Internet of Things (IoT) European Research Cluster Activity Chain

International Framework for IoT Structure and Governance

(CASAGRAS2 Deliverable 4.1 – A Specification of rules and procedures for governance)

Anthony Furness
CASAGRAS2 Technical Coordinator
Technical Director, Smart ID Association (formerly AIM UK)

Establishing an International Framework for IoT Structure and Governance

Contents

1. Introduction

2. Internet Governance and Critical resources for Future Internet and IoT

2.1 Evolutionary considerations

2.2 Critical Infrastructure

2.3 Protection in international law

3. Moving beyond the bounds of Internet Governance

4. Linking IoT Governance to Smart City developments

5. Staged Approach to realising an international framework for IoT Governance

5.1 Preparation of IoT Statement of Purpose and Structure

5.2 Identification of an international IoT Governance Stakeholder Group

5.3 Identification and recruitment of a International (or Global) Legislator and Regional Legislators and the Governing Body

5.4 Legislator/Stakeholder agreement on Regulatory approach

5.5 Legislator/Stakeholder review and agreement on IoT Statement of Structure and Purpose

5.6 Legislator/Stakeholder agreement on an international legal framework

5.7 Legislator/Stakeholder Identification and positioning of trans-governmental networks for IoT Governance and liaison with Internet Governance Developers

5.8 Legislator/Stakeholder development and agreement on governance content requirements

5.9 Legislator/Stakeholder agreement on foundational substantive principles for governance and governance procedures

5.10 Legislator/Stakeholder agreement on infrastructural requirements and policy for on-going consideration

5.11 Legislator/Stakeholder agreement on access to governance procedures and liaison with Internet governance developers

5.12 Legislator/Stakeholder agreement and pursuance of governance and legal agenda on governance requirements

6. IERC Activity Chain for Governance Tasks

Annex 1 - International Framework for Purpose, Structure and Governance of the Internet of Things – Initial Considerations

1. Introduction

An International Framework for Purpose, Structure and Governance of the Internet of Things has been proposed through the CASAGRAS2 project (see Annex 1 - International Framework for Purpose, Structure and Governance of the Internet of Things – Initial Considerations). Primarily, the framework provides the basis for establishing an international foundation for Governance and associated legal underpinning.

The following staged developments are proposed as being necessary for implementing an international framework for Structure and Governance:

1. Preparation of IoT Statements of Purpose and Structure within an initial reference document for defining and setting-up an international body for IoT Governance.

2. Identification of an international IoT Governance Stakeholder Group.

3. Identification and appointment of an International (or Global) Legislator and Regional Legislators and the Governing Body.

4. Legislator/Stakeholder agreement on Regulatory approach – prospectively Self-regulation with subsidiarity (central authority or trans-governmental network having subsidiary function in handling tasks or issues that cannot be handled by the self-regulatory authority) rather than international agreement.

5. Legislator/Stakeholder review and agreement on IoT Statement of Structure and Purpose.

6. Legislator/Stakeholder agreement on international legal framework.

7. Legislator/Stakeholder Identification and positioning of trans-governmental networks for IoT Governance.

8. Legislator/Stakeholder development and agreement on governance content requirements.

9. Legislator/Stakeholder agreement on foundational substantive principles for governance and governance procedures.

10. Legislator/Stakeholder agreement on infrastructural requirements and policy for on-going consideration of infrastructural requirements and attention to robustness, availability, reliability, interoperability, transparency and accountability.

11. Legislator/Stakeholder agreement on access to governance procedures and liaison with Internet governance developers.

12. Legislator/Stakeholder agreement and pursuance of governance and legal agenda on governance requirements.

An essential precursor to pursuing the staged development of an IoT Structure and Governance Framework is an attendant knowledge of the Internet governance. This is required to facilitate a contribution to Internet development per se and to structure an appropriate strategy for collaboration with Internet governance bodies. It is also important as basis for considering parallel and additional issues of governance for the IoT. It is therefore important to review the aspects of governance for the Internet and the critical resources that underpin the success and continued success of the Internet.

2. Internet Governance and Critical resources for Future Internet and IoT

A significant foundation for the review of Internet governance is the report prepared by the Council of Europe Secretariat entitled, "Internet governance and critical internet resources"[1].

Based upon this report in three important areas of consideration can be distinguished, which in turn may form the framework for a more in-depth study of the respective issues and how they may relate to the international framework for structure and governance of the IoT:

1. Evolutionary considerations
2. Critical Infrastructure
3. Protection in international law

In each case there is a need to consider the implications of IoT development in relation to the Internet and Internet-independent networks and with respect to the object-technology base that will facilitate the very important functions of interfacing and interacting with the physical world as well as providing foundational components for applications and services in their own rights, seen as independent or latent IoT. Critical infrastructure constitutes a substantially expanded area of consideration when viewed in relation to the object-connected, object-associated technologies that comprise the foundational components for interfacing and interacting with the physical world.

2.1 Evolutionary considerations

The Internet is essentially viewed as a large, heterogeneous collection of interconnected systems that can be used for communication between connected entities[2]. It has evolved over a period of some years to the point where its ubiquity and facility to impact beneficially upon all aspects of business and domestic life is imposing a critical reliance upon Internet resources and their sustainability. Stability, security and on-going functionality depend upon these resources and how effectively they are managed. Currently these resources, including root name servers, the Domain Name System (DNS), backbone structures and Internet Protocols, are managed by separate agencies and without any overall approach to governance. However, the need for governance is well recognised and a number of Internet-related agencies, although specific in their individual remits, contribute to governance activity. These agencies include[3]:

- **Internet Engineering Task Force** (IETF) – Protocol engineering & development
- **Internet Architecture Board** (IAB) – Overall architecture and advisory body
- **Internet Engineering Steering Group** ((IESG) – Technical management of IETF and Internet standards process
- **Internet Society** (ISOC) - Non-government, international professional membership body – standards, education and policy
- **Internet Corporation for Assigned Names and Numbers** (ICANN) – Responsibility for IP address space allocation, protocol parameter assignment, domain name system management and root server system management functions
- **Internet Research Task Force** (IRTF) – Promote Internet research

[1] Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.
[2] Internet Engineering Task Force (IETF – Mission statement – RFC3935, 2004)
[3] Rappa, M (2010) Managing the Digital Divide – http://digitalenterprise.org/government/gov_text.html

- **World Wide Web Consortium** (W3C) – To develop common protocols that promote Web development and interoperability

Additional to this list is **Internet Commerce Association** (ICA) which, in recent months, has been active in criticising the US Department of Commerce (DOC) over a letter to ICANN's Government Advisory Committee (GAC) regarding provisions concerning new generic top level domains (gTLDs). The nature of the DOC disagreements concerning the gTLD provisions has raised an important issue over the future of gTLDs. "If ICANN's Board were to acquiesce to the positions advanced by the DOC it would not only mark the end of a new gTLD program that envisions an unlimited number of applications and approvals, but the practical end of ICANN as a private sector-led entity in which policy is developed through a bottom-up consensus process"[4]. It would seem that the US government is proposing to convert ICANN into an organisation in which the GAC (which exercises oversight over the ICANN process for developing new gTLD rules) would move from advisory role to a supervisory role with the power of exercising ultimate veto over any new policies being considered by ICANN[5]. This clearly has implications for the Internet development and the development of an Internet-dependent IoT, not only in respect of domains but also in respect of international governance.

Hinging upon an appropriate domain structuring and governance are three primary and burgeoning evolutionary constructs:

1. **Internet of Things (IoT)** – for which this framework proposal is a strategic component in helping to identify a coherent structure for IoT development.
2. **Social Networks and the manifestation of an Internet of Services** – exploiting developments towards an increasingly participative Web (Web 2.0), enhanced automation and the Semantic Web. Each of these developments, particularly automation and the Semantic Web, may be seen to have relevance and positioning with respect to the IoT (see CASAGRAS discussion document, "International Framework for Structure and Governance of the Internet of Things – Initial Considerations").
3. **Technological and Media Convergence onto the Internet** – wherein telephone, television and video technologies are converging onto the Internet, at content level developments in respect of video-on-demand and television over Internet Protocol networks (IPTV) and at the business and service level the integration of Internet, television and telephone services. Again relevance can be seen in each of these areas with respect to the IoT.
4. **Mobile access technologies** – exploiting the increasing range of portable Internet access-supported devices, such as mobile telephones, portable televisions, personal digital assistants (PDAs), portable computers, GPS-supported devices and gaming consoles. Such devices may be considered an integral part of the object-connected or associated edge technologies for supporting IoT applications and services.
5. **Data Transfer Technologies** – responding to the predicted increase in demand in Internet services and associated needs in respect of speed, volume and reliability of data traffic over the net, recognising the potential impact that convergence, mobility and the IoT will have in relation to data traffic and associated architectural needs.

[4] Corwin, P (2011) – on behalf of the Internet Commerce Association, "The ICA Blasts The Department of Commerce Letter to ICANN Committee: "May Mean the End of New gTLDs"" http://www.thedomains.com/2011/02/02/the-ica-blasts-the-department-of-commerce-letter-to-icann-committee-may-mean-the-end-of-new-gtlds/
[5] Ibid

As the Internet evolves still further, with the expectation of escalating growth in connectivity, complexity in structures, technological developments and attendant risks in respect of privacy, security and safety, the need is being seen for more formalised governance, with protection of Internet values and standards on democracy, law and human rights viewed as a priority[6].

2.2 Critical Infrastructure

As far as the Internet is concerned there are a number of critical resources that define the existing infrastructure and areas of consideration for its development. They comprise[7]:

- **Root servers** – essential part of the architecture for providing a stable and secure globally operable Internet, wherein 12 operators running 13 root servers service the underlying domain name system, provide an authoritative directory for ensuring Internet services, answering well over 100,000 queries per second, and take responsibility to maintain adequate hardware, software, network and other associated resources. Presently, the root server operations are performed without any formal relationship with any authority. They have no clearly defined responsibilities and accountability, especially in relation to stability and secure functioning of the Internet. The current geographical distribution of root servers is uneven which in consequence raises issues of significant degraded performance within the area concerned should one of them fail.
- **Backbone structures** – comprising the many different large network structures that are interconnected and serviced by backbone providers, often by individual Internet Service Providers (ISPs). These providers generally supply and handle connection facilities in many cities and are themselves connected to other backbone providers through Internet Exchange Points (IXPs). Only 79 countries around the world have operational IXPs, yet their importance will grow as critical infrastructure as Internet data traffic increases and traditionally-based analogue services are digitised. The IXPs are essentially governed through a mutually-owned membership organisation.
- **Broadband access** – is seen as an important communications enabling technology of international significance in supporting the growth of Internet connections and in promoting developments towards faster access and lower costs of access, both fixed and mobile. Presently there are substantial differences in broadband access among different countries with many factors influencing the take-up and use of broadband which if sustained will create a greater digital divide and prospective information exclusion through lack of access facility. For the future Internet and associated developments broadband may thus be seen a critical resource requiring governments around the world to strengthen still further their programmes for high-speed broadband network proliferation.
- **Network neutrality** – with a move towards bundling of television and Internet services with fixed and mobile telephony concerns are arising over preserving neutrality as it evolves. With associated developments in traffic management techniques there are concerns over anti-competitive practices predicated upon unfairly slowing, prioritising traffic flows and even blocking data flows. Currently, few countries around the world have in place regulations to ensure that access providers exercise a duty to provide neutrality.

[6] Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.
[7] Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.

- **Internet system for names and numbering** – constitutes a critical resource in respect of Internet Protocol address space allocation, protocol identifier assignment, country code and generic Top Level Domain (ccTLD & gTLD) name system management and root server functions. The resource is effectively governed by ICANN.

  As the Internet develops to accommodate the IoT requirements there will be a need to accommodate legacy numbering and identification systems, such as the GS1 numbering systems, electronic product code (EPC) and uCode and the various object identifiers (OIDs) and associated unique item identifiers (UIIs).

Manifest as the Internet these infrastructural components need to be protected in order to ensure security, stability and effective exploitation as a global resource comparable with other global resources such as water and energy[8]. As with other resources the Internet is subject to accidents and incidents that compromise capability and must therefore be protected against such accidents and incidents, and appropriate to user needs and human rights. Similarly, the IoT will reveal other infrastructural components that will also require protection, particularly in respect to autonomous and self-functionality, such as self-diagnosis, self-repair and self-defence against infrastructural attacks.

2.3 Protection in international law

In recognising the Internet as a critical resource there is an intrinsic need to protect the resource in much the same way that other critical resources may be protected. Being an international resource it also follows that it requires an international cooperative approach to protection using international law. The protection is in part grounded in accountability which in turn requires a legal framework for providing regulations and sanctions to handle non-compliance with accountability requirements.

The nature of the entities for protection is required relate to:

- **Technical risks**, to both accidental and intentional incidents resulting in damage to the infrastructure of the Internet or detrimental trans-boundary effects upon the Internet.
- **Cyber attacks**, characterised by deliberate attempts to disrupt or damage Internet functions, services and applications.
- **Inter-state conflict**, characterised by issues arising during times of crisis in terms of stability and security within a country relating to important resources. While protection can be seen as requirement under such circumstances it is likely that this will not be ensured through international law. Consequently, other measures are almost certainly required to facilitate protection in those situations in which conflict cannot be resolved through process of law.

These issues are not mutually exclusive and each have a bearing upon the stability, security and safety of the IoT as well as the Internet per se, potentially to the extent that additional protection measures may be required.

In all these areas concerning the Internet and Internet governance and there relevance to IoT there is a need to delve more deeply into their nature and possible impact upon the governance of the IoT. The critical resources that characterise the Internet must be borne in

[8] Council of Europe (2009) Internet governance and critical internet resources, Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, April 2009.

mind in pursuing the proposed staged approach to structuring a framework for IoT Structure and Governance.

3. Moving beyond the bounds of Internet Governance

Because of the IoT imperative for interfacing and interacting with the physical world there will be aspects of critical infrastructure that arguably go beyond the bounds of what is considered Internet governance, particularly in relation to:

- Implementation, maintenance and development of the IoT physical world infrastructure (Internet linked or Internet-independent) characterised by object-connected and other the other edge-technologies that are used to interface and interact with physical world entities and systems, including wireless sensor networks and control systems.
- Environmental disruption and impact associated with deployment and maintenance of fixed position IoT object-connected devices, systems and networks, and the end-of-life recycling or disposal of devices, systems and networks; exacerbated by an expected exponential growth in use of object-connected and other edge-technology devices.
- Environmental and societal impact of mobile devices and fixed in-mobile devices and networks such as in-car engine and other management systems.
- Attendant implications of extensive populations of object-connected and integrated system devices and networks with respect to functionality, reliability, safety and responsible deployment and use of such devices and networks.
- Energy and materials conservation including the control and recycling of object-connected and other physical edge-technology e-waste.
- Privacy (including corporate privacy) and security associated with object-connected data or information contained in object-connected and other edge-technology devices, additional to those characterised by radio frequency identification (RFID) and including optical-based data carriers, smart card devices, mobile phones, tablet media devices and so forth.
- Privacy (including corporate privacy) and security of communications between object-connected and other edge-technology devices and data transfer systems.
- Security of infrastructure, applications and services, particularly in relation to autonomous systems communications and functionality where current Internet capabilities may be viewed as inadequate.
- Functionality and performance demands in relation to physical world interaction that may be beyond the capabilities of existing Internet support, particularly where critical safety and critical business functions may be put at risk and where latencies, delays, loss of synchronisation and issues of temporal decomposition may impose problems.
- Accommodation of Internet-independent network and communication structures and prospects of new infrastructural developments that are IP-independent and exploiting the physical world interfacing and interaction capabilities of object-connected and other edge-technologies.
- Standards and regulatory recognition and developments to accommodate the broader based vision of the IoT and its significant object-connected and other edge-technology base.

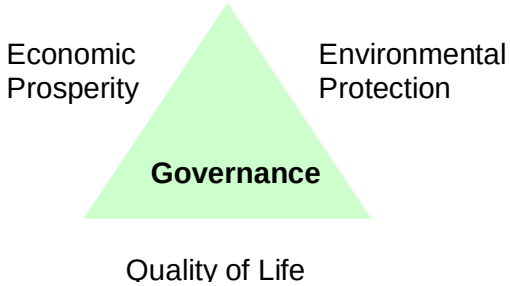
Ethical and issues of responsible usage of resources will also need to be addressed in the governance arena. The often promoted notion of every object being connected to the IoT is

not only ludicrous but irresponsible in principle. Only objects that need to be connected should be connected and ostensibly only when required to be connected. Unnecessary object connectivity must clearly be seen as a drain on material resources and energy, particularly if numbers are of an astronomical scale.

4. Linking IoT Governance to Smart City developments

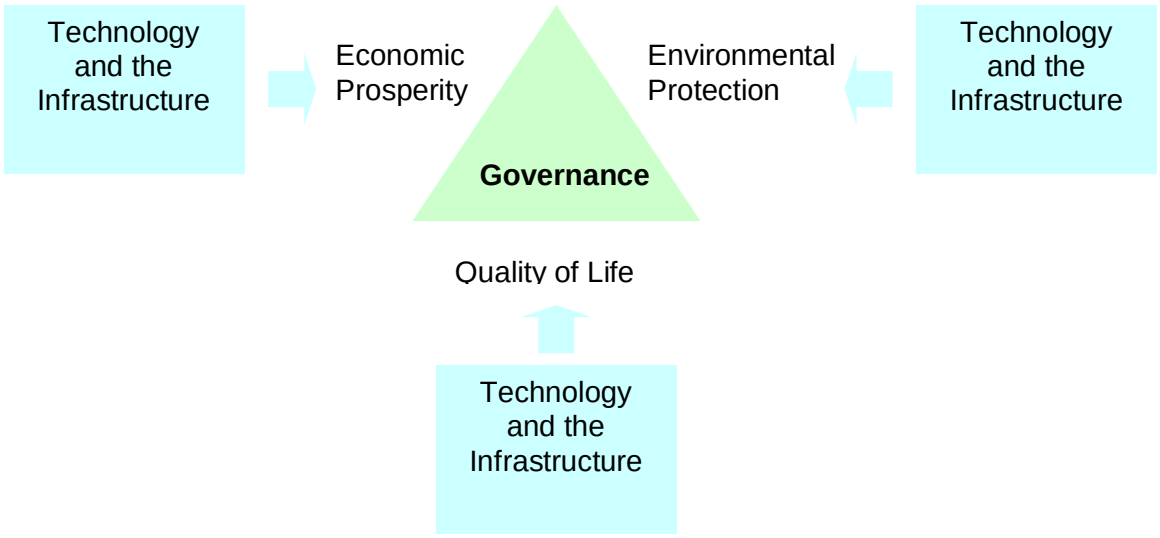
An important manifestation of IoT development will be in the realisation of 'Smart' cities. Such developments are inevitable, with growth in city populations (with the tipping point in urbanisation being reached in 2009[9]) and developments already being seen through the roll out of broadband to the community and applications exploiting mobile communications. To exploit the digital capability to the full, bearing in mind too the continuingly changing landscape for digital products and innovation, it is important to take a strategic approach to the design and realization of smart city infrastructure. It is also important to align such an inclusive model and 'smart' developments with a well-founded socio-economic and governance paradigm for city development. Such a paradigm is to be found in the Hazel model[10].

The Hazel report, which focused upon the infrastructure of megacities – cities that account for a disproportionately high share of national economic growth and generate a significant percentage of global gross domestic product (GDP), was based upon a survey of 525 city leaders (politicians and decision makers). It yielded a theory of city governance predicated upon three commanding considerations; quality of life, economic prosperity, and environmental protection.



Governance was seen as the means of balancing these three functional goals. Such a model has significant links to infrastructural developments that exploit technology for achieving socio-economic goals. Such a model may also be argued to have significance with respect to smaller city complexes and city regions in providing a governing oversight with respect to technological intervention with respect to infrastructure, and its potential with respect to economic power, interlinking with the global economy and attraction for investment. Technology can and will impact on all aspects of city infrastructure and with outcomes determined by the governance model.

[9] United Nations report (2009)
[10] Prof George Hazel report entitled "Megacity Challenges", MRC McLean Hazel Consultancy.



In the drive towards smart digital cities there will be an inevitable social backlash, pointing to the limitations and detrimental impact that such change can engender. Where personal identification and data is concerned there is often fear of the unknown. Appropriate design and protection measures, derived under appropriate governance, can allay such fears. Without such protection measure we would not now be exploiting the ubiquity of smart cards and other carriers of personal identity and activities such as on-line financial transactions; protection that will be enhanced as further technological measures are introduced to combat identity theft.

Putting aside for the moment the social issues, the concept for an inclusive model for digital cities can be summarised in a framework that:

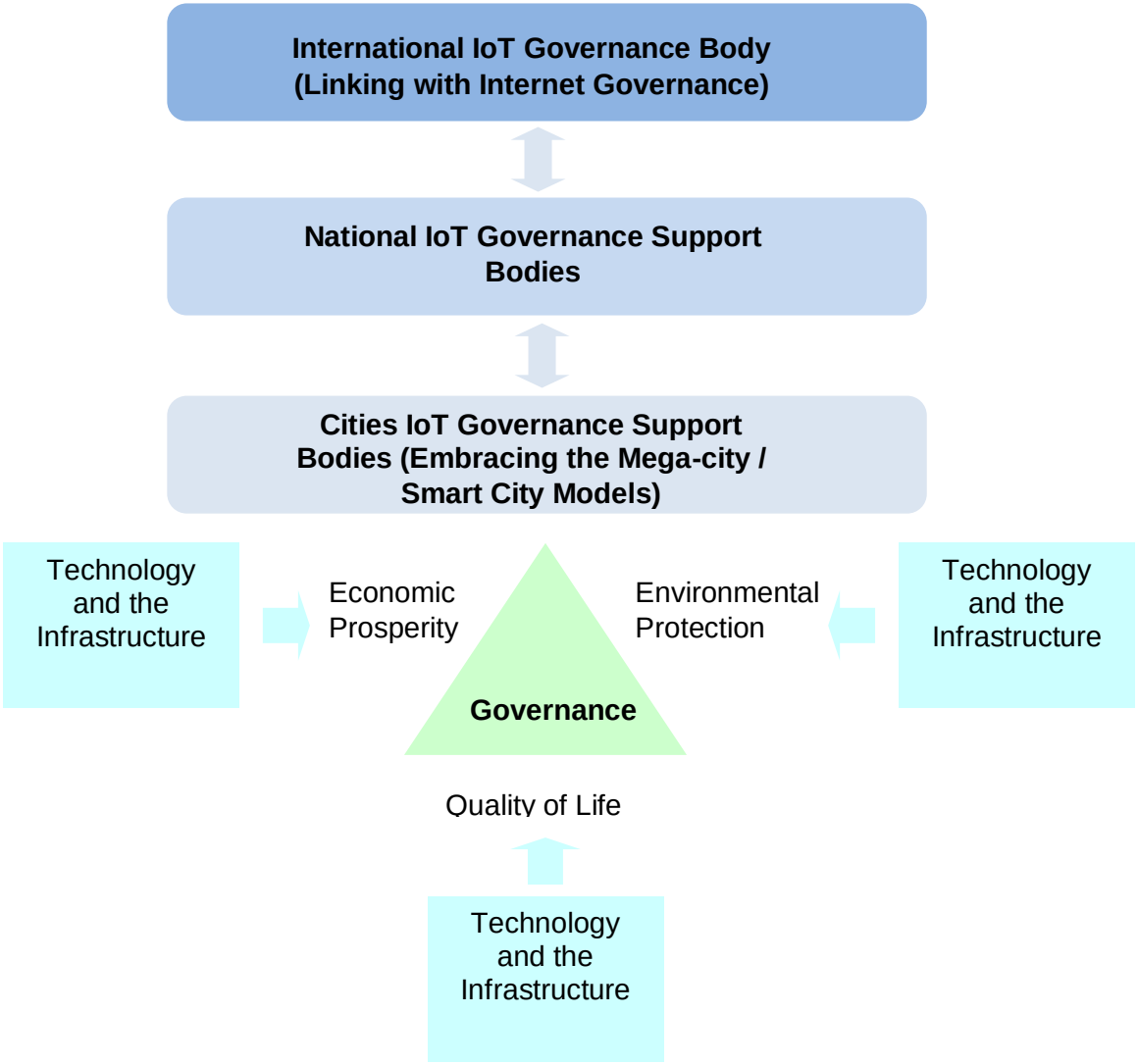
1. Distinguishes the various components of the physical city infrastructure (buildings, roads, underground facilities and so forth) on or in which digital technologies can be exploited to serve the city complex and its organisational and social support components of the infrastructure.
2. Distinguishes the communications and physical resourcing and utility structures that support city life that can benefit from digital intervention and innovation.
3. Distinguishes the infrastructure for security, surveillance and emergency services.
4. Distinguishes communications infrastructure and public support hubs, and very significantly the role and impact of Internet-enabled services.
5. Distinguishes the various components of mobility within and between city infrastructures that can benefit from digital intervention and innovation.
6. Distinguishes the various components of city functionality and city services that can benefit from digital intervention and innovation.
7. Distinguishes the various dimensions of digital intervention for identification, data and information exchange, location and positioning, timing, sensing, actuation and control.
8. Distinguishes an extendable framework of technology drivers for implementing digital developments.
9. Distinguishes a standardisation framework for facilitating the needs for interoperability and scalability in city developments and inter-city integration and communications.

10. Distinguishes a progressive strategic agenda for determining city needs that could benefit from digital intervention and innovation, including those of a socio-economic nature.

This ten point framework, along with a governance model, can form the basis for positioning and considering open innovation proposals for future IoT-enabled services in “smart” cities.

The governance model seeks to assure that applications and services, be they Internet-based, IoT-based or other provision, contribute to the prosperity, protection and quality of life. By applying the model to the considerations of Internet- or IoT-enabled services, confidence may be gained in their relevance to city requirements and city acceptance, the rationale being how a proposed service or services relate to the three areas of governance concerned.

The Smart City governance may be seen to link to IoT governance through national IoT governance supporting bodies, the overall framework being as depicted below.



5. Staged Approach to realising an international framework for IoT Governance

To accommodate the wide ranging needs associated with an international framework for governance that contrast and yet integrates with Internet governance requires a careful staged approach to its formation. This staged approach proposal, and the associated requirements for completing each stage, are summarised as follows, together with the liaison and work requirements to be undertaken to realise the objectives for each stage.

5.1 Preparation of IoT Statement of Purpose and Structure

These statements are seen as forming an initial reference document for developing international framework for IoT Governance, wherein the statements are appropriately qualified to explain scope and meaning of any potentially ambiguous terms that may be used. For developing such statements the following constructs are offered as starting points:

- **Purpose of Internet of Things** (Based upon the foundational imperatives of Internet support and interfacing and interaction with the physical world) –

  The purpose of the IoT may be considered to be the exploitation of the existing and future capabilities to interface and interact with physical objects of any kind, animate or inanimate, through automatic identification and object-connected technologies and, through Internet and other computer, communications and network developments, derive and apply applications and services that serve the international economic community, knowledge and wealth creation, and the increased welfare and well being of human kind.

- **Statement of Structure for the Internet of Things** (Based upon the foundational imperatives of Internet support and interfacing and interaction with the physical world) -

  An integrated, internationally agreed and standards-supported network, communications, interface and actuation structure that exploits the existing and future Internet, existing and future fixed and mobile telecommunications systems, existing and future object-connected technologies, coupled prospectively with non-Internet private networks and associated communication, interface and actuation structures, organised to facilitate development of application and service layers specific to physical world, object-oriented, needs and opportunities relating to the identified purpose for the Internet of Things.

  Object-connected technologies are those technologies that are embedded-in, attached-to, accompany or are associated with tangible physical entities of any kind and facilitate identification of the objects concerned together with other data capture and actuation functionality as appropriate for interfacing and interaction with said objects and as appropriate the environment in which they are situated. Automatic data capture, sensing, positioning and communication technologies are representative in this respect.

It is necessary for projects represented in the European Research Cluster for the Internet of Things (IERC) Activity Chain model to respond and contribute to the development of framework statements prior to presenting them for consideration by international partners. This process will apply to other stages in the framework development process and will therefore require Activity Chain projects to nominate contacts to facilitate the collaboration.

5.2 Identification of an international IoT Governance Stakeholder Group

Appropriate identification and representation of stakeholders are important requirements for realising both an effective governance body and a body to liaise with the Internet governing bodies. In terms of sector representation the Working Group for Internet Governance (WGIG) identify three stakeholder sectors:

- **Government** - geared towards creating an environment for encouraging developments in ICT and development, as appropriate, of laws, regulations and standards, to foster the exchange of best practices and engage in oversight functions.
- **Private sector** – geared to promoting industry self-regulation and the exchange of best practices, developing policy proposals, guidelines and tools for policy makers and participation in national law making and fostering of innovation through its own research and development.
- **Civil society** – geared to mobilizing and engaging in democratic and policy processes, network building and consideration of other views.

The World Summit of the Information Society (WSIS) has indicated a slightly different sector identification (implied in Article 49 of the WSIS declaration), with the addition of a fourth sector embracing international organisations. Here the sectors are recognized as:

- **States** - as agents for policy authority for Internet-related public policy issues (including international aspects).
- **Private sector** – geared to the development of the Internet, both the technical and economic fields.
- **Civil society** – geared to dealing with Internet matters, especially at community level, intergovernmental organisations and the coordination of Internet-related public policy issues.
- **International organisations** – geared to the development of the Internet-related standards and relevant polices.

For the purposes of IoT governance the four sector model, coupled with the gearing identified in the WGIG delineation of stakeholders, may be considered more appropriate, particularly if the scope of IoT development embraces both Internet and Internet independent components as suggested in the CASAGRAS2 discussion paper (Annex 1) – “International Framework for Structure and Governance of the Internet of Things – Initial Considerations”. The prospect may also be seen for reformatting specific roles within these sectors. With significant corporate developments being seen in large international organisations with respect to ‘smart cities’, ‘smart planet’ and other smart-based developments significant prospects may be seen for an Internet-parallel network-of-networks as part of the IoT vision. This being so the role of the private sector and international organisations will assume even greater prominence in IoT governance.

Within the four-layer model for stakeholders the States and Civil Society representatives will undoubtedly assume increasing importance in dealing with physical world infrastructural matters and associated matters, addressed earlier, concerning:

- Implementation, maintenance and development of the IoT physical world infrastructure.
- Environmental disruption and impact associated with deployment and maintenance of fixed position IoT object-connected devices, systems and networks, and the end-

of-life recycling or disposal of devices, systems and networks; exacerbated by an expected exponential growth in use of object-connected and other edge-technology devices.

- Environmental and societal impact of mobile devices and fixed in-mobile devices and networks in transport structures.
- Attendant implications of extensive populations of object-connected and integrated system devices and networks with respect to functionality, reliability, safety and responsible deployment and use of such devices and networks.
- Energy and materials conservation including the control and recycling of object-connected e-waste.
- Privacy (including corporate privacy) and security associated with object-connected data or information contained in object-connected devices and communications between object-connected devices and data transfer systems.
- Security of infrastructure, applications and services, particularly in relation to autonomous systems communications and functionality.
- Functionality and performance demands in relation to physical world interaction.
- Standards and regulatory recognition and developments to accommodate the broader based vision of the IoT.
- Accommodation of Internet-independent network and communication structures and prospects of new IP-independent infrastructural developments.

As part of the requirements for identifying any of the stakeholders the need must be seen for determining the responsibilities and accountability of stakeholders.

There are clearly some important issues concerning structure, roles, responsibilities and accountabilities to be considered in formulating the stakeholder group for IoT governance that need to be addressed within the IERC Activity Chain and the international forum to be set up by IoT-i in collaboration with CASAGRAS2. The physical world infrastructural matters and associated matters listed above will not only require consideration from a stakeholder standpoint, but also consideration as components of content within the governance agenda.

5.3 Identification and recruitment of a International (or Global) Legislator and Regional Legislators and the Governing Body

While the term legislator has intrinsic legal implications, the prospective roles of international and regional legislators may be proposed to have a broader meaning in relation to governance and regulation. However, it must be seen as an important component in establishing an international legal framework. For an international development of the size envisaged for the IoT the international legislative role will need to be an organisation that is knowledgeable of IoT developments and Internet governance. This would suggest an existing organisation rather than a new organisation, albeit that the form and function of the IoT is not as yet completely defined. Suggestions[11] being proposed for the role of International Legislator include the World Trade Organisation (WTO) and the Organisation for Economic Co-operation and Development (OECD). However, the need can be seen for further research and consideration of the International Legislative role, eligibility requirements and prospective contenders. Similarly, the Regional Legislators, with

[11] Weber, R H (2011, Accountability in the Internet of Things, Computer Law & Security Review, 27 (2011) 133-138.

consideration as to what would constitute a regional entity, continental or by country, for example.

In specifying the need for an International Legislator the question arises as to its relation to the Governing Body. It seems logical that the organisation providing the international legislative role should feature significantly in the Governance process, along with regional legislators and Stakeholders. It also raises questions of costs and funding formula for such a body.

The issues concerned here for international and regional legislators are such that it requires informed expert attention to define roles and eligibility requirements. Ideally it requires expertise that spans the technical, governance and legal issues relating to the IoT. From a technical and international standpoint the need can be seen for considering IERC Activity Chain input to the derivation of roles and suggestions for fulfilling the international and regional Legislator requirements. Suggestions may also be presented for the formation of the Governing Body and the funding strategy required to support its formation, functionality and sustainability.

5.4 Legislator/Stakeholder agreement on Regulatory approach

The regulatory approach to IoT governance is seen as a matter for Legislator and stakeholder agreement. However, in drawing upon collective wisdom on governance, suggestions may be made for such an approach. Self-regulation with subsidiarity (central authority or trans-governmental network having subsidiary function in handling tasks or issues that cannot be handled by the self-regulatory authority) is perhaps seen as a logical choice. A possible alternative would be by international agreement, but would probably be rejected in preference for self-regulation, because of the often protracted nature and long time intervals for achieving and applying such agreements.

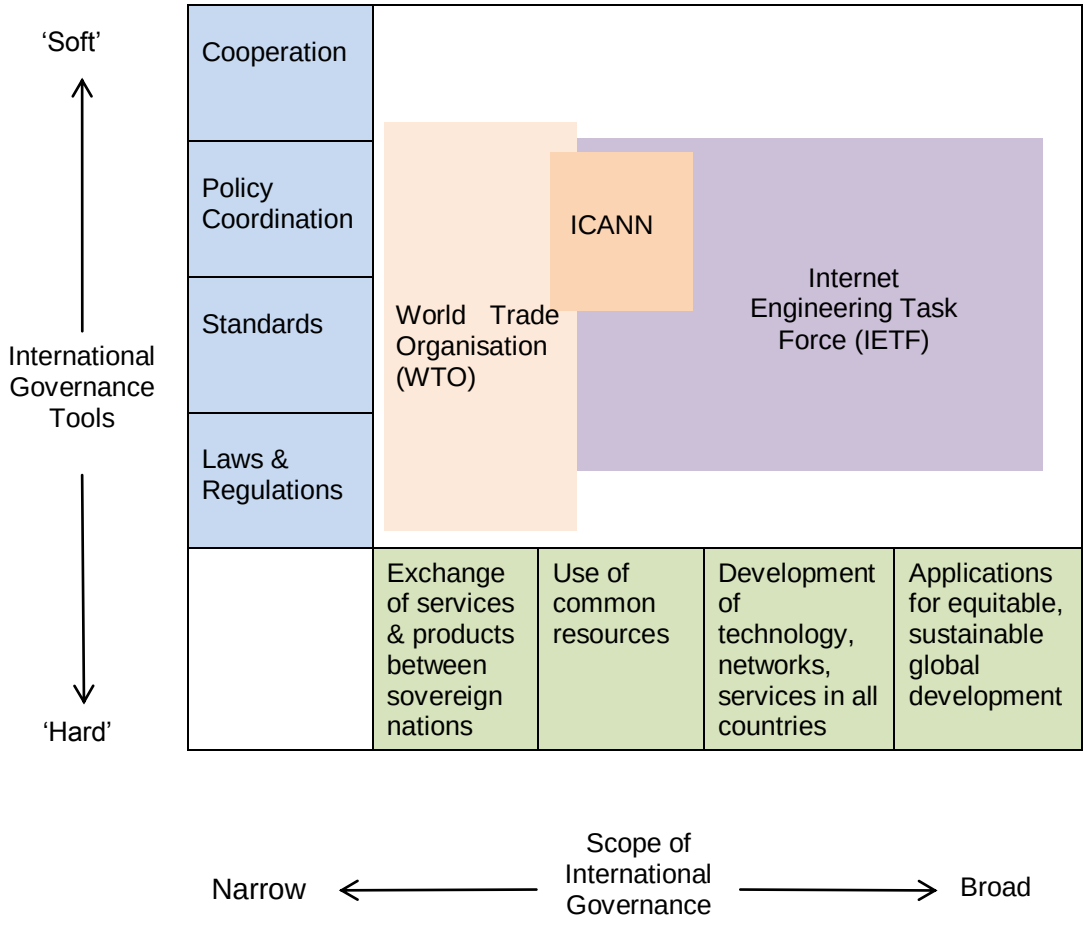
While the regulatory approach is a matter for agreement at the Legislator/Stakeholder level suggestions may be provided to assist in this process, Together the Legislators and Stakeholders, or representatives there of, will form the principal part of the Governing Body for the IoT and as such will implement the regulatory processes and procedures. The IERC Activity Chain may assist in suggesting a regulatory approach, processes and procedures along these lines and in so doing inject the necessary expertise in IoT developmental matters.

Rules for Governance - In looking at the rules for governance it is useful to delineate:

1. Those required for effecting governance within the governance body and its affiliated links, in the case of IoT extending to grass-roots national and city governance.
2. Those that relate to content and in particular to operational aspects of governance and relating to structural matters.

Rules in this context are viewed as regulations or principles governing conduct or procedure within a particular area of activity. In both cases the specification of actual rules are seen as the responsibility of the governing body. However, in considering the scope of such rules it is useful to consider the model presented by MacLean[12] in respect of legal quality of regulations (soft to hard law) and the scope of international governance (narrow to broad) as depicted in the schematic presented below. It is also useful for positioning organisations in respect of these two determining dimensions.

[12] Cited in Weber, R (2009), Shaping Internet Governance: Regulatory Challenges, Springer.



After MacLean, cited in Weber, R (2009)

The 'mapping' space on this schematic simply depicts three organisations are their relative coverage of the dimensional elements, with the World Trade Organisation covering most of the governance tools in relation to exchange of services and products between sovereign states, whereas the IETF covers policy coordination and standards with respect to broader aspects of governance.

Clearly, as far as the IoT is concerned the required tools for governance must embrace the needs in respect of cooperation, policy, coordination, standards and laws and regulations. So too in respect of scope and the need to embrace exchange of services and products, use of common resources, development of technologies, networks and services, and applications for equitable, sustainable global development. Ideally, for a global legislator for IoT, the organisation concerned should fill the mapping space. In the absence of such an organisation the prospect may be seen for strong linkage with the IEFF and possibly with the WTO. These are essentially matters to be decided by an IoT governance task force with appropriate international representation.

5.5 Legislator/Stakeholder review and agreement on IoT Statement of Structure and Purpose

With a Governing Body in place it will be necessary to establish a frame of reference for IoT through the statements of Purpose and Structure. It is therefore essential that these statements are well founded, clearly and unambiguously stated and present the overall vision of the IoT. They must also have a precision that assist the development of an associated legal framework for underpinning governance.

The IERC Activity Chain has a role in developing these statements as a foundation for IoT governance. It may also be seen to require a multi-disciplinary input to the development to ensure an appropriate balance of technical and societal reach.

5.6 Legislator/Stakeholder agreement on an international legal framework

There are many aspects to defining an international legal framework for the IoT (see CASAGRAS2 Briefing Statement 4 – Structure & Governance), including the basis upon which various governance instruments are formulated. Parallels may be drawn with the legal aspects of Internet Governance wherein[13] attention may be directed to:

- **Legal issues** *per se*, including cybercrime, intellectual property rights, data protection, privacy rights, and consumer rights;
- **Legal mechanisms** for addressing Internet governance issues, including self-regulation, international treatise, and jurisdiction"
- **Cyberlaw vs Real Law** – WSIS/WGIG discussions emphasise the need to use existing national and international legal mechanisms for regulating the Internet.
- **Global regulation** – while desirable in many aspects, national and regional regulations are assuming greater relevance.
- **Variable geometry approach to governance** – recognising it as a method of differentiated integration which acknowledges differences within the integration structure and separation between integration units.
- **Differences between International Public Law and International Private law** – recognising the significance of public law in the context of Internet governance.
- **Harmonisation of National Laws** – supporting the need for global regulation, resulting in one set of equivalent rules at global level
- **Elements of International Public Law** – that could be effectively applied to Internet and IoT governance, including:
    - Treaties and conventions
    - Customary law
    - Soft law – frequently encountered in governance debate

Soft Law may be seen as a useful vehicle for deriving instruments for governance. While it refers to quasi-legal instruments, which are not legally binding or otherwise somewhat "weaker" than the binding force of traditional law, soft law is generally associated with international law and used to assist in deriving:

- Resolutions and Declarations
- Statements, principles, codes of conduct, codes of practice often found as part of framework treaties;
- Action plans
- Non-treaty obligations

Soft Law would also appear to have some additional benefits in formulating international contributions to legal framework proposals, including:

- **Not legally binding** – cannot be enforced through international courts or other

[13] Kurbalija, J Internet Governance and International Law in Reforming Internet Governance: Perspectives from WGIG, 106-115

dispute resolution mechanisms

- **Contain principles and norms rather than specific rules** – usually found in international documents such as declarations, guidelines and model laws
- **Used for building** mutual confidence, stimulating progress, introducing new legal and governmental mechanisms
- **Less formal approach,** not requiring official commitment of states, reducing potential policy risks
- **Flexible**, enough to facilitate the testing of new approaches and adjustment to rapid developments
- **Greater opportunity for multi-stakeholder approach** than does an international legal approach restricted to states and international organisations

While these features may give some direction towards formulating an international legal framework for IoT it has to be recognised that it is a specialist legal task to complete such a framework. Ideally it requires expertise that spans the technical, governance and legal issues relating to the IoT. From a technical and international standpoint the need can be seen for considering IERC Activity Chain input to the derivation of the legal framework.

5.7 Legislator/Stakeholder Identification and positioning of trans-governmental networks for IoT Governance and liaison with Internet Governance Developers

In developing the IoT the prospect may be seen for the establishment of trans-governmental networks tasked with dealing with IoT matters and promotion at the governmental level, including input into governance. A role may therefore be seen for Legislators and Stakeholders (or more formally the IoT Governing Body) identifying and positioning trans-governmental networks for IoT in the strategy for IoT governance.

The IERC Activity Chain may assist in helping to define the role and networking capability of these trans-governmental networks.

5.8 Legislator/Stakeholder development and agreement on governance content requirements

In considering the requirements for IoT Governance and how it differs or could differ from Internet governance, content is clearly a critical distinguishing factor requiring careful attention to what is required. While it may be considered that governance is more about the operation and usage of the network than its structure, aspects of structure will naturally have a bearing upon governance issues. Structural and operation issues are therefore important aspects of governance content and may be usefully considered in relation to technical, economic, institutional, policy and legal perspectives[14]. The items of content viewed in relation to technical, economic, institutional, policy and legal perspectives provide the basis for a matrix approach to presenting and considering content for governance (see Annex 1 - CASAGRAS2 discussion paper – "International Framework for Structure and Governance of the Internet of Things – Initial Considerations"). It is also dynamic in the sense that content can be added and considered as appropriate to IoT developments.

Aspects of governance relating to structure will draw upon the items listed above in respect of stakeholder considerations and include:

[14] Kurbalija, J Internet Governance and International Law in Reforming Internet Governance: Perspectives from WGIG, 106-115

- Physical world object-connected infrastructure for IoT, and associated policy and provisions
- Security policy and provisions
- Safety policy and provisions
- Energy conservation policy and provisions
- Regulatory policy and provisions
- Standardisation policy and provisions

Aspects of governance relating to operational and usage will include:

- Physical world deployment, maintenance and usage of object-connected technologies and associated policy and provisions
- Accommodation of object-connected e-waste and recycling and associated resource management
- Environmental disruption, impact and management policy and provisions
- Global Numbering issues and Resolver schemes for identification and discovery
- Social Capital, Privacy, Security and Identity management policy and provisions
- Ethical and user protection policy and provisions
- Cyber-crime protection policy and provisions
- Intellectual Property protection policy
- Performance Indicators, rules and norms for IoT operation
- Developmental policy

The matrix approach may be considered a useful tool for assisting Legislators and Stakeholders in identifying and considering content for governance and the IERC Activity Chain may assist in structuring an initial matrix of content viewed in relation to technical, economic, institutional, policy and legal perspectives.

5.9 Legislator/Stakeholder agreement on foundational substantive principles for governance and governance procedures

In determining the foundational substantive principles for IoT governance and governance procedures it is clearly sensible to consider those being applied for Internet governance. This aligns with the need identified above for collaboration with Internet Governance developers. However, it is also important to consider particular needs in relation to IoT structure and functionality, and the very important issues concerning physical world infrastructure for the IoT.

In recognising the importance of Internet governance in respect of principles and procedures it important from an IoT perspective to list, describe and consider their significance in relation to IoT development and governance requirements. This is a precursory activity that could be fulfilled within the IERC Activity Chain to assist Legislators and Stakeholders in pursuing their roles in governance.

5.10 Legislator/Stakeholder agreement on infrastructural requirements and policy for on-going consideration

IoT infrastructure and associated policy for on-going consideration of IoT infrastructural developments is a significant governance requirement with a need to address robustness, availability, reliability, interoperability, transparency and accountability. The technical nature of these requirements demands appropriate technical support.

This is a further precursory activity that could be fulfilled within the IERC Activity Chain to assist Legislators and Stakeholders in pursuing their roles in governance.

5.11 Legislator/Stakeholder agreement on access to governance procedures and liaison with Internet governance developers

In recognising the Internet as one of the foundational imperatives for the IoT it is essential that any Governing Body for the IoT liaises effectively with organisations influencing Internet Governance. A number of such organisations exist, with varying responsibilities for Internet development and associated governance, including:

- **Internet Engineering Task Force** (IETF)
- **Internet Architecture Board** (IAB)
- **Internet Engineering Steering Group (**(IESG)
- **Internet Society** (ISOC)
- **Internet Corporation for Assigned Names and Numbers** (ICANN)
- **Internet Research Task Force** (IRTF)
- **Internet Commerce Association** (ICA)
- **World Wide Web Consortium** (W3C)

While not an exhaustive list it is representative of the significant effort and areas of influence upon Internet governance.

The need may be seen for deriving a strategy and hierarchical approach to implementing collaboration and cooperation for governance purposes. An incisive study may be required to best determine the role of each of these influential bodies and the best way to effect the collaborative role, ideally in a synergistic way. The multi-disciplinary nature of these Internet groups suggests the need for trans-project considerations within and across the IERC Activity Chains.

5.12 Legislator/Stakeholder agreement and pursuance of governance and legal agenda on governance requirements

The manner in which governance is pursued and in which collaboration is achieved with Internet governance bodies is an important consideration for which a strategic agenda is required. Each must be well founded from a legal perspective and agreed from an international stakeholder standpoint. Again the need can be seen for considering the approach that is adopted in pursuing Internet governance. As far as the legal agenda is concerned that must be seen as a specialist legal activity requiring appropriate legal expertise.

Deriving an account of Internet governance procedures may be considered a further precursory activity that could be fulfilled within the IERC Activity Chain to assist Legislators and Stakeholders in pursuing their roles in governance.

6. IERC Activity Chain for Governance Tasks

Given this starting point for proposing an international framework for Structure and Governance the request is for IERC Activity Chain representatives to consider and contribute to any changes in the proposal and once consensus is achieved to participate in undertaking the declared IERC Activity Chain tasks in taking the framework forward.

Anthony Furness

Technical Coordinator
CASAGRAS2

Annex 1 - International Framework for Purpose, Structure and Governance of the Internet of Things – Initial Considerations

Anthony Furness
Technical Coordinator CASAGRAS2

Preamble

The Internet of Things (IoT) is a concept relating to the existing and future Internet, but has the prospect of going beyond the bounds of the current Internet concept. It is a concept that is attracting attention throughout the world. However, there are numerous definitions and interpretations and for which there is corresponding confusion and fuzziness as what the IoT is in real terms. This fuzziness is leading to islands of applications and value propositions, but without any coherent framework to underpin the IoT development as a cohesive, internationally agreed paradigm having global economic significance. While these islands of application may exhibit technological innovation and demonstrate economic benefit in their own right they may do little to contribute to a coherent global paradigm and the potential it could offer. Moreover, disparate, incidental developments of this kind are likely to precipitate problems of interoperability and contention that could also inhibit the development of a truly global, internationally supported structure for the IoT.

Without an internationally accepted framework for the IoT the considerable European programme of research and support is also in danger of degenerating into a less than effective force in influencing the global dimensions demanded of such a concept. The need for global discussion on realising an adequate global system for IoT governance has been recognised as a means of avoiding "the emergence of market-driven new monopoly with unintended negative political, economic, commercial and social effects"[15].

An international framework for purpose, structure and governance is required to facilitate the development and realisation of the IoT. Advantage may also be seen in accepting the need for a legal framework based upon 'soft law' formulations derived potentially through self-regulation. It is a framework that must accommodate the future and the scope that may be derived by considering the unequivocal imperatives that are currently clouded in their interpretation by the myriad developments that are being purported to constitute or be part of the IoT. The wide ranging definitions for IoT add to the confusion and it is only in considering the unequivocal imperatives for IoT and where they may lead that a clearer proposition for IoT can be derived.

Having considered the deficiencies and fuzziness associated with definitions for the IoT CASAGRAS2 is proposing as a matter of urgency an outline framework description for purpose, structure and governance, as a basis for discussion among international partners and stakeholders. It is also seen as a platform for establishing the precursory collaborative and legal framework for development of an international Governance and liaison body. The starting point in deriving the international framework is to establish statements of purpose, structure and governance based upon the foundational truths or imperatives.

Foundational Imperatives for the Internet of Things

Two unequivocal imperatives present themselves as the basis for the Internet of Things (IoT):

1. Integration within the existing and future Internet

[15] Santucci, G (2011) The Intenernet of Things: The Way Ahead, in "Internet of Things – Global Technological and Societal trends" (Editors: Ovidiu Vermesan & Peter Friess), River Publishers.

2. Interfacing and interaction with the physical world through object-connected technologies and electronically accessible identifiers

They underpin the purpose of the IoT and the framework criteria for distinguishing IoT Applications and Services.

Purpose of Internet of Things

Given the foundational imperatives stated above, the purpose of the IoT may be considered to be **'The exploitation of the existing and future capabilities to interface and interact with physical objects of any kind, animate or inanimate, through automatic identification and object-connected technologies[16] and, through Internet and other computer, communications and network developments, derive and apply applications and services that serve the international economic community, knowledge and wealth creation, and the increased welfare and well being of human kind'.**

The generalised nature of the statement allows for future influences of technological change and response to developments that may change the detailed nature of supporting structures and protocols, whilst retaining a cohesive conceptual framework that embodies the vision of an object-focused and responsible use of object-connectivity.

Underpinning for a Statement of Structure

The statement of structure for the IoT, given the above imperatives and statement of purpose, has to be based upon a detailed review of the imperatives, and the implications and opportunities they present. With the Internet being viewed as the core of the IoT development it is clearly important to view the capabilities it presents for linking with the second imperative of interfacing and interacting with the physical world. In performing such a review it is also important to consider how the second imperative may also relate to new and parallel dimensions in network-of-network developments that could, in principle at least, lead to a bifurcated or multi-faceted Internet-independent or IP-independent structures for the IoT.

The Internet as a vehicle for the IoT – The Internet is generally viewed as a large, heterogeneous collection of interconnected systems that can be used for communication between connected entities[17], comprising:

- **Core Internet** – Internet Service Provider (ISP) networks
- **Edge Internet** – Corporate and private networks, often connected via Firewalls, application layer gateways and similar devices

Conventionally, the connected entities within the Internet are computers with human-computer interfacing and, increasing numbers, computer supported entities such as portable data terminals and embedded data capture and sensor terminals. The former can be seen as a human-to-human platform for IoT distinguished applications and services and the latter to object-to-object and object-to-human platforms for IoT applications and services. Thus,

[16] Object-connected technologies are those technologies that are embedded-in, attached-to, accompany or interact to derive data or information concerning the object itself (image capture, speech recognition and natural features, such as fibre patterns, for example), the objects being tangible physical entities of any kind.
[17] Internet Engineering Task Force (IETF – Mission statement – RFC3935, 2004)

the Internet can be seen to provide an existing platform for IoT development based upon the imperative of interfacing and interacting with the physical world. In order to extend and distinguish the IoT beyond being simply part of the existing Internet it is necessary to determine:

1. The extent to which the Internet capability can embrace further computer-based nodes that interface and interact with the physical world.
2. The extent and the implications of interfacing further with physical objects of all kinds through object-connected technologies and as a basis for supporting Internet-enabled applications and services.
3. The extent to which the Internet application layer components, such as the world wide web, can be exploited and extended to accommodate IoT applications and services.
4. The extent to which legacy automatic identification coding can be resolved to link with Internet Protocol (IP) addressing and discovery services.
5. The extent to which the existing and future Internet capabilities can support the growth and diversity in IoT communication and transfer needs, commensurate too with needs in performance.
6. The extent to which structures will serve activation and control needs within the physical world and accommodate important legacy systems, such as the supervisory control and data acquisition (SCADA) and distributed control systems (DCS) that have served, and continue to serve industry and the needs for automation.
7. The extent to which physical identifiers will relate to virtual identifiers and virtual entities.
8. The extent to which security, privacy and consumer needs will need to be enhanced to serve new and automatic systems for IoT support.

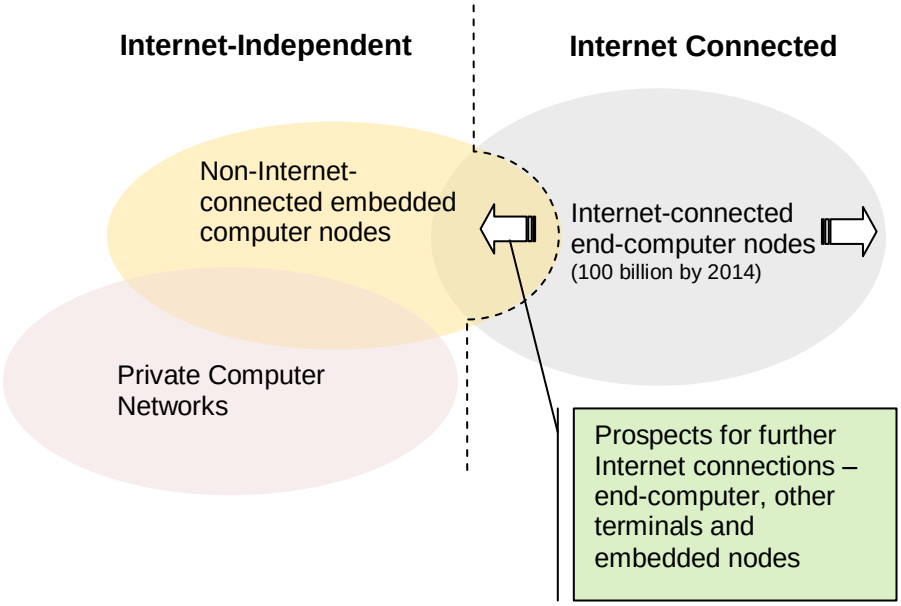
Clearly, the development of the IoT will need to progress through appropriate collaboration with Internet developers and the associated facilities for Governance. The expectation is that the number of nodes comprising the Internet will grow to well over 100 billion within a short period of time and by 2014 will be supporting some 42 Exabytes (10^{18}) per month of consumer Internet traffic[18].

Non-Internet (IP-independent) Connected Structures in the IoT - Independent, not connected to the Internet, are computer and sensor networks, private and public, that may or may not resort to Internet support or may exist and develop as Internet-independent or IP-independent structures. These structures may also interface and interact with the physical world and so relax the Internet imperative as the only network-of-network requirement for the IoT. The prospect is thus presented for an integrated IP/IP-independent structure[19] for the IoT and even the development of a new network-of-networks comparable with that of the Internet itself and governed by an extended set of principles, possibly more geared to industrial and business needs.

[18] FIArch Draft Document (2011) Fundamental Limitations of Current Internet and the path to Future Internet.

[19] Note: by referring to IP/IP-independent rather than Internet/Internet-independent structure, structures and protocols, particularly at the physical edge (such as Ethernets), may be considered that can form commonality between the two.

To what extent commercial developments relating to the Smart Cities and other Smart initiatives will influence both IP and IP-independent IoT progression is yet to be seen, but there is clear potential for progression either way.



Such a concept may be further supported in considering the object-connected technologies applied to physical objects that facilitate identification and connection with the Internet and non-Internet network structures through intermediary readers or read-write interrogators offering two-way data transfers. These may be technologies without embedded computers but capable of carrying machine-readable identification codes and offering various levels of functionality dependent upon type. Bar code, two-dimensional code and radio frequency identification (RFID) technologies are representative in this respect.

Adding the object-connected layers and the associated interfacing and interacting with the physical world, and the role of human linkage in structures, a view emerges of a prospective IoT structure that comprises IP and IP-independent components together with physical world intranet structures that have the prospect of linking with either of these components. The facility to accommodate future developments is also seen as a necessity in seeking a statement of IoT structure.

Important areas of object-connected legacy that must be considered in IoT development are the supervisory and data acquisition (SCADA) systems and distributed control systems (DCS). In general terms SCADA systems usually refers to centralised structures which monitor and supervise the control of entire sites, often spread out over large areas, ranging from industrial sites to national support structures. SCADA solutions often incorporate distributed control system (DCS) components and the use of the standardised control programming language, IEC 61131-3 (a suite of 5 programming languages including Function Block, Ladder, Structured Text, Sequence Function Charts and Instruction List), to create programs which run on remote terminal units (RTUs) and programmable logic controllers (PLCs).

The Internet and wireless communications has clearly had impact upon SCADA developments, with first generation monolithic systems giving way to second generation distributed systems and now the impact of a third generation of network systems predicated upon the use of IP and TCP based protocols. Application specific SCADA systems, hosted

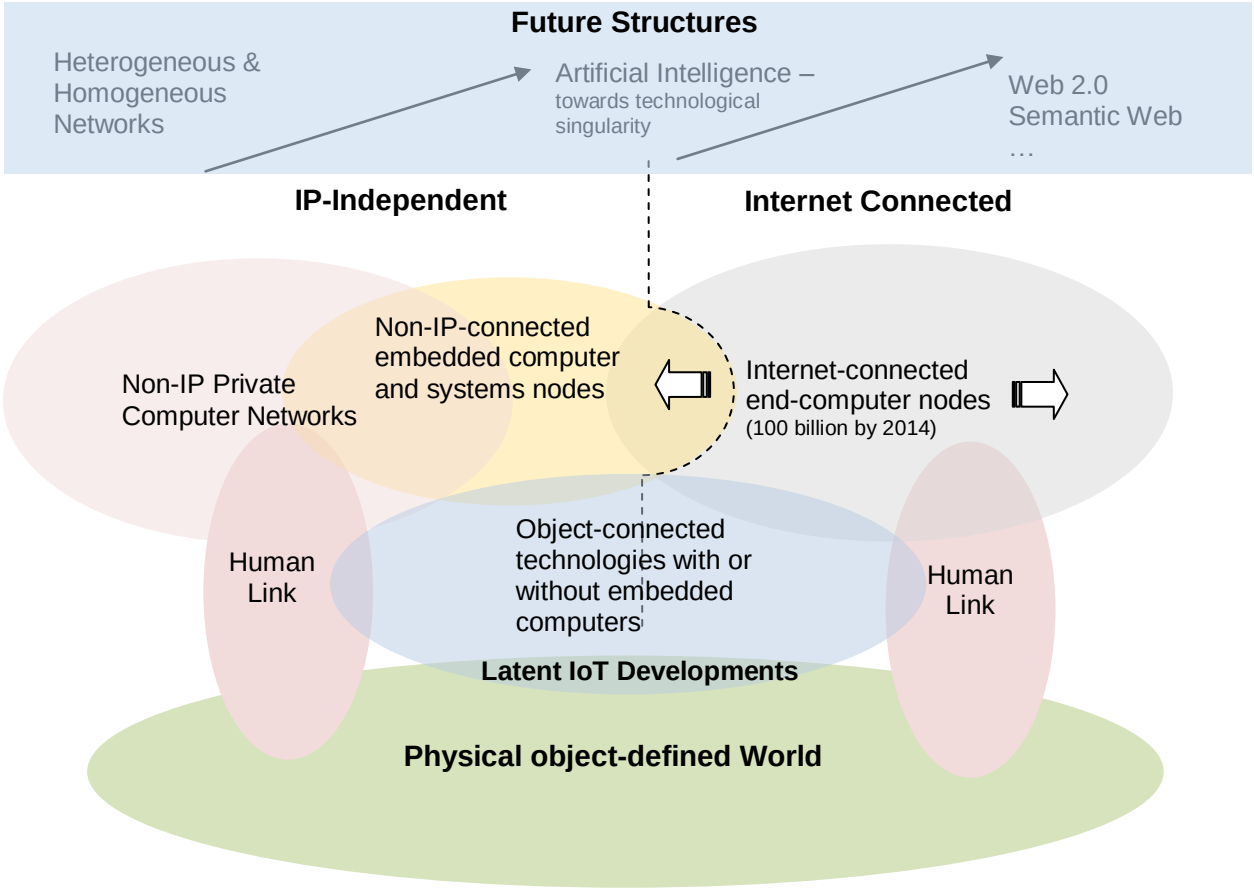
on remote platforms over the Internet, are now being offered to end users, and thin clients web portals, and web-based products are gaining popularity as a consequence of Internet attributes for easing end-user installation and commissioning requirements. However, there remain concerns over Internet security provisions, reliability of Internet connectivity and latency.

While efforts will be clearly made to accommodate such concerns through Internet development per se other options residing in IP-independent structures may also be developed.

Framework for IoT Structure

While the Internet is taken has an imperative for IoT development, what emerges from the consideration of Internet together with the imperative for physical world interfacing and interaction, is a prospect for both Internet and Internet-independent (or IP-independent) IoT developments. It has also raised the prospect of what may be described as Latent IoT developments, developments that initially have no link with Internet of IP-independent network of network structures but could well be linked in some way at a future date. Many automatic identification and data capture (AIDC) applications fit into this category of structure. Examples may also be seen to be arising from European IoT projects.

The schematic below is an attempt to represent the holistic tri-state structure being here proposed for the IoT.



Overlap of ellipses in the above graphic signifies a combination of features, such as Internet connected computers linked to object-connected technologies on the right and private networks linked to embedded systems and object-connected technologies by overlaps on

the left. Given appropriate quantitative data these ellipses and their overlaps could represent numbers of corresponding nodes. As indicated, without quantification, they simply signify, qualitatively the nature of such nodes.

Characterising Applications and Services

With prospective IoT structure partitioned into Internet, IP-independent and Latent IoT sectors of development, the prospect may also be seen for characterising applications and services in accordance with these sectors and subsequently into sub-sectors determined by the architectures and capabilities of the sector components. In the case of Internet structures this includes the capabilities offered by the networking and communication structures, generic top level domains and the Internet protocol stack (see below - Exploiting the Internet Component for IoT Applications and Services).

Statement of Structure for the Internet of Things

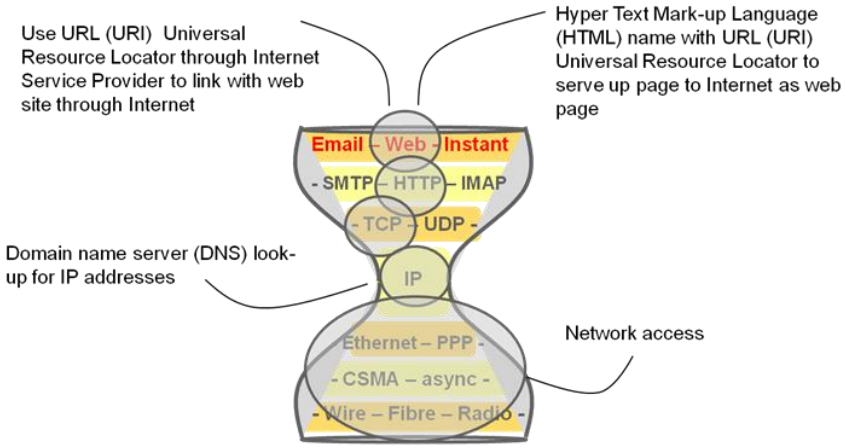
Based upon the consideration of imperatives so far, and the view that emerges, a statement of structure can be proposed that takes the following form: '**An integrated, internationally agreed and standards-supported network, communications, interface and actuation structure that exploits the existing and future Internet, existing and future, fixed and mobile telecommunications systems, existing and future object-connected technologies, coupled prospectively with non-IP private networks and associated communication, interface and actuation structures, organised to facilitate development of application and service layers specific to physical world, object-oriented needs and opportunities relating to the identified purpose for the Internet of Things'.**

As with the statement of Purpose this too is a generalised statement directed at providing a flexible and extendable frame of reference to allow for change and technological developments. In contrast to definitions (although the differences may be slight) the platform for statement allows for further description and explanation of terms. Object-connected technologies, for example, may be described as those technologies that are intrinsic to, embedded-in, attached-to, accompany or are associated with tangible physical entities of any kind and facilitate identification of the objects concerned together with other data capture and actuation functionality as appropriate for interfacing and interaction with said objects and as appropriate the environment in which they are situated. Automatic data capture, sensing, positioning and communication technologies are representative in this respect.

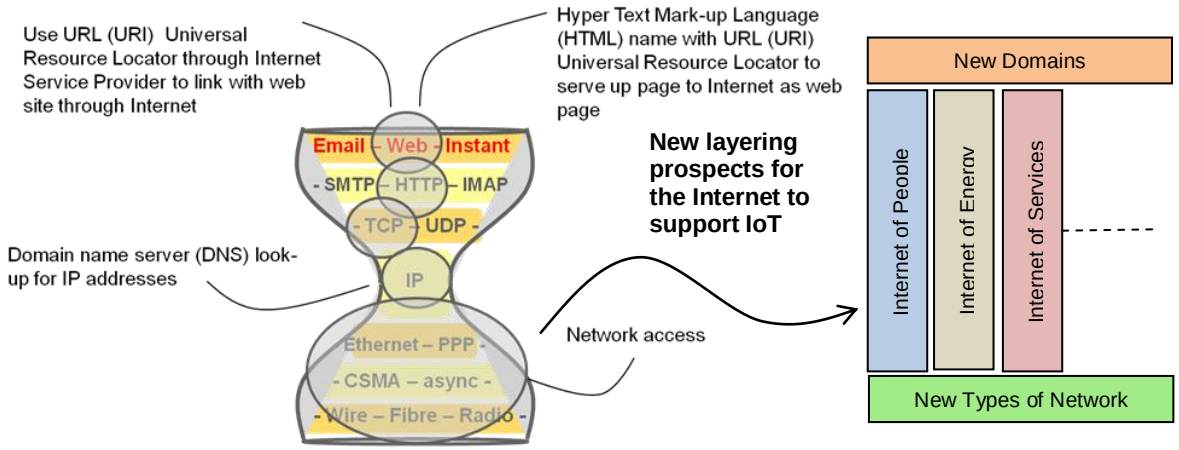
The **platform** for statement also allows for international input and consensus.

While the consideration of imperatives may be viewed as somewhat simplistic it does point to the clear prospect of a partitioning of contributory elements to the Internet of Things and a platform for considering application area layering with attendant consideration of area needs.

Exploiting the Internet Component for IoT Applications and Services – The Internet provides a protocol stack, on top of which is a 'generic' application layer. The world wide web (www or Web) is generally considered the most prominent of applications presented in this layer, with e-mail and messaging constituting further applications at this level. Applications and services that interface and interact further with the physical world can be expected to exploit these facilities and the associated Internet protocol stack and the Internet Protocol (IP) addressing (IPv4 and IPv6).



While different combinations of protocols from this stack and the generic application layer may be selected to support different domain level applications the prospect may be seen for other protocols and domain level applications specifically developed for IoT purposes, including for example generic top-level domains for IoT. Layered application areas may be considered in this way to accommodate new Internet concepts such as those being proposed for Internet of People, Energy, Services and so forth; not as separate Internets but layered upon the Internet of Things and facilitated in part through developments in interfacing and interactions with the physical world. The question therefore arises as to whether the existing Internet structure can accommodate such developments both in terms of functionality and performance. By exploiting the generic domain principle the differing architectural needs could conceivably be accommodated through the domain providers and the responsibilities they would have in maintaining such domains. The question then arises as to the economic feasibility for such structures.



Along with these prospective developments may be seen the prospect for additional network types and associated access. Irrespectively, all such prospects will clearly require the cooperation of the Internet developers, such as the Internet Engineering Task Force (IETF) and the associated Governance bodies.

Resolving identifiers across the Internet – More than a prospect is the need to accommodate legacy numbering and identification systems, such as the GS1 numbering systems, electronic product code (EPC) and uCode and the various object identifiers (OIDs) and associated unique item identifiers (UIIs) within the IoT. This is because they are specifically concerned with identifying physical entities.

In many ways the GS1 and EPC constitute a special case being essentially proprietary codes for which GS1 and EPCGlobal have developed their own products and protocols and contributed to international standards to handle Internet-based applications. Other identifiers and their resolution requirements are part of the on-going CASAGRAS2 resolver developments.

Data carrier and transfer principles – The interfacing and interaction features of the IoT will exploit the object-connected technologies and the identification and carrier principles characterised by the body of knowledge and experience collectively know as automatic identification ad data capture (AIDC). This very important, extensive and growing body of knowledge has never been effectively introduced into main stream information and communications technology (ICT) curricula, yet constitutes a foundational underpinning for physical world interfacing and interaction. It can therefore be seen as a foundational underpinning for the IoT applications and services design and should be developed accordingly.

Very significant in this underpinning are the principles of identifying, carrying, caching and transferring data or information to meet particular application needs in a more flexible manner. Too often assumptions are made that the IoT will simply identify objects by numbers and through these numbers deliver data or link to information stored elsewhere and accessed via the Internet. AIDC and the broader base of object-connected ICT offers other options to practical data carrier, transfer, processing and storage that can enrich the capabilities of application solutions and ease the inevitable problems associated with connectivity and Internet traffic[20]. So too with applications requiring response and actuation wherein an Internet connection may not be a necessity, and may even constitute a hazard where safety and business-critical issues are concerned.

Communication Networks – The whole issue of Internet traffic is being brought into sharp focus by the growth in video streaming largely generated by social networking, content-rich sites such as YouTube and the on-demand services providing TV entertainment. From an IoT standpoint the situation may be further exacerbated by the edge-defined data streams and cloud-based developments. To what extent such developments will compare with video traffic is yet to be seen. However, the need can be seen for pre-empting capacity, latency and other network needs with respect to other data-intensive developments.

The success of cloud-based initiatives would appear to hinge on the use of public wide area networks (WANs), but with attendant concerns over entrusting data to external agencies, associated privacy and security, and growing demands on public network bandwidth. In addressing these concerns attention is being directed at contracting issues and trust, enhanced security, and performance enhancement opportunities such as WAN optimisation and effective use of caching in relation to Web servers, browsers and edge-defined functionality of networks.

The issue of ‘private clouds’ has also been muted where a shared private network infrastructure is advocated as a means of resolving some of the security issues through single firewall control. While such an approach may be considered fine in theory the practical challenge of providing a cost and beneficially effective solution may point to a hybrid or virtual solution where there is further consideration of security needs, shared resources and automation.

[20] Cisco annual Visual Networking Index (VNI) suggests that Internet traffic will quadruple to 767 Exabytes (767 x 10^{18} bytes) by 2014.

Such issues are illustrative of the networking considerations to be addressed in developing the IoT, and prospective partitioning of Internet and IP-independent areas of development.

Underpinning principles of Object-connected ICT and IoT applications and services design - In parallel with any development in the IoT must be a parallel positioning and development of object-connected ICT within mainstream ICT curricula.

While statements of purpose and structure may be derived in this way, the global nature of the IoT demands that they be considered, and as necessary modified to accommodate perspectives derived through international cooperation and collaboration, as points of reference in deriving a framework for IoT Governance.

International Governance Framework for the Internet of Things (IoT)

Given the foundational imperatives for the Internet of Things presented above it is clear that any International Governance Framework for the IoT must align with and / or influence the existing and future Internet on matters that exploit the Internet structure and functionality. As with the existing Internet the need may also be seen for developing an international governance framework that:

1. Recognises the need for Global Regulation, possibly based upon self-regulation with subsidiarity and supported by a soft-law framework for regulation.
2. Recognises the need for a Global Legislator and distinguishes the criteria for such a role.
3. Recognises the importance of Internet Governance and the roles of WGIG, WSIS and ICANN and IoT input into an integrated structure for Internet and IoT Governance.
4. Supports an international legal framework covering legal issues and mechanisms, including regulation.
5. Supports a multi-disciplinary approach to governance based upon Technical, Policy, Economic, Institutional and Legal perspectives.
6. Supports by infrastructural substantive principles and requirements for robustness, availability, reliability, inter-operability, transparency, accountability and access to governance proceedings.
7. Supports an open knowledge environment as a foundation for bridging digital divide, encouraging creativity and economic development.
8. Includes international stakeholder groups, comprising States, Private sector, Public sector, Civil Society and International organisations.
9. Includes trans-governmental networks and Regional Legislators.

As a staring point in considering these requirements it is expedient to consider the developments with respect to Internet Governance. IoT Governance will most likely be inextricably linked to that of the Internet governance. However, the IP-independent challenge and the nature of the object connectivity point to the need for an additional governing body for the IoT concerning content that is beyond the bounds and acceptability currently seen for Internet governance.

The Need for Internet Governance - Phenomenal growth of the world wide web in the early 1990's and subsequent integration of the internet as a vital part of the economy and society led to a United Nations call for a World Summit of the Information Society (WSIS) directed at

discussing the governance of the Internet as a global critical infrastructure[21], culminating in the Working Group of Internet Governance (WGIG)[22] and the Internet Governance Forum (IGF) which continues to promote discussions on the Internet.

The WGIG provided a working definition for Internet governance, stating:

"**Internet governance** is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures, and programmes that shape the evolution and the use of the Internet. It should be made clear however, that Internet governance includes more than Internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN): it also includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet" (WGIG 2005).

Such a definition may also be seen as the basis for IoT governance.

Stakeholders - WSIS suggested (implied in Article 49 of the WSIS declaration) a division in roles for stakeholder groups:

- **States** - "policy authority for Internet-related public policy issues (including international aspects)
- **Private sector** – development of the Internet, both the technical and economic fields"
- **Civil society** – "important role on Internet matters, especially at community level" intergovernmental organisations – "the coordination of Internet-related public policy issues"
- **International organisations** – "development of the Internet-related standards and relevant polices"

The range of stakeholder interests need to be accommodated in an appropriate model or framework – a single Internet governance framework using a variable geometry approach[23].[24], conceptual framework differentiating between the international law of coexistence, based on the principle of sovereign equality, and the international law of cooperation, which includes the equality of participation but the differentiation of tasks and obligations[25].

Governments will invariably draw upon the IGF concepts in developing policy, law and controls within their jurisdiction. It is therefore reasonable that they will also draw upon such concepts in seeking a governance platform for the Internet of Things.

WGIG's multidisciplinary approach to Governance has allowed it to accommodate Internet governance issues from the following perspectives:

- Technical
- Policy

[21] Benhamou, B (2007) A European Governance Perspective on the Object Naming Service, Proceedings of the Portuguese EU Presidency conference on RFID: The next step to The Internet of Things.

[22] The WGIG is an international body comprising members from government, industry, civil society and academe (research).

[23] (Kurbalija, J, Internet Governance and International Law)

[24] Kurbalija, J Internet Governance and International Law in Reforming Internet Governance: Perspectives from WGIG, 106-115

[25] Abi-Saab, G (1998) Whither the International Community?, European Journal of International Law.

- Economic
- Institutional
- Legal

Each relate significantly to the IoT

Two broad Governance issues raised by the Internet and the IoT are technical and legal:

- **Technical, including:**
  - Domain names
  - Internet Protocol (IP) addresses
  - Root name servers
  - Standardisation

For IoT this is extended through the resolver work, search and discovery requirements, and associated standardisation needs.

As far as legal issues relating to Governance are concerned the WGIG's discussions have focused upon[2]:

- **"Legal issues** *per se*, including cybercrime, intellectual property rights, data protection, privacy rights, and consumer rights;
- "**Legal mechanisms** for addressing Internet governance issues, including self-regulation, international treatise, and jurisdiction"

Each of these relate significantly to the IoT.

Legal aspects of Internet Governance also include attention to[2]:

- **Cyberlaw vs Real Law** – WSIS/WGIG discussions emphasise the need to use existing national and international legal mechanisms for regulating the Internet.
- **Global regulation** – while desirable in many aspects, national and regional regulations are assuming greater relevance.
- **Variable geometry approach to governance** – recognising it as a method of differentiated integration which acknowledges differences within the integration structure and separation between integration units.
- **Differences between International Public Law and International Private law** – recognising the significance of public law in the context of Internet governance.
- **Harmonisation of National Laws** – supporting the need for global regulation, resulting in one set of equivalent rules at global level
- **Elements of International Public Law** – that could be effectively applied to Internet and IoT governance, including:
  - Treaties and conventions
  - Customary law
  - Soft law – frequently encountered in governance debate

Soft Law refers to quasi-legal instruments which are not legally binding or otherwise somewhat "weaker" than the binding force of traditional law. The term is generally associated with international law and used to cover such elements as:

- Resolutions and Declarations
- Statements, principles, codes of conduct, codes of practice often found as part of framework treaties;
- Action plans
- Non-treaty obligations

Soft Law[26] would appear to have some benefit in formulating international contributions to legal framework proposals, the following attributes being representative of these benefits:

- **Not legally binding** – cannot be enforced through international courts or other dispute resolution mechanisms
- **Contain principles and norms rather than specific rules** – usually found in international documents such as declarations, guidelines and model laws
- **Used for building** mutual confidence, stimulating progress, introducing new legal and governmental mechanisms
- **Less formal approach,** not requiring official commitment of states, reducing potential policy risks
- **Flexible**, enough to facilitate the testing of new approaches and adjustment to rapid developments
- **Greater opportunity for multi-stakeholder approach** than does an international legal approach restricted to states and international organisations

As far as the framework and media base for developing governance proposals are concerned, technical, policy, economic, institutional and legal would appear to be natural categories for consideration with the soft law and variable geometry being the methods of approach for formulating the content of such proposals where legal matters are concerned. The latter requires legal expertise and for IoT considerations expertise in respect of international law.

Legal Perspectives on the Internet of Things – A recent publication[27] entitled, "Internet of Things – Legal Perspectives" addresses a number of the legal aspects presented above and provides a set of foundational considerations for Governance of the Internet of Things. A general approach to the legal framework suggests a self-regulating structure as soft law and a model for social control and an international legal framework based upon global and regional legislator representation and substantive international principles. Strong attention to privacy and security is advocated within this legal framework.

A structure is proposed in the publication for governance of the IoT with attention to establishing a Governance Structure, together with considerations for legitimacy and inclusion of stakeholders, transparency, accountability and allocation of critical resources. However, it is referenced to a model of the IoT that is largely predicated upon RFID and EPC with the Global Legislator, EPCglobal, ICANN and the International Telecommunications Union being identified as the only bodies subject to governing principles. By recasting the model to a more inclusive one the principles can be readily applied to define a more inclusive Governing Structure.

[26] Kurbalija, J Internet Governance and International Law in Reforming Internet Governance: Perspectives from WGIG, 106-115
[27] Weber, R H & Weber, R (2010), Internet of Things – Legal Perspectives, Springer

As far as the content for governance is concerned there is the need to consider what is significant for IoT in relation to technical, policy, economic, institutional and legal matters, and with initial reference to the recommendations from CASAGRAS1.

Drawing upon the recommendations of CASAGRAS1

The Internet itself continues to need the guidance and direction of the IGF and through its deliberations will impact the conceptual approach that governments will take concerning the evolution of the Internet. Governments will invariably draw upon the IGF concepts in developing policy, law and controls within their jurisdiction. It is therefore reasonable that they will also draw upon such concepts in seeking a governance platform for the Internet of Things. This may be considered even more so when viewing the Internet of Things as integration with the existing and evolving Internet. The global nature of the exercise demands an international, IGF-linked, platform structuring governance platform for the IoT.

A range of issues will need to be accommodated in realising such a platform. The European Commission consultation process on RFID revealed that 86% of respondents supported the need for a "governance model that is built on transparent, fair and non-discriminatory international principles, free of commercial interest".

While the core of the Internet, the governance structure, has not been subject to legislation, countries around the world, and within Europe, have introduced laws to ensure that Internet usage does not conflict with national laws and international rights and conforms to the norms and values of societies in general.

Issues of legislation will undoubtedly arise with respect to the IoT, particularly where concerns arise that are of a privacy and security nature.

With respect to RFID concerns have been expressed over openness and neutrality of database structure that are used to hold unique identifiers. This is also of direct relevance to the IoT and global coding. Ethical and secure systems management is required with processes that are interoperable and non-discriminatory[28].

These considerations provide lessons for considering the governance requirements for the IoT.

With the scale data traffic being proposed for the IoT and the associated prospect of an emerging federated service infrastructure that could possibly emulate the growth potential of the world wide web public policy issues are likely to present significant governance considerations for which no one country could be seen to have authority. Social and economic dependence points to the need for a regional based approach[29]. Benhamou[30] views the IoT as an emergent critical resource and advocates the need for different countries and regions to progress work on different options to meet the governance needs.

In view of the latent requirement for integrating the IoT with that of the Internet it is important that proposals for governance and other issues are considered in cooperation with relevant authorities and organisations involved with parallel developments of the Internet. Within Europe the European Future Internet Assembly is an example of such an organisation in

[28] Wolfram, G et al, (2008) "The RFID Roadmap: The Next Steps for Europe", Springer.
[29] Ibid
[30] Benhamou, B (2007) A European Governance Perspective on the Object Naming Service, Proceedings of the Portuguese EU Presidency conference on RFID: The next step to The Internet of Things.

which one of its aims is to develop the tools and approaches harnessing the potential of the IoT.

A further aspect of governance requiring attention is the need to consider whether a registration authority is required for identifiers and the management of a global scheme for resolving them.

All this begs the question as to whether the IoT should be governed separately from the Internet or as part of the Internet governance. The logic and the existing Internet Governance framework suggest that it should be an integral part of Internet governance. However, the needs for governance and how they may differ from the issues for the Internet demand further research and consideration.

Given the nature and status of these disparate considerations the obvious recommendations in respect of governance for the IoT, as far as the recommendations of CASAGRAS 1 are concerned, are:

- To establish an international IoT Development and Governance Forum that can influence Internet Governance and undertake rapid research into the issues for ensuring and agreeing appropriate and effective governance, including the revenue and registration schemes that will be needed and the political framework that will be necessary to facilitate appropriate international collaboration.
- Agree an initial federated structure for the IoT and initiate an international programme of application and services development.

In view of the multi-dimensional nature of the governance issues the need may be seen for an overarching programme of research and development geared to accommodating all the necessary socio-economic, business and technical dimensions, including the protection of such a network against attack and abuse.

Building a Framework of IoT Governance Requirements

In building such a framework it is expedient to consider the WGIG working definition for the governance of the Internet with respect to “shared principles, norms, rules, decision making procedures, and programmes that shape the evolution and the use of the Internet”.

While it should also be recognised that governance is more about the operation and usage of the network than its structure, aspects of structure will naturally have a bearing upon governance issues.

These **aspects of governance relating to structure** will include:

- Partitioning of IP, IP-independent and Latent IoT structures and associated areas for Applications and services
- Security policy and provisions
- Safety policy and provisions
- Energy conservation policy and provisions
- Regulatory policy and provisions
- Standardisation policy and provisions.

Aspects of governance relating to operational and usage will include:

- IP, IP-independent and Latent IoT structures and associated areas for Applications and services
- Global Numbering / Resolver scheme for identification and discovery
- Social Capital, privacy and Identity management policy and provisions
- Ethical and user protection policy and provisions
- Cyber-crime protection policy and provisions
- Intellectual Property protection policy
- Performance Indicators, rules and norms for IoT operation
- Developmental policy

Establishing an International Governance Framework

Based upon the considerations presented above the process of establishing an international governance framework for the IoT requires an attendant knowledge of the Internet governance. This is to facilitate a contribution to Internet development and associated governance based upon considerations specifically targeted at IoT governance content.

As far as the specific framework for IoT governance is concerned the following staged development may be considered:

13. Preparation of IoT Statement of Structure and Purpose as an initial reference document for developing international IoT Governance.
14. Identification of an international IoT Governance Stakeholder Group.
15. Identification and appointment of a Global Legislator and Regional Legislators.
16. Legislator/Stakeholder agreement on Regulatory approach – prospectively Self-regulation with subsidiarity (central authority or trans-governmental network having subsidiary function in handling tasks or issues that cannot be handled by the self-regulatory authority) rather than international agreement.
17. Legislator/Stakeholder review and agreement on IoT Statement of Structure and Purpose.
18. Legislator/Stakeholder agreement on international legal framework.
19. Legislator/Stakeholder Identification and positioning of trans-governmental networks for IoT Governance and liaison with Internet governance developers.
20. Legislator/Stakeholder development and agreement on governance content requirements.
21. Legislator/Stakeholder agreement on foundational substantive principles for governance and governance procedures.
22. Legislator/Stakeholder agreement on infrastructural requirements and policy for on-going consideration of infrastructural requirements and attention to robustness, availability, reliability, interoperability, transparency and accountability.
23. Legislator/Stakeholder agreement on access to governance procedures and liaison with Internet governance developers.
24. Legislator/Stakeholder agreement and pursuance of governance and legal agenda on governance requirements.

Stage 1, Preparation of IoT Statement of Structure and Purpose, as an initial reference document for developing international IoT Governance has been outlined in this discussion document and is pivotal as far as a basis for considering developmental potential and foundations for IoT applications and services. Because it is viewed as pivotal the statements of purpose and structure, including the partitioning into Internet, IP-independent and Latent IoT developmental structures, requires both European and international consensus.

Stages 2 to 12 are essentially tasks to be undertaken by an international group, as yet to be set up, to fulfil the role of IoT governance and liaison with Internet governance bodies. CASAGRAS2 is presently considering the initial statements of purpose and structure proposed and will also seek to make recommendations in respect of content for stages 2 to 12. However, from a European standpoint it is an IERC Cluster Activity Chain requirement to take the Governance framework to the next level of consideration, potentially based upon tasks relating to the content of each of the stages proposed.

The first requirements in taking this forward are to:

1. Identify representatives from the IERC Cluster projects who will participate in the Governance Activity Chain.
2. Circulate the discussion document for consideration by project representatives and with a particular view to agree or otherwise with the propositions on:
    a. Statements of Purpose and Structure for IoT.
    b. Sectors of IoT structural development – Internet, IP-independent and Latent IoT.
    c. Propositions and stages for establishing an IoT Governance and Legal Framework.
3. Deliver responses to the IERC Cluster leader for the Governance Activity Chain.