory Group, *Strategic orientations and priorities for IST in FP6*, Office for Official Publications of the European Communities, 2002 (www.cordis.lu/ist/istag-reports.html).
- [IST-03] IST Advisory Group, *Ambient Intelligence: From Vision to Reality. For participation in society and business*, Office for Official Publications of the European Communities, 2003 (www.cordis.lu/ist/istag-reports.html).
- [IST-04] IST Advisory Group, *Grand Challenges in the Evolution of the Information Society*, Office for Official Publications of the European Communities, 2004 (<http://www.cordis.lu/ist/istag-reports.html>).
- [ITU-05] ITU, *The Internet of Things*, Executive Summary, International Telecommunications Union Reports, November 2005.
- [J&P-05] J&P Management Consultancy, *Russia: Broadband Market*, Expert Opinion, Moscow 2005.
- [Lan-91] Lane J., *Situated learning: Legitimate peripheral participation*, Cambridge University Press, USA, 1991.
- [MITF-04] Mobile IT Forum, *Towards the 4th Generation Mobile Communications Systems (The Flying Carpet Report)*, ver. 2.0, Japan, April 2004.
- [Mur-05] Murakami T., "Japan's National IT Strategy and the Ubiquitous Network", *NRI Papers*, Paper no. 97, Nomura Research Institute, Japan, November 2005.
- [Mur-04] Murakami T., "Ubiquitous Networking: Business Opportunities and Strategic Issues", *NRI Papers*, Paper no. 79, Nomura Research Institute, Japan, August 2004.
- [Mur-03] Murakami T., "Establishing the Ubiquitous Network Environment in Japan", *NRI Papers*, Paper no. 66, Nomura Research Institute, Japan, July 2003.
- [NITRD-04] Networking and Information Technology R&D (NITRD), *Grand Challenges: Science, Engineering and Societal Advances Requiring Networking and Information Technology Research and Development*, 2nd printing, March 2004.
- [NRC-03] National Research Council, *Embedded Everywhere: A Research Agenda for Networked Systems of Embedded Computer*, Committee on Networked Systems of Embedded Computers, National Academy Press, USA, 2003.
- [NIST-01] National Institute of Standards and Technologies, *Proc. of the IT Conference on Pervasive Computing*, 2001 (www.nist.gov/pc2001/about_pervasive.html).
- [OECD-05] OECD, *Broadband Statistics*, Telecommunications and Internet Policy, July 2005.

- [PITAC-05a] President's Information Technology Advisory Committee, *Computational Science: Ensuring America's Competitiveness*, Report to the President, USA 2005.
- [PITAC-05b] President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization*, Report to the President, USA, February 2005.
- [Sat-01] M. Satyanarayanan, "Pervasive Computing: Vision and Challenges", *IEEE Communications*, Vol. 8, No. 4, pp. 10-17, August 2001.
- [Suc-85] Suchman L., *Plans and situated actions: The problem of human-machine communication*, XEROX Park Technical Report ISL-6, February 1985.
- [WHI-03] The White House, *National Strategy to Secure Cyberspace*, USA, February 2003.
- [Wie-XX] Wieser's views on UbiCom, www.ubiq.com/hypertext/weiser/UbiHome.
- [Wie-93b] Weiser M., "Hot Topics: Ubiquitous Computing", *IEEE Computer*, Vol. 26, No. 10, pp. 71-72, October 1993.
- [Wie-93a] Weiser M., "Computer Science problems in Ubiquitous Computing", *Com. of the ACM*, Vol. 36, No. 7, pp. 74-83, July 1993.
- [Wie-91] Weiser M., "The Computer for the Twenty-First Century", *Scientific American*, Vol. 265, No. 3, pp. 94-104, September 1991.
- [WWRF-01] Wireless World Research Forum (WWRF), *The Book of Visions 2001: Visions of the Wireless World*, ver 1.1, 2001 (www.wireless-world-research.org/general_info/BoV2001-final.pdf).

Short CV of the authors

Dimitris Gritzalis (dgrit@aub.gr) is an Associate Professor (ICT Security) at the Dept. of Informatics of the Athens University of Economics and Business, (AUEB) where he leads the Information Security and Critical Infrastructure Protection Research Group. He holds a BSc (Mathematics) from the Univ. of Patras (Gr), an MSc (Computer Science) from the City University of New York (USA) and a PhD (Security-Critical Information Systems) from the Univ. of the Aegean (Gr). His current research interests include security in AmI, security ontologies, VoIP systems security, security paradigms, privacy enhancing technologies, ICT security education, etc. He is the national representative of Greece to IFIP/TC-11, and a former Associate Data Protection Commissioner of Greece and President of the Greek Computer Society.

Marianthi Theoharidou (mtheohar@aub.gr) is a Researcher with the Information Security and Critical Infrastructure Protection Research Group at the Dept. of Informatics of the Athens University of Economics and Business (AUEB). She holds a BSc (Informatics) and an MSc (Information Systems) degrees, both from AUEB (Gr). She is currently pursuing her PhD degree; her research interests include security outsourcing, security in AmI, security paradigms, and ICT security education.

Stelios Dritsas (sdritsas@aub.gr) is a Researcher with the Information Security and Critical Infrastructure Protection Research Group at the Dept. of Informatics of the Athens University of Economics and Business (AUEB). He holds a Diploma (Electrical and Computer Engineering) from the Univ. of Patras (Gr) and an MSc (Information Systems) degree from AUEB (Gr). He is currently pursuing his PhD degree; his research interests include privacy enhancing technologies, security ontologies, VoIP systems security, and sensor networks security.

Giannis F. Marias (marias@aub.gr) is a Lecturer (Computer and Network Security) at the Dept. of Informatics of the Athens University of Economics and Business and a Senior Researcher with the Information Security and Critical Infrastructure Protection Research Group at AUEB. He holds a Diploma (Computer Engineering and Informatics) from the Univ. of Patras (Gr) and a PhD (Informatics and Telecommunications) degree from the Univ. of Athens (Gr). His current research interests include privacy enhancement technologies, and trust management in autonomic, wireless, and distributed environments.