ALEXANDER VON HUMBOLDT
INSTITUT FÜR INTERNET
UND GESELLSCHAFT

DRAFT PAPER prepared for the 1st Berlin Symposium
on Internet and Society
October 26th – 28th 2011

Policy implications of future network architectures and technology

Conference Draft, October 2011

Avri Doria
avri@acm.org

The author wishes to thank the reviewers of this paper for their patience with the early versions and for their comments. These kind souls include: Elwyn Davies, and Joy Liddicoat, who not only reviewed but also contributed conceptually. The author especially thanks the Institute for Internet & Society as well as The Social Science Research Center Berlin for enabling the study, with particular acknowledgement to Jeanette Hofmann and Christian Katzenbach for their guidance and assistance. Of course despite all of this help, any and all of the flaws in this paper are the responsibility of the author alone.

It is the author's intent to do a last update of this paper after the 1st Berlin Symposium on Internet and Society to be held on 26-28 October taking into account the discussions held during that meeting.

Overview

The study looked at many of the technological innovations that the Internet[1] is likely to experience over the next decade. This report discusses some of the possible policy implications of some of those innovations in the light of this study. The main assumption for the study has been that the development of technology and policy are inextricably interrelated and that they affect each other at each stage of technological and policy development. The study explored this relationship and this report attempts to extrapolate from the relationship and from ongoing technological innovation to discuss the various policy issues that will need attention over the next decade. As part of the discussion, several possible areas for continued research are mentioned.

The organization of this paper is to first expose a view of the Internet as a complex system influenced by a set of principles. While the normal view of the Internet as a set of services and protocols is necessary for a technical discussion, it is not as helpful when trying to look at the effect of changes in the Internet on policy. To understand the relationship of the Internet to policy it is necessary to look at how the principles upon which the Internet is built affect the structure and usage of the system. The first section of this paper discusses this assortment of principles. This section of the study and of this paper became more exhaustive than originally intended because the framework for looking at policy from *both* the technical and social perspectives, as opposed to just one perspective, is not yet well developed. This is a substantial hindrance to any analysis that is required to understand how the technology, the policies of that technology and governance policy interact and might affect each other in the future. This is, therefore, a possible goal for the

[1] Often academic articles refer to the Internet as the internet. This paper uses internet when referring to the general problem, of autonomous network being formed into a coherent network, .i.e. an internet, and uses Internet when referring to the global network of autonomous networks. It should be noted, that the trademark holders of the term Internet, CNRI, insist that whether it is spell with all capital letters or none, the meaning is always the same and is determined by them. The author apologizes to them for treating the word as if it still belonged to the language commons.

Institute for Internet & Society: Develop a practical and theoretical framework for understanding and using the inherent and inextricable interrelationship of technology and social policy.

Perspective on predictions

In terms of making predictions on what may or may not happen in the future, a cyclical, non linear, perspective is taken on the history of computer networking. That is, in looking back at Internet history, one can see that the central paradigm has periodically alternated between opposing views of various attributes, e.g., centralization versus decentralization, regulation versus deregulation, and homogeneity versus heterogeneity. Of course, in each cycle, the nature of the choice varies with the available technology and the policy trends at the time. In positing possible futures, the report will rely on this cyclical nature of Internet history. In looking at predictions, it is also important to remember this cyclical nature.

Another perspective that colors any predictions made is an emerging phenomenon like the Internet is approached from the perspective of genetic epistemology; a perspective that tends to see the phenomena under study as a entity that develops in a series of assimilations and accommodations where at first a new thing is understood using the pre-existing constructs of prior entities and only later is understood as a thing-it-itself[2]. [Piaget 95]

The later parts of the paper look at several technological trends and point to some of the governance policy areas that might be affected in a 'continuous and perpetual mechanism of readjustment or equilibrium.' [Piaget 95]

Recommendations for further research

Throughout this paper, suggestions are made for areas that would benefit from

[2] thing-in-itself or noumenon is a concept that originated in Greek Philosophy and was brought into modern usage by Emanuel Kant. In the philosophical usage, it often points the essential nature of a thing as opposed to its phenomenal appearance. In the usage in this paper, the notion ignores any possible differentiation between the phenomenal appearance and a putative real existence, but rather refers to the nature of a thing understood within its own context as opposed to being understood solely in reference to some other thing.

further academic study. The recommendations will principally be in applied research that, using the same model as this initial study, relies on the interrelated nature of technology and policy and of theory and practice. The author recognizes that this report only touches lightly on many of the issues.

Principles

The study commenced with a review of the various principles that have guided and continue to guide the development of Internet architecture and technology as well as policy. Each of several sets of technological and policy principles are described in this paper. This first part of the work relies on a simple exegesis of a sampling of the major written principles; that is what various writers and groups have said that affects the understanding and framing of the issues for the future, from both the technological and policy perspective.

Technology Principles

Essentially, technological principles are engineering constructs that are used to guide system designers. In engineering a complex system, designers often have many possible ways in which to solve a technical problem. In making these decisions, system designers need a basis for making choices between equally acceptable engineering solutions. In general a system designer needs to balance considerations such as cost, ease of deployment, environmental suitability and political sensitivities. Additionally, a commonly accepted set of design principles enables a distributed community of designers and architects to build a single consistent system.

In the sections that follow, three types of principles will be discussed: general system engineering principles, Internet design principles and Internet operational principles. Some of these principles were first stated in [RFC1958] Architectural Principles of the Internet, which was updated by [RFC3439] Some Internet Architectural Guidelines and Philosophy. These documents, especially [RFC3439], go much further into Internet Architecture and describe several principles that are not discussed in this report.

General System Engineering Principles

The first three principles are general principles that apply to most all large system designs.

Amplification Principle

In engineering a system as complex as the Internet there are non-linearities that occur at large scale, which do not occur at small to medium scale. This means that something that might work in a small system of 100's of computer nodes would not work in a system of millions of nodes. Internet system and protocol designers must take these non-linearities into account when designing the technology to be used on the Internet. [RFC3439]

Simplicity Principle

If there is a simple and a complex way to do something, use the simple way [RFC1591]. This is the engineering variant of Occam's principle, but instead of applying it to hypotheses, it is applied to how a designer should choose between competing possible solutions. All other considerations being equal, a designer should choose the solution that appears simplest, while covering the requirements. Many system faults are found in cases where a more aesthetically pleasing solution was chosen as opposed to the simplest solution. As a system grows in necessary complexity, the opportunities for error increase. Choosing a more complicated engineering solution compounds the possibility of building an erroneous system.[RFC3439]

Variation in outcome

This is best quoted from the authors of "Tussle in Cyberspace: Defining Tomorrow's Internet" [Clark 02]:

> Design for Variation in outcome so that the outcome can be different in different

> places, and the tussle takes place within the design, not by distorting or violating it. Do not design so as to dictate the outcome. Rigid designs will be broken; designs that permit variation will flex under pressure and survive.

A system designed to be flexible is a system that grows and adapts to the needs its users place on it. For example, the most successful protocols defined for the Internet are those that serve purposes their creators could never have imagined.

Internet Design Principles

The principles described in this section pertain directly to the system that is currently called the Internet. Though the Internet might not yet have existed when some of these principles were first stated, the Internet has depended on adherence to these principles in its development. While most of these principles were designed with networking in mind, they have occasionally been applied, and sometimes misapplied, to topics other than network design.

Creative Anarchy

This has also been termed as the generative nature of the Internet [Zittrain 08]. It essentially refers to the fact that there is no top down design for the Internet. Most artificial complex systems designed before the Internet had a design committee headed by a chief designer. In the case of the Internet, there was no design committee, nor a chief designer. Instead a set of principles and the creativity of a multitude of engineers contributed and continue to contribute to the 'design' of the Internet. Anyone, anywhere, can still contribute the next innovation. They just need to be creative and know how to code.

The principle is credited for the invention of new application models such as wikis and social networks. It should be noted that this is also seen by some commentators, such as Jonathan Zittrain [Zittrain 08], as one of the fundamental problems of the Internet and as responsible for mis-features such as spam and viruses.

Packet based nature of the network

Packet switching is a network technology that was first described by Paul Baran and Leonard Kleinrock in the 1960s, as part of the Arpanet project to build a network. It differs fundamentally in concept and structure from the communication infrastructure that existed at the time, the Public Switched Telephone Network (PSTN). In a PSTN for there to be communication between a source and a destination, a circuit must be created by a centralized switch. In a packet-based network there is neither a physical circuit nor a centralized switch. Instead, the information that is being transmitted is broken up into discrete units called packets, or sometimes datagrams, and is passed across the network hopping from one independent system, called a router, to another. This is called hop-by-hop routing where there is no predetermined selection of routes and in fact no requirements that each of the unit of a message travel the same route between source and destination. It must be added that unless multi-route routing is used, routers in a system have usually converged a single route from a source to a destination and unless there is some failure during the transmission of a message, the packets will all travel the same route.

Packet switching also allows for the creation of an emerging network. There was no need to conceive of the Internet, or of any of the sub-networks within the Internet a priori. Rather, each group that is interested in building a network can build one and then find ways of connecting to others who are also building a network. This works especially well as long as they use the same protocols and develop them in an interoperable manner. Failing this, complex translation is required at the boundaries in systems called gateways. The Internet is a collection of independent networks that have agreed to use a common communications paradigm and that were interconnected with one another. In making these interconnections, there is no authority beyond the bilateral agreement for those interconnecting. The only authority involved concerns the assignment of the addresses and network numbers, also called Autonomous System (AS) numbers. Addresses will be discussed later in this paper under the section on Operational Principles.

The End-to-End Principle

The end-to-end principle was first described in 1984 [Saltzer 84] and has, to a large extent, also remained central to the architecture of the Internet. It is one of the unusual Internet principles that has migrated into policy and is frequently cited in political arguments about the future direction of the Internet. Many use the end-to-end principle to support their views, though sometimes with different interpretations that do not necessarily reflect the original principle or its meaning.

The end-to-end principle, often referenced to as e2e, states that a function can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. [Saltzer 84] In its simplest form, a corollary of the principle suggests that the only elements that belong in the core layers of the network are those that are useful to all other parts of the network. It has often been interpreted to mean that the specific functionality an application needs should be as close to the user as possible, in other words "at the edge or end of the network". While this is sometimes true, there is a proviso – provided that this function is not also needed by other applications.

Another way in which this is sometimes expressed is the proposition that, in the Internet, 'intelligence' is or should be 'at the edges of the network'. However this reflects a misunderstanding of the principle, which focuses on placing functionality at the most appropriate place in the network. If the function is most usefully placed in the core and is needed by most, or all, of the network, then it is in keeping with the end-to-end principle to put it at the core rather than at the edge. For example, the 'intelligence' needed to route messages from one network to another is placed in the core of the network without this being an infringement of the end-to-end principle.

Layered architecture and the hourglass model

A layered architecture is one where data moves from one layer to another and is subject to a different form of processing at each layer.

In a basic explanation of Internet protocols, reference is usually made to 'layers'. The basic notion of layers involves the idea that a particular sort of task is dealt with by one protocol in an ordered set of protocols called a protocol suite or stack. In contrast to the OSI 7 layer model, the Internet is sometimes discussed as having four essential layers above the hardware. The services provided by the Internet rely on these protocols and the mechanisms provided by the layered architecture for progressive encapsulation of data received from the higher layer protocols. In this, the layered architecture principle is related to the end-to-end principle in that it provides the framework for putting functionality at a relative edge within the network's protocol stacks.

The principle, however, goes beyond the end-to-end principle, especially when it is paired with the hourglass model. Simply put, this is the design decision that places the Internet Protocol, at the centre of an hourglass. An hourglass is an object that has a large container at the top and the bottom connected by a single narrow channel. The Internet protocol stack's basic design follows this pattern, with protocol functionality related to applications in the upper part of the virtual hourglass, and protocol functionality related to the underlying hardware infrastructure in the bottom half of the architecture. The narrow channel between the halves of the hourglass is designated as the Internet protocol (IP as in IPv4 and IPv6 and not as in 'Intellectual property'). The point of this arrangement, related loosely to layering, was that the technical work and skills, related to applications was fundamentally different than the work and skills, related to interfacing with hardware. By strictly separating these functions across a relatively simple protocol interface the two parts of the network were allowed to evolve independently but yet remain connected. As long as the protocol connection was made to IP, any application could work over any communications infrastructure. So while the original protocols might have made use of the File Transfer Protocol (FTP) and the original home dial-up communication infrastructure layered over the PSTN, the applications could evolve to become the World Wide Web and the home communications infrastructure could be replaced by Asynchronous Digital Subscriber Line (ADSL) or WiMax without any change to the fundamental nature of the Internet core.

Shared Fate

To share fate, means that the data path in the Internet is the same as the management path in the Internet. In the PSTN and most other networks, there is a management or control layer that is used to monitor and manage the network. In a shared fate network such as the Internet, that control information travels the network along the same transport path as the data. This means that instead of requiring a complicated set of management protocols to know when a problem occurs in the network, the interruption of the data flow is sufficient to make that known to the monitoring functionality. It also means that when functionality is disrupted, the originating and/or receiving units themselves must have the ability to determine the problem and initiate remediation. It also means that it is much more difficult for external entities to monitor what is going on at core parts of the network.

Without an assumption of shared fate, there needs to be an entire separate network management structure. Not having to create this separate management structure was another enabler for Internet innovation. It is also one of the thorns in the side of those who want to create operational networks that could be controlled externally.

Postel Robustness Principle

This principle, originating with the internet standards pioneer Jon Postel [RFC793], is summarized as follows: "Be conservative in what you send and liberal in what you accept". In the network sense it means that the utmost effort must be made to allow messages to continue their way across the system. By being as strict as possible in what a system sends, it attempts to be clear in its instructions and not give another system ambiguous information. On the other hand it also accepts that even when some other system is not as careful in the strictness of its messages, if there is any way to comply with the request within the security and stability constraints set by the system, the message should be processed.

While the robustness principle originated in the description of TCP, it has been applied to most of the protocols in the TCP/IP suite. It has also been applied on occasion to the way people should behave in the creation of protocols in protocol standards development organizations (SDO).

Operational aspects of the Internet

The aspects discussed in this section are a cross between de-facto principles and practices that apply primarily to the assignment, allocation and use of names and numbers in the network. For the most part these aspects, while considered purely technical by the engineers are governed by a set of assumptions and principles.

Internet Numbering

Internet numbers come in four basic forms: IP version 4 (IPv4) addresses [RFC791][3], IP version 6 (IPv6) addresses [RFC2460][4], autonomous system numbers [RFC1930][5] for the component networks of the Internet and the numerical protocol parameters[6] that are necessary to assure interoperability for most every protocol used. Based on the information contained in these numbers, as well as other information that may or may not be used, a message is sent from one system to another system along a route determined by rules set in the routing system of the Internet, using protocols whose behavior is constrained by various numeric parameters. Most debates in this policy area revolve around the two varieties of IP address, though occasionally, AS numbers will also be raised in non-technical discussions.

[3] RFC791 only provides the basic definition of the IPv4 address. There are at least 15 other RFCs that deal with IPv4 addresses and their use. http://en.wikipedia.org/wiki/IPv4

4 RFC2460 has been updated by three other RFCs; RFC5095 "Deprecation of Type 0 Routing Headers in IPv6", RFC5722 "Handling of Overlapping IPv6 Fragments" and RFC5871 "IANA Allocation Guidelines for the IPv6 Routing Header"

[5] There are 28 RFCs dealing with Autonomous System Numbers and their use with different protocol numbers.

[6] http://www.iana.org/protocols/

When IPv4 addresses were first created, the engineers who designed the system believed that that this addressing architecture would provide more then enough addresses to meet all future requirements while facilitating effective operation of the available hardware. At the time of writing this report, all of the IPv4 address blocks under control of the Internet Corporation for Assigned Names and Numbers (ICANN), about half of all IPv4 addresses, have been assigned by the Regional Internet Registries (RIR). This happened because of the expansion of the Internet and the increase in the number of devices connected to the Internet that require a separate IP address, e.g. computers, telephones, and appliances. While there are still many individual addresses left, the remaining distribution of large blocks of addresses to the RIRS is very uneven with ARIN, the US RIR having a comfortable supply that should last many years, while other RIRs like APNIC, which serves Asia and the Pacific, and AFRNIC, which serves Africa, having a more limited supply. Three solutions exist for increasing the availability of addresses. One solution that is not visible to most users is called Classless Inter-domain Routing (CIDR) [RFC462] and was introduced in 1993. CIDR radically changed the way in which IPv4 addresses where assigned and routed in the network at a time when it looked like IPv4 addresses would run out in the 1990's. Another technical solution, which is widespread, is Network Address Translation (NAT). The designated final solution is IPv6. Additionally, efforts are underway to find a solution to recover unused IPv4 addresses and discussions are ongoing about methods of allowing a market to develop in IPv4 addresses. This last is a policy issue of some significance that has been and will continue to be a subject for global debate.

Network Address Translation (NAT)

For many years, several ranges of private addresses [RFC1918][7] have been used by

[7] It should be noted that while the IETF defined the private address spaces, it did not standardize Network Address Translation (NAT). RFC1631 "The IP Address Translator" was originally published as an informational RFC on NAT in 1994; it was updated by RFC3022 "Traditional IP Address Translator". For most part the IETF has deemed NAT a violation of the Internet architecture perpetrated by industry. This was documented in RFC2993 "Architectural Implications of NAT" There have been over 60 RFCs on some aspect of NAT.

corporate networks and home networks. These addresses can only be used locally and may not be routed beyond this. Many readers, for example, will be familiar with an address like 192.168.1.1, which is the default address, found in most of the home routers sold on the open market.

While a very successful technology for allowing the Internet to grow despite an IP address depletion problem that was first announced 20 years ago, NAT has been seen as a pernicious problem by many Internet engineers [RFC2993] and is seen by some as the reason that the Internet Engineering Task Force (IETF) rushed to make decision about IPv6 in 1996 as they desired a solution that would obviate the need for NAT. One of the most frequent complaints against 'NATted networks' is that they interfere with the end-to-end nature of the network, because the system at the edge of a private network is responsible for translating the private address into a public, globally unique address. Certain protocols embedded IP addresses relating to the end points into their messages; NATed networks interfere with the operation of these protocols. Both the use of embedded addresses and the effects of NAT operations can be considered either as breaches of the end-to-end principle or as unwarranted assumptions about the meaning of that principle. On the other hand NAT technology has allowed the Internet to grow and can be said to keep translation at an edge as close as possible to the user.

However, NAT alone cannot solve the shortage of IPv4 addresses for large countries with rapidly expanding Internet user communities – such as Brazil, China, India and Russia – countries that need access to very much larger blocks of IP address numbers than are now available. This has created impetus for the deployment of IPv6, a protocol in search of a network for the past fourteen years.

IPv4 and IPv6

IPv6 increases the number of addresses available. IPv6 addresses are longer and have a different internal structure from those in IPv4. Because its addresses are longer, the IPv6 addressing system can be used to facilitate a greater number of systems without needing the NAT local addressing techniques necessary in IPv4[8].

The format of IPv4 and IPv6 are significantly different. This has meant that the two protocols do not interoperate. As there is no backward compatibility, Internet service providers need to support two IP networks, and all users need to run a dual stack that contains both IPv4 and IPv6. "16 years after the Internet Engineering Task Force (IETF) adopted IPv6, more than 99 percent of the Internet is still based on the older IPv4" [Leavitt 11] There are various theories on why IPv6 has not yet managed to become the IP protocol of choice. One theory is that the success of a transition to a new communications protocol is related to the degree to which a transition strategy is compatible with and reuses an older technology. The proponents of IPv6 were absolutely certain that the market would recognize the superiority of the new protocol and transition quickly. While there were those who ardently advocated a strategy of coexistence and backward compatibility, this was rejected time and time again. So sixteen years later, IPv6 remains relatively unused.

Within the IETF, there is a procedure, which is a corollary of the principle of creative anarchy; a proposed protocol only becomes a standard when it has been accepted by the market. And if the market does not accept the protocol, it is allowed to remain on the shelf until needed. To its credit, the IETF has not declared IPv6 a standard, it remains a proposed standard, but great effort is being placed on marketing the protocol; a first in the history of the IETF. There is a concerted effort among some Internet policy groups and some parts of the technical communities to foster a transition to IPv6.

One implication of the introduction of IPv6 is that it has widened the waist of the hourglass, mentioned above, such that now applications and link technologies need to have awareness of more then one network protocol, i.e. of both IPv4 and IPv6. While this has been facilitated somewhat by versatile application program

[8] It must be noted, that the use of NAT is expected to continue even under IPv6 is deployed in the Internet as users have found other features of NAT that they find useful.

interfaces (API) and the encapsulation of IPv4 addresses in the IPv6 addressing architecture [RFC3513], it has resulted in duplication in routing and network management. This duplication is a problem that requires a solution. Despite the fact that there are many reasons why IPv6 will be deployed within the next decade, there is a need for research to begin on finding a way to heal the rift in the network layer of the Internet. Given that the bottom-up Internet governance structure is now a reality, it is to be hoped that a solution to the IP problem will be discussed by protocol architects and governance architects in cooperation with each other. This is an opportunity for the next decade, but it must be understood that any solution will take more than a decade and that many of localized addressing problems can't wait that long, making the adoption of IPv6 by some major portions of the Internet necessary. Yet, the more that IPv6 is deployed, the greater will be the need to heal the diremption9 of the networking layer.

Internet Routing

Routing is a critical capability in the Internet and is intimately linked with the addressing architectures. Routing is the area in which many of the properties; both advantages and liabilities, of addresses are revealed. It is also the area in which the operational principles are established as de-facto principles.

Routing on addresses not names

One of the fundamental decisions made in the Internet is that the domain names that users are familiar with need to be translated into names of a different kind, the IP addresses. This decision, while reasonable given the technology on the 1970's is not necessarily obligatory given the state of today's technology. Given the QWERTY[10] like nature of the Internet, however, changing this principle is

[9] As diremption is not found in many dictionaries as it is considered obsolete, a definition is provided: a tearing apart, a violent separation

[10] QWERTY refers to the tendency of a technological system to become stuck with an early limitation. QWERTY refers to the placement of the keys in order to avoid collision in early manual typewriters. While technological improvements could have reorganized the keyboard within a short time, the users had already become accustomed to the organization of the keys and even today when there are no mechanical type and when user interface engineers have demonstrated that typing could be done more efficiently with another keyboard organization, most keyboard are still QWERTY keyboards.

something that is not often considered.

Overloading/Separation of Endpoint Identifier and Location Identifier

IP addresses are used both as the name of the node on the network (strictly speaking, an interface to such a node) and as the location of the node on the network. This means that nodes not only have domain names, but those names are translated into another form of name, an IP address used as the endpoint identifier, which also functions as a location identifier. This works fine in a fixed network where systems rarely move. In a mobile network, when a node frequently moves from one location to another it becomes confusing because the node should get a new location identifier but it can't do that easily because its location's identifier is its endpoint identifier, i.e. its IP address. It is as if each person in the world got a new name every time they moved from one apartment to another apartment. This use of an IP address for two inherently different purposes is referred to as overloading the meaning of the IP address. Research has been underway on how to achieve decoupling of identity and location to suit this new environment. Combined with the need to use overloaded IPv4 and overloaded IPv6 addresses this has put a strain on the routing system. One of the perennial questions asked about IPv6 is why the address overload problem was not fixed while creating the new IPv6 addressing structure. The IPv6 addressing architecture allows for the inclusion of identity identifiers, conceptualized as MAC addresses which are sometimes considered universally unique, as subfields of the IPv6 address [RFC3513]. It is uncertain to what degree these will be used to provide for a clearly mobile addressing architecture that supports the idea of a mobile Internet.

Internet Naming

Every system or network participating in the Internet has a name known as a *domain name*. These names are currently defined in a single distributed global naming framework called the Domain Name System (DNS) [RFC1034][11]

[11] RFC 1034 has been updated by the following: RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 2065, RFC 2181, RFC 2308, RFC 2535, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 4592, RFC 5936

[RFC1035][12].

The domain name system is a directory system that provides mapping between the domain name of a system or a service and the IP address by which and at which that named entity can be found as explained above. By referencing the DNS system with a domain name, the system gets back the IP address it needs to find and send packets to the target system or service.

Overall management of the domain name system is currently the responsibility of ICANN. One of main tenets of ICANN is that there can be only one naming system, and only one authority for this naming system. While this has been challenged by people since the creation of ICANN, no one has ever succeeded yet in materially challenging this doctrine.

Policy Principles

Over the last number of years, Internet governance policy[13] principles have been expressed by various groups. Unlike the engineering principles outlined above, these principles, while declared, most have never actually been used to build anything, although they were declared to be principles upon which the information society should be built and governed. While it will not be specifically discussed in this paper, it must be noted at the beginning of this discussion that many of the policy principles to be discussed in this paper hearken back to the Universal Declaration of Human Rights [UDHR], the International Covenant on Civil and Political Rights [ICCPR] and the International Covenant on Economic, Cultural and Social Rights [ICECSR]. Or at least they claim to.

Foundation: RFC 1591

[12] RFC 1035 has been updated by the following: RFC 1101, RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2137, RFC 2181, RFC 2308, RFC 2535, RFC 2845, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 5936, RFC 5966

[13] In this paper 'Internet governance policy' refers both to descriptive sets of policy as developed and applied by various institutions that deal with the governance of the Internet and to the normative sets of policy developed by governments, industry, the technical community and multi-stakeholder groups. As opposed to an attempt to derive separate terms at this point in the research, the text will reveal the context in which the term is being used.

In the beginning of the Internet Jon Postel, wrote an RFC entitled "Domain Name System Structure and Delegation." This document has been important in many ways and is the touchstone of the Internet domain naming system. As important, though, as the original naming delegations, are the principles contained in this document. These principles that are the underpinning of the multi-stakeholder governance system that is the foundation of Internet governance,[14] though they have never been called as such.

In this document Jon Postel indicated the following [RFC1591]:

- Every domain needs a designated manager
- Every domain name manager is a trustee for the public good and had 'a duty to serve the community'
- The domain name manage must treat all groups interested in a name equitably
- Significantly interested parties, aka stakeholders, should agree that the designated domain name manager is the appropriate domain name manager.

In many ways, while this was written in relation to country codes (ccTLDS), this is the foundational principle for the variation of participatory democracy being termed multi-stakeholder governance.

WSIS Outcome Documents

The World Summit on the Information Society was a process that had two focal meetings, one held in 2003 in Geneva, and one held in 2005 in Tunis, with many preparatory meetings for the focal meetings. As outcomes of this process, four (4) documents were released:

- Geneva Declaration of Principles
- Geneva Plan of Action
- Tunis Commitment

[14] The realization of the importance of this document was pointed out by Joy Liddicoat in conversation and in her blog: Human rights and Internet protocols: Shared Values, http://advocacy.globalvoicesonline.org/2011/09/30/human-rights-internet-protocols-shared-values/

- Tunis Agenda for the Information Society

As the titles suggest, these documents attempted to define a set of principles, a plan, a commitment and an agenda. It was a very ambitious plan to create order from what governments saw as the chaos of the Internet. By and large this process was a failure trumpeted as a great success, though there are pockets of activity that relate to the agenda. The most important thing that came out of this process was something that was not really considered at the beginning but became unavoidable at the end, an acceptance of the multi-stakeholder process by which the Internet is and should be governed. This multi-stakeholder process, something that is still not well understood, is one of the threads that will come out of this period and will affect all policy issues in the Internet for the foreseeable future. The model on which the multi-stakeholder Internet governance process is based, according to one of the leaders[15] of the WSIS process, is that we had to be as clever in defining Internet governance policy as the inventors of the Internet had been in creating the Internet. This was achieved by reinventing the process that was described in Postel's RFC1591 and that was in use by ICANN's ccTLD community.

Returning to the principles, the participating governments defined 34 principles covering the following areas [GDP 03]:

- The role of governments and other stakeholders in the promotion of ICTs for development
- Information and communication infrastructure: An essential foundation for an inclusive Information Society
- Access to information and knowledge
- Capacity building
- Building confidence and security in the use of ICTs
- Enabling environment
- ICT applications: benefits in all aspects of life
- Cultural diversity and identity, linguistic diversity and local content
- Media

[15] Several versions of this saying can be found. The author is uncertain of who said it first, or of the exact quote. The general opinion of several experts is that it was said during one of the Working Group on Internet Governance (WGIG) meetings under Chatham House rules that only permit quotes without attribution.

- Ethical dimensions of the Information Society
- International and regional cooperation

This document [GDP 03] and the principles in the document are rarely mentioned in today's Internet policy discussions, but the content of the principles listed under these headlines continues to have influence. Discussion on the principles in the WSIS and the Working Group on Internet Governance (WGIG) led to the publication of the Tunis Agenda, which still controls much of the policy discussion through the ITU Action Lines and the Internet Governance Forum (IGF). It is uncertain to what degree these activities will affect the future of policy decisions but as they constitute agreed upon language by the governments, anything in the four (4) outcome documents of WSIS can be brought up in discussion among or with governments. Such language can also be quoted by other stakeholders in the process as definitive argument.

ICANN Government Advisory Committee (GAC)

The Government Advisory Committee in ICANN[16] is a novel creation of Internet governance practice. The GAC gives its advice to the ICANN Board in various forms including[17]:

> 1) letters signed by the GAC Chair on behalf of the GAC.
> 2) communiqués and submissions endorsed by the GAC at face-to-face meetings and inter-sessionally.

[16] ICANN has a very interesting organizational architecture <http://www.icann.org/en/about/>. It is a volunteer organization that is supported by a professional staff, which is responsible for both helping the volunteers in creating policy and for operationalizing that policy with all that entails. The volunteer organization is composed primarily of three types of group: a Board of Directors, a set of Supporting Organizations organized according to areas of responsibility, e.g. gTLDs, ccTLDs and IP Addresses, and a set of Advisory Committees such as Government Advisory Committee (GAC), At-Large Advisory Committee (ALAC), Security and Stability Advisory Committee (SSAC) and Route Server System Advisory Committee (RSSAC). The organization has a woven architecture. The Advisory Committees are like the warp in a weave (the threads running lengthwise that provide continuity and the strength of a fabric) responsible for reminding the organization of relevant principles, and the Supporting Organizations are the weft in the weave (all the colorful horizontal threads that makes up the pattern and the design of a fabric) responsible for recommending policy to the Board. Without each other they are just balls of thread, but woven together they make the whole cloth of bottom-up multi-stakeholder governance. Internally the structure of the organization is quite gothic and takes most newcomers a year, with a competent guide, to understand. Explaining it adequately would require a paper as long as the current paper. Unfortunately there is no adequate source the author can recommend on this subject at this time.

[17] https://gacweb.icann.org/display/gacweb/GAC+Advice

3) overarching "principles" documents, typically developed over successive face-to-face GAC meetings.
4) "issues" documents, including interim issues documents.

According to the ICANN Bylaws [ICANN 11] the ICANN Board must take this advice into account when making its decisions, and when it does not accept the advice, the ICANN Board must first attempt to reach agreement with the GAC, but if it still disagrees it must document the basis of its rejection of the GAC's advice.

The ICANN multi-stakeholder model represents the first time that the roles between the private sector and governments have been reversed, with the governments being in the role of advisors as opposed to being the ones receiving the advice from the private sector. For some this role reversal has been difficult, and some countries have been slow to accept such a role and join. As some of the extraordinary events of 2011 have shown, the relationship within a public sector organization of a private sector Board of Directors and an intergovernmental group is still very much an emerging relationship that is neither fully understood nor stable. As such, it is groundbreaking and worthy of study and would be a worthwhile research topic that would contribute both to practical and theoretical understanding. Specifically: What are the normative and descriptive conditions of a multi-stakeholder environment where the role of governments does not include the ultimate responsibility for making decisions?

Two recent issues exercised the bylaws requirement that establishes the relationship between the GAC and the ICANN Board regarding advice for the first time since ICANN was founded: the .xxx (aka Triple X) decision and the new gTLD decision.

In the .xxx decision[18], the ICANN Board had originally given provisional approval

[18] The description that follows is simplified and leaves out many complicating discussions. Give the recent nature of the events, it is the author's assumption that studies are either ongoing or planned on the governance implications of this decision. For the most part the description is based on the author's recollection as one of the participants in the ICANN community at the time.

to the ICM Registry in 2005 and then rejected the application after receiving a letter sent in 2006 by the GAC to the Board opposing the decision to approve .xxx. After this rejection The International Foundation for Online Responsibility (IFFOR)[19] appealed the ICANN Board's decision using the bylaws defined reconsideration mechanism. An external reconsideration panel ruled against the ICANN Board, saying that it had not followed its own procedures correctly in rejecting the application. While their ruling was not binding, the ICANN Board announced that it would reconsider its decisions and created a process for that reconsideration. While that process was unfolding, the GAC again reviewed its position and sent advice to the Board indicating[20]:

> - There is no active support of the GAC for the introduction of a .xxx TLD.
> - While there are members, who neither endorse nor oppose the introduction of a .xxx TLD, others are emphatically opposed from a public policy perspective to the introduction of a .xxx TLD.

The ICANN Board accepted this as meaning that there was no consensus advice against approval, thus that there was no by-laws barrier to approval. The Board approved the application in March 2011. While many in the GAC were displeased with the approval of .xxx, most of the community felt that a crisis had been avoided by the diplomatic language used in the GAC advice. The ICM .xxx issues, however, set the stage for the next Board-GAC tussle relating to new gTLDs. It also set in motion work by various governments and intergovernmental groups to find a solution to what they saw as ICANN's unwillingness to do as it was told.

The ICANN new gTLD process has been a long and involved process. It is a process that began in November 2005 and has not yet completed, as the application period for new gTLD is not scheduled to begin until January 2012 and the new gTLDs are not expected in the Internet until the end of 2012 at the earliest.[21].

[19] http://iffor.org/

[20] https://gacweb.icann.org/download/attachments/1540116/20110316+GAC+Advice+on+.xxx.pdf?version=2&modificationDate=1312469527000

[21] The content of this section, with the exception of quoted materials rest on the recollections of the author who was a member of the committee responsible for recommending new gTLDs, the GNSO, from the initial setting of terms of reference, and was

The GAC involvement with the new gTLD process began early. Its first advice was sent to the ICANN Board in March 2007[22]:

> New gTLDs should respect:
>
> a) the provisions of the Universal Declaration of Human Rights which seek to affirm " fundamental human rights in the dignity and worth of the human person and in the equal rights of men and women".
>
> b) the sensitivities regarding terms with national, cultural, geographic and religious significance.

Between February 2011 and June 2011, the ICANN Board and the GAC exchanged many communiqués and had many meetings in an attempt to resolve the issues that the GAC brought up in its 'scorecard' of February 2011.[23] To almost all observers, the process of the ICANN Board and the GAC negotiating their differences was the first real embodiment of the multi-stakeholder process being applied to a decision involving both the private sector and the governments is a peer situation. Many of the issues were resolved in these exchanges, but several were not. The GAC's final advice to the ICANN Board on the approval of new gTLDs was sent on 18 June 2011 detailing issues that the GAC believed had yet to be dealt with before the program could be approved. The ICANN Board made its decision to approve new gTLD on 20 June 2011. In so far as the decision disagreed with some remaining GAC advice, the ICANN Board documented its reasons for disagreeing[24]. While much of the community was very happy with the Board's decision, some, including many in the GAC were not. This situation has opened the door for many discussions on the future of ICANN and multi-stakeholder governance. Many of the initiatives by governments to propose new models for

the chair of that group when the recommendations were approved and sent to the ICANN Board of Directors. This brief description will not attempt to describe the entire process as this is yet another candidate for studies, dissertations and books.

[22] https://gacweb.icann.org/download/attachments/1540128/gTLD_principles_0.pdf?version=1&modificationDate=1312358178000

[23] https://gacweb.icann.org/download/attachments/1540128/20110223_Scorecard+GAC+outstanding+issues+20110223.pdf?version=2&modificationDate=1312465657000

[24] http://www.icann.org/en/minutes/resolutions-20jun11-en.htm

Internet governance policy that are describe later in this report can be seen as responses to the GAC's failure to get 100% of what it wanted from the ICANN Board. It should be pointed out, that had the ICANN Board given the GAC 100% of what it wanted, the organization would have lost much of the legitimacy it has with the rest of the community as a bottom-up multi-stakeholder organization. In its decisions of June 2011 the ICANN Board was positioned at the nexus point in the emerging process of Internet multi-stakeholder governance policy.

A third area in which the GAC has given advice is the area of Whois. It is mentioned here briefly because this is another area where ICANN is at the center of a policy tussle - the pull between privacy rights and the responsibility assumed by governments to protect its citizenry. Whois is a service wherein the registrant of every domain name is required to give and maintain accurate information on name, address and contact details. Part of the Whois service mandates that this identifying information be publicly available on the Internet for anyone to obtain. Law enforcement and trademark attorneys insist on their need to access accurate Whois information instantly, in bulk and for fee. Privacy experts indicate that not only does the public display of such information put individual registrants in danger in many instances; it also contravenes privacy rights that have been codified in various international covenants and national laws. This tussle has been a fundamental ingredient of GNSO policy since the beginning and has become one of the policy jokes of ICANN.

GAC gave the following advice on Whois:[25]

> The GAC recognizes that the original function of the gTLD WHOIS service is to provide a look up service to Internet users. As the Internet has evolved, WHOIS data is now used in support of a number of other legitimate activities, including:
>
> > 1. Supporting the security and stability of the Internet by providing contact points for network operators and administrators, including ISPs, and certified

[25] https://gacweb.icann.org/download/attachments/1540132/WHOIS_principles.pdf?version=1&modificationDate=1312460331000

> computer incident response teams;
>
> 2. Allowing users to determine the availability of domain names;
>
> 3. Assisting law enforcement authorities in investigations, in enforcing national and international laws, including, for example, countering terrorism-related criminal offences and in supporting international cooperation procedures. In some countries, specialized non governmental entities may be involved in this work;
>
> 4. Assisting in combating against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.
>
> 5. Facilitating enquiries and subsequent steps to conduct trademark clearances and to help counter intellectual property infringement, misuse and theft in accordance with applicable national laws and international treaties;
>
> 6. Contributing to user confidence in the Internet as a reliable and efficient means of information and communication and as an important tool for promoting digital inclusion, e-commerce and other legitimate uses by helping users identify persons or entities responsible for content and services online; and
>
> 7.Assisting businesses, other organizations and users in combating fraud, complying with relevant laws, and safeguarding the interests of the public.

What is most critical to understand in this statement of GAC principles on Whois is the significance of this pronouncement on all privacy discussion regarding the Internet. In many ways this represents one of the sides in a tussle that is currently showing no path to resolution. It is safe to believe that this is a struggle between two fundamental positions supported by conflicting responsibilities. It is also safe to believe that it will be resolved within ICANN only when the conflict between security and privacy is resolved in other areas of society. It is not noted as a new area for research, but it will always be a rich area for research.

e-G8 and the G8 communiqué

In May of 2011, President Nicholas Sarkozy invited business leaders to a forum to discuss policy on the Internet. While many anticipated that this was one more step in governments' attempts to gain control of the Internet, many leaders in technology, the media and other areas attended the conference. The eG8 was interesting mostly for the way it exposed the governments' policy intentions and the resistance to those intentions by other stakeholders. It should be noted that while the government of France had opened the door to communication with business and technology leaders, it had mostly refused to invite civil society leaders, though some of the technology leaders, as members of civil society, did succeed in contributing a civil society perspective to the discussions.

The government leaders attending the G8 then released a set of Internet principles within its final communiqué. One can question the degree to which these principles had been pre-determined before the eG8 conference and the degree to which anything said in the eG8 affected those principles. The communiqué said the following on the Internet:[26]

> 5. We discussed new issues such as the Internet which are essential to our societies, economies and growth. For citizens, the Internet is a unique information and education tool, and thus helps to promote freedom, democracy and human rights. The Internet facilitates new forms of business and promotes efficiency, competitiveness, and economic growth. Governments, the private sector, users, and other stakeholders all have a role to play in creating an environment in which the Internet can flourish in a balanced manner. In Deauville in 2011, for the first time at Leaders' level, we agreed, in the presence of some leaders of the Internet economy, on a number of key principles, including freedom, respect for privacy and intellectual property, multi-stakeholder governance, cyber-security, and protection from crime, that underpin a strong and flourishing Internet. The "e-G8" event held in Paris on 24 and 25 May was a useful contribution to these debates.

The focal point of this statement is a realization that a balance point needs to be found between privacy and security. The Whois issue that is described as on ongoing topic in ICANN is a part of the topic that need to be balanced, among many others. It is relevant that the G8 leaders recognized the conundrum and placed all of the competing rights and responsibilities of a par. This is a small improvement on the GAC position of 2007.

OECD

Over the past years, the Organization for Economic Development (OECD), an intergovernmental organization has also begun to focus on Internet policy. Coincident with that new focus, it has also begun to explore ways in which to add a

[26] http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html

degree of multi-stakeholder participation, though decisions still rest with the governments. The OECD proposed policy statements in several areas, including:[27]

- Promote and protect the global free flow of information:
- Promote the open, distributed and interconnected nature of the Internet
- Promote investment and competition in high speed networks and services
- Promote and Enable the Cross-Border Delivery of Services
- Encourage multi-stakeholder co-operation in policy development processes
- Foster voluntarily developed codes of conduct
- Develop capacities to bring publicly available, reliable data into the policy-making process
- Ensure transparency, fair process, and accountability
- Strengthen consistency and effectiveness in privacy protection at a global level
- Maximise individual empowerment
- Promote Creativity and Innovation
- Limit Internet intermediary liability
- Encourage co-operation to promote Internet security
- Give appropriate priority to enforcement efforts

In some of the discussions that ware included on these points, for example, in the case of promoting free flow of information, the OECD cautioned on the need to "to work towards better protection of personal data, children online, consumers, intellectual property rights, and to address cybersecurity. In promoting the free flow of information governments should also respect fundamental rights."[OECD 11] In other words, once again reintroducing the tussle between freedoms on one hand and prohibitions in the name of security on the other.

The civil society participants in the OECD process, a group of over 80 organizations represented by the Civil Society Information Society Advisory Committee (CSISAC) released a separate statement that rejected several of the OECD's principles especially those dealing with freedom of expression, the free flow of information, with the responsibilities of Internet Service Providers (ISPS) to act as Internet policemen, and allowing for filtering of lawful content. [CSISAC 11]. It is interesting to note that although one of the principles concerned the importance of

[27] http://www.oecd.org/dataoecd/40/21/48289796.pdf

the multi-stakeholder process, civil society was forced to issue a separate minority statement. The OECD is to be praised for supporting the multi-stakeholder model, but they have a distance to travel yet on this road within their own organization.

The European Commission

Neelie Kroes the Vice President and Digital Agenda Commissioner of the European Commission proposed a set of principles for the Internet in June of 2011 she termed a "Compact for the Internet"[28]:

> - **C**ivic responsibility. On the internet, we are not atoms. And just as when we are out in "normal", offline society, we bear responsibilities to each other which go beyond the purely legalistic, especially when there is harmful behaviour out there.
> - **O**ne internet – we should safeguard the idea that, on the Internet, every node can communicate with every other. This unity is what allows the Internet to thrive in the way it has; we need to avoid fragmentation.
> - **M**ultistakeholder governance of the Internet – because the participation of all stakeholders in policy making is a good one, which we support in this domain and others.
> - **P**ro-democracy. With the right tools – like open access to Government information, and platforms for collective action – the Internet can become an instrument supporting democratic life, and we should promote it as such.
> - **A**rchitecture matters – the architecture of the internet is fundamental to its dynamics. I'm sure the architecture will change in the future as new challenges emerge – but we need to be aware of the implications that different models might have.
> - **C**onfidence of users is a prerequisite: barriers to confidence and trust are barriers to access. If we don't solve problems like protection of personal data, privacy and identify; like online safety for children; like cybercrime and resilience of the network, then people will be turned off the net and we won't unlock the Internet's potential. And finally,
> - **T**ransparent governance – so that the multistakeholder model doesn't fall apart. In particular we need to be transparent about the role which government representing their citizens play, and ensure that those views aren't ignored.

Many Internet governance policy watchers saw this statement as a direct expression of the governments' displeasure concerning the ICANN .xxx and new gTLD decisions discussed above, specifically the reference to "ensure that those views aren't ignored". It was also seen as a direct challenge to ICANN independence and as pressure on the board to change decisions concerning the new gTLD program before the January 2012 start of the program.

Since then, the European Commission has been far more aggressive in putting forth

[28] The bolding of the first letter of each on the principles is quoted.

principles on the policies by which the Internet should be governed in groupings like the GAC. Just recently a group of papers by the Information Society and Media Directorate-General were leaked. These papers included the following points [McCarthy 11] :

- A government veto over any new Internet extensions
- The creation of a list of names, drawn up by governments, that would be banned from registration
- Significant structural changes at overseeing organization ICANN, including at Board level and in the crucial IANA contract
- An obligation for ICANN to follow governments' advice unless deemed illegal or damaging to the Internet's stability
- Two new bodies to oversee ICANN decision-making and finances

These leaked documents would represent the greatest threat to date of ICANN's independence and its bottom-up multi-stakeholder process. The Internet governance policy proposals in these documents would establish international government oversight over ICANN's decisions. As discussed later in this paper, this policy action could have technical consequences and would certainly cause a tear in the structure of Internet governance, as it has existed to date. May in the private sector, civil society and the Internet technical community consider these threats to be the biggest policy challenges facing the Internet today, and probably into the future. As such these relate to possible research on the appropriate role for governments participating in multi-stakeholder governance.

Council of Europe Principles

The Council of Europe (COE) has been developing a set of principles for the past few years. This set of principles originated with a set of principles originally being developed in one of the Internet Governance Forum's (IGF) groups working on an Internet Bill of Right, a group in which members of the COE were active.

While the principles have not yet been approved, the COE has used an open model in the process of developing the principles that is very much oriented to multi-stakeholder participation. While the decision to accept the principles will rest with government ministers as the COE is a intergovernmental organization, it appears to be accepting the advice of other stakeholders [COE 11]:

> ... the Committee of Ministers of the Council of Europe:
>
> – welcomes the Internet governance principles progressively developed by stakeholders in various policy processes and which, for the purpose of this document, are articulated in the form set out below;
>
> – declares its firm commitment to these principles and underlines that they should be upheld by all member states in the context of developing national and international Internet-related policies;
>
> – encourages other stakeholders to embrace them in the exercise of their own responsibilities.

The COE principles currently address the following areas [COE 11]:

1. Human rights, democracy and rule of law
2. Multi-stakeholder governance
3. Responsibilities of states
4. Empowerment of Internet users
5. Global nature of the Internet
6. Integrity of the Internet
7. Decentralised management
8. Open architecture
9. Network neutrality
10. Cultural and linguistic diversity

Report of the UN Special Rapporteur

In May 2011, the UN's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue gave a report to the 17th session of Human Rights Council. Mr. La Rue's report has been welcomed by many in the human rights advocacy area of the Internet as he addresses some of the major issues related to human freedoms, including expression, access to content and access to infrastructure. In his conclusions he covers the following: [LaRue 11]

> The Special Rapporteur emphasizes that there should be as little restriction as possible to the flow of information via the Internet, except in few, exceptional, and limited circumstances prescribed by international human rights law. He also stresses that the full guarantee of the right to freedom of expression must be the norm, and any limitation considered as an exception, and that this principle should never be reversed.
>
> The Special Rapporteur is cognizant of the fact that, like all technological inventions, the Internet can be misused to cause harm to others. As with offline content, when a restriction is imposed as an exceptional measure on online content, it must pass a three-part, cumulative test: (1) it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); (2) it must pursue one of the purposes set out in article 19,

> paragraph 3, of the International Covenant on Civil and Political Rights , namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). In addition, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory. There should also be adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application.
>
> A. Restriction of content on the Internet
>
> 1. Arbitrary blocking or filtering of content on the Internet
> 2. Criminalization of legitimate expression
> 3. Imposition of intermediary liability
> 4. Disconnecting users from Internet access, including on the basis of intellectual
> 5. Cyber-attacks
> 6. Inadequate protection of the right to privacy and data protection property rights law
>
> B. Access to the Internet and the necessary infrastructure

In relation to access, he calls "on States, in particular developed States, to honour their commitment, expressed inter alia in the Millennium Development Goals, to facilitate technology transfer to developing States, and to integrate effective programmes to facilitate universal Internet access in their development and assistance policies." [LaRue 11] the recommendations he makes are the most stringent made by anyone in a position of responsibility in an Intergovernmental organization on the type of policies that should be implemented on the Internet.

More Proposals on Governance Policy Principles

This report has only touched on a few of the efforts to develop set of governance principles for the Internet, and focused mostly of the activities that included governments. For example two of the major contributions to the parade of governance principles, a proposal by IBSA[29] for oversight of all critical Internet resource organizations, and a proposal by the permanent representatives of China, Russia, Tajikistan and Uzbekistan to the United Nations[30] recommending an

[29] IBSA: India, Brazil, and south Africa, http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf

[30] http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm

International Code of Conduct for Information Security that makes all Internet governance decisions subject to government approval, are not discussed. Also not discussed are the "10 Internet rights and principles"[31] recently compiled by the Internet Rights and Principles Dynamic Coalition of the IGF or the Brazilian Bill on Internet Rights.[32] The reason that one set over another set of policy principles was included in this report has to do with trying to pick just a few that suggested the primary issues in the debate between those who believe in the participatory democracy of multi-stakeholder governance and those who look for government control of Internet governance.

It should be obvious from the discussion that there is still a great debate concerning Internet governance policy. One of the outcomes of the recent IGF meeting in Kenya is a proposal that the various stakeholders begin to work on a coordinated set of governance policy principles for the Internet before the 2012 IGF meeting. Research on the degree of agreement and disagreement between the various sets of principles as well as their relationship to various political theories would also be a valuable contribution from a research institute.

Continuities and Discontinuities

There are obvious continuities and discontinuities between the principles used by those who created and continue to create the Internet and it applications, and those who are attempting to create principles by which to govern the Internet. In one case the underlying principle is openness and the freedom to express and create. In the other, while giving voice to the protection of basic liberties it is always modulated by a requirement to control and to limit. The difference between the principles put forward by Internet technologists and those put forward by governments looking to control the network is a reflection of the tension that one finds in the ICCPR:

> Article 19

[31] http://irpcharter.org/campaign/

[32] http://direitorio.fgv.br/sites/direitorio.fgv.br/files/Marco%20Civil%20-%20English%20Version%20sept2011.pdf

> 1. Everyone shall have the right to hold opinions without interference.
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
> (a) For respect of the rights or reputations of others;
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Put simply: when are limits on freedom of expression and association permissible under international law and when do these limitations apply to a private corporation coordinating a public space?

One thing that can be predicted with certainty is that this dynamic will continue to play out between technology and governance policy for the foreseeable future. The differences that are seen in theoretical frameworks between technology and governance policy are often attributed to ignorance or the striving for power. It is possible, however, to attribute them to the tensions that run through human beings, which can be described as "fault lines." The task then becomes an attempt to identify and map out the intersections of these different understandings of the world [Ricoeur 92]; technological, political or otherwise. Borrowing from Ricoeur's dialectic, the motivation for the ongoing research is to find the unity in the continuities and discontinuities of technology and governance. As with any dialectic, snapshots can be taken along the way and there are annealing points that are useful in a practical sense, but the process is ongoing. This report is just one such snapshot at this moment in time.

Technology Projections

This part of the study investigated various technological innovations that are either in the late stages of research and development or the early stages of implementation and deployment. This section of the report discusses the technology and the possible impact of the technology on policy discussions.

In the study, two things became apparent. First almost none of the developments that the public sees as new are as new they seem when the public first learns of them. Many are the reflections of previous trends that did not succeed because the underlying technology did not exist. Fast CPUs and memory as well as increased bandwidth and storage capacity have made many of today's innovations possible. This report does not discuss the continuing advancement of underlying technology based on Moore's law[33] and its corollaries of bi-annual doubling in speed and capacity, but every technological advancement is somehow enabled by that progress. The upshot of this is that many of today's innovations were first thought of years before they made an appearance on the market.

The other realization is that there aren't one or two big changes that will necessarily be the cause of the need for policy work, but rather lots of more distinct changes that will contribute to the complex set of issues that become part of the social sphere and lead to policy discussions.

The author of this report is under no illusion of having done an exhaustive search on new technological advances or the full scope of global research on new technology and architectural frameworks in this brief study. Moreover, only a small selection of what was found is included. In addition to only having scratched at the surface of the plethora of ongoing research projects, such study needs to be longitudinal and needs to follow major research trends over a long period to understand not only their affects on the policy, but policy's affect on the research. One recommendation for the Institute for Internet & Society is that one or more of the topics mentioned in this report be subjected to longitudinal study.

It must also be noted that although the earlier parts of the paper posited the inextricable link between the technological process and the policy process, this

[33] Gordon E. Moore, one of the founders of Intel, described the tendency of the number of transistors that could be placed in an integrated circuit to double every two years. This correlates with progress in digital components, including for example memory, processing speed, or pixels in digital cameras to double in capacity every two years. http://en.wikipedia.org/wiki/Moore's_law

report is only a snapshot on one moment in that continuous process and it is looking only at the effect that technological change including any possible ongoing changes in the architectural framing, might have on the policy process. Many of today's technological improvements, for example the work done in network security, have been driven by policy imperatives. The effect of past policy on motivating today's mix of technology projects was not within the scope of this brief study, but would be very much in scope of historical studies and on exhaustive longitudinal studies focused on the interplay between technology and policy. In some cases, the description of the technological innovation will, however, include a brief mention of relevant policy pressures that affected the development, but in no case is this discussion complete.

Clean-slate research versus evolutionary research

There has been a continuous discussion for twenty years or more on whether future Internet research should take a clean-slate approach that designs a new network architecture and protocols to replace the current Internet or take an evolutionary approach that changes parts of the Internet without affecting other parts. Both approaches are being funded in the Europe, in the US and elsewhere.

On the side of the clean-slate approach are arguments on the need to create a network that is worthy of society's trust where pervasive security problems such as spam, denial-of-service-attacks and phishing can be prevented by technology that is built into the network. Additionally a clean-slate approach would allow for a genuinely mobile architecture, a well thought out service model adapted to the streaming requirements of today's applications and the correction of many other faults and mis-features in today's network. [Rexford 10]

On the side of the evolutionary approach, there is a concern that replacing the network with a new network would be impossible, how does one have a 'flag day'[34]

[34] a *flag day* for the Internet is the day that one Internet is turned off, and the new one is turned on. There was a flag day between the NCP predecessor to the Internet and the introduction of the IP based Internet.

for a new Internet? Additionally, the notion that a new network could be created that would have none of the ills of the current network is optimistic at best. It is difficult to say which new problems a new network would create.

A prediction that can be made is that the research efforts on both the clean-slate approach and the evolutionary approach will continue, with the clean-slate approach bringing computer science new insights and technology that can be integrated into the existing network and the evolutionary approach improving the existing Internet in a stepwise fashion. In terms of governance, both of these approaches bring challenges. With the clean-slate approach the policy concerns could be solved in the architecture, if only the designers of the new architectures take them into account and if the tussle of policies does not complicate the process of design beyond what is manageable. With the evolutionary approach, the researchers and policy makers can, if they are willing, work together on the adjustments needed one at a time, and while this would not see the Internet 'fixed' in its entirety, it would help to generate improvements.

In the rest of this section, there will be a distinction between the efforts that lean toward clean-slate, and those that lean toward an evolutionary approach. Only in an academic sense, would the distinction be complete, i.e. that some project would be purely clean-slate or purely evolutionary. In the give-and-take world of engineering, there will always be a mix. Additionally, there are few projects that are clean-slate in terms of the entire network, most focus on some part of the layering without touching other layers. For example there can be a clean-slate approach on the network layer that would have only tangential effects on the application layers, or vice versa.

Peer-to-Peer Technology

Peer-to-peer (p2p) is more of a communications model than a technology or architecture. It is, however, a model that is beginning to be part of many projects, both clean-slate and evolutionary. Its first applications were in file sharing that disturbed copyright holders such as the motion picture industry and in the technology that made the search for extraterrestrial life SETI@home possible. It is an engineering method that does not require any changes in the network and can operate at the edges of the network. Both of the early applications sat on top of the lower layers of Internet as we know it. This technology continues to evolve and is finding more and more uses. For example, while BitTorrent is blocked or has jitter[35] injected by some ISPs because it is frequently used to download movies and music, it is also used in industry to distribute bulk data such as software updates and news feeds. Skype is probably the most famous of the p2p technologies, though many companies filter it because it uses their company resources to route its information without explicit permission to do so. As will be discussed in some of the discussions below, p2p is seen as a useful model for the possible creation of a new Internet domain names information system. Such a use would have more of a clean-slate effect than an evolutionary effect. Two of the key aspects of p2p are that it lowers the barriers for innovative services by using the computing resources of many cooperating users and that it is truly decentralized. This last aspect, its decentralization, is also one of its major liabilities as this causes commercial angst and legal challenge. [Rodrigues 10]

Clean-State Technology

In this section, only a very few of the many clean-slate technologies are discussed. In fact none of the clean-slate technologies discussed involve a complete revamping of the network. Rather they involve activities that take a radical look at new ways of looking at one or more of the layers within the Internet's layered architecture. None of the activities described would violate the hourglass model or other Internet principles such as the end-to-end principle. In a sense they are all innovations that respond to a real need for a change to the Internet. It is also important that each of

[35] Jitter is a technical term that refers to rapid changes in frequency with which data is transferred. Because jitter requires extensive use of buffering technology to smooth out the reception of messages, it makes the use of some technology difficult.

them will involve a revision in the way some governance policy issues are approached.

Jon Crowcroft, the Marconi Professor of Communications Systems in the Computer Laboratory, of the University of Cambridge had the following comment on Future Internet research:

> I'm so Bored of the Future Internet (FI). There are so many initiatives to look at the Internet's Future, anyone would think that there was some tremendous threat like global warming, about to bring about its immediate demise, and that this would bring civilisation crashing down around our ears
>
> The Internet has a great future behind it, of course. However, my thesis is that the Future Internet is about as relevant as Anthropogenic Global Warming (AGW), in the way it is being used to support various inappropriate activities.
>
> Remember that the start of all this was not the exhaustion of IPv4 address space, or the incredibly slow convergence time of BGP routes, or the problem of scaling router memory for FIBs[36]. It was the US research community reacting to a minor (as in parochial) temporary problem of funding in Communications due to slow down within NSF and differing agendas within DARPA. [Crowcroft 10]

Likewise, the European Commission's Future Internet initiative was a reaction to the US research agenda. "It is therefore time to strengthen and focus European activities on the Future Internet to maintain Europe's competitiveness in the global marketplace." [Bled 08] Coincidentally, the Bled Declaration was signed by the 95 projects that were funded by the European Commission. Of course not all of the funded projects are just excuses for funding. Some do support real goals to solve real problems in both the European and US future Internet research portfolios.[37] This section discusses a few of those efforts chosen because of their possible affect on policy discussions.

Information Centric Networking

Information Centric Networking (ICN) is one of the major goals in research on the Future Internet in both Europe and the US where there are at least six funded projects. The model differs from the current Internet model in that they focus on the

[36] FIB is the acronym of forwarding Information Base, which is the data structure a routing protocol builds so that the forwarding components of a router know how to forward each packet that comes in.

[37] Full Disclosure, the N4C project in which the author was involved and which paid the author's salary at the time was one of the signatories to the Bled declaration.

placement and movement of information or content and not the mapping of computer-to-computer information as is currently done in the Internet.

The closest current technology to ICN are today's Content Delivery Networks (CDN) running over today's Internet such as the web acceleration done by systems such as Akamai. The research on ICN has been made necessary by the amount of information that is transferred in today's network. Services such as Akamai attempt to bring information closer to the requestor through mirroring the information and then manipulating routing table entries as needed. This has the additional benefit that it avoids the concentration of request/response traffic at a single source in the network. Unfortunately, because they are still layered over the normal Internet protocols, they suffer from latency and packet loss. Increasingly CDN networks are beginning to use private networks to connect their caching servers. It can be argued that current CDN networks violate Internet core principles by modifying routing table entries based on data content requirements. The techniques can also be considered to violate the integrity of information in that the responses to the same query can be different, depending on where the query is made. Users may consider this to be a benefit (e.g. if a query form is delivered in their native language) but it may also be a threat to transparency and integrity of information as the user has little control over the process and may be unaware of subtle changes in the delivered information.

The current state of research in ICN was recently discussed at a seminar in Dagstuhl [ICN 11]. The ICN community is currently investigating the use of Delay- and Disruption-Tolerant Networking[38] (DTN) [RFC4838] techniques. ICN and DTN are highly synergistic because DTN provides in-network caching to overcome network disruptions; the cached data provides a resource that can be exploited by ICN. DTN also has the advantage of being a message oriented architecture that is independent of the underlying infrastructure. So while it can work over the

[38] It is interesting to note, that one of the earliest proponents of the new DTN architecture was Vint Cerf, considered one of the creators of the Internet.

Internet, it does not need to be layered on the traditional Internet and can span several networks, including the Internet.

Topics that were discussed in the recent Dagstuhl seminar included [ICN 11]:

- The relationship of networking architecture innovation vs. so-called over-the top approaches in the application layer
- The support of an Internet of Things and Services by an ICN architecture
- How to migrate towards an information centric architecture, and whether and how to use it as a migration enabler for, e.g., an IPv4/IPv6 technology step
- The role of and needs for naming and addressing and name resolution systems, along with the necessary security aspects of a naming scheme; a fundamental dichotomy between flat and hierarchical naming schemes that needs to be resolved
- Efficiency and robustness of ICN data dissemination vs. specific content distribution overlay solutions
- The desirability of using s transport protocols for ICN vs. the use of standard protocols like TCP or disruption tolerant protocols like the DTN Bundle protocol
- The integration and placement of caches inside a network
- Can the introduction of a new ICN architecture enable new types of applications that were too complex to create/operate/deploy/maintain in traditional networks?

The change of paradigms would radically change the nature of the network. IP addresses would lose their pre-eminent role and names would become more important. Additionally, the ICN would be far more decentralized than the Internet is today, and an authority such as ICANN that provided centralized name assignment would lose much of its relevance. Though DTN could be used over the traditional Internet, and probably would originally be implemented in this manner, over time the need for this layering would wither away. One Internet architect who is working in this area, Elwyn Davies[39], views the possible change to ICN over a DTN layer as one way that the next revolution in communications systems could proceed. He points to an approximately twenty-five (25) year cycle in which each new technology is first layered on the older technology and then becomes the

[39] Much of this section is based on conversations with Elwyn Davies. Elwyn Davies was a member of the Internet Architecture Board, and was the lead architect of a DTN project that produced technology for communications challenged communities.

primary communications technology, as the infrastructure is adapted to suit the technology until it becomes the underlying technology for the next innovation. This happened with the manual telephone switching that was replaced first with local automated analogue switching, then replaced by global automated switching (trunking), replaced by digital switching, and then by internet technology. Each of the changes in the form of communication available to the population served as a driver for social change and with it brought new demands for governance policy.

Given the early stage of development in ICN/DTN technology, this technology development and its relationship to communications governance policy is a good target for longitudinal study, though this study would benefit from a prior study on the cyclical history of communications systems and the corresponding changes in governance policy that occurred during each cycle.

De/re-construction of the official DNS root

For the past few years the motto of ICANN has been "One world, one Internet". This is meant to convey that there is just one set of Internet numbers and just one set of Internet names. This is a belief that conveys an accepted operational principle that there can only be one set of names and numbers or else the Internet will cease to function.

Alternate roots[40], also referred to alt roots, are a topic that is often mentioned in whispers. They are both a threat and a promise: a threat to the status quo and a promise to those outside of the status quo. Fifteen years ago, before the creation of ICANN, a lot of work was done on new roots. The fear of these new roots was enough to inspire the governments of the world to first wake up to the importance of the Domain Name System (DNS).

About five years ago during the WSIS process, it became apparent that various

[40] Much of this section is based on personal experience and information gleaned from extended email conversations with Karl Auerbach (www.cavebear.com/) Mr. Auerbach is the first and only person to have been elected to the ICANN Board of Directors from North America and is a Henry C. Yuen Fellow of Law and Technology at the California Institute of Technology (CalTech) and Loyola Law School. I am responsible, however, for what is written.

governments had begun thinking about establishing their own roots. When the Internet Architecture Board (IAB) saw a possibility that the Internet Engineering Task Force (IETF) would be asked to start working on a technical response to the problem of alternate roots, the IETF decided that it could not do so, for to do so would be to give permission to those who wanted to fragment the root. In [RFC2826] the IAB presented several reasons for discouraging any work in that direction.

> To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore it is not technically feasible for there to be more than one root in the public DNS. That one root must be supported by a set of coordinated root servers administered by a unique naming authority.
> Put simply, deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations, against the will of the web page designers.
> This does not preclude private networks from operating their own private name spaces, but if they wish to make use of names uniquely defined for the global Internet, they have to fetch that information from the global DNS naming hierarchy, and in particular from the coordinated root servers of the global DNS naming hierarchy.

About six months ago, during the debate on .xxx in ICANN, one of the distinguished sages of the Internet[41], argued that it was important to avoid approving names that countries might filter on, because that might lead to the splitting of the root[42], something that had to be avoided at all costs. The logic was that if many countries filtered on a TLD, the registry responsible for that TLD would be tempted to use an alternate root to circumvent the filtering countries' filters. Others have argued that those applicants in the new gTLD process soon to be initiated by ICANN, who may be rejected by ICANN for new gTLDs after having spent hundred of thousands of dollars or more on the applications process and all that entails, may be enticed to join alternate roots if these can show how they might be used reliably and profitably. In other words, no matter what happens in the new gTLD process, the expansion of the name space might just be the

[41] This was related in a private conversation and as this expert has not been consulted for permission to quote, he is not named.

[42] Spitting or fragmenting the root is another name for the use of alternate roots

impetus needed for new root systems.

Fragmentation of the Internet

As mentioned above the most frequent argument one hears against the idea of alternate roots or alternate Internet naming systems is that this will fragment the Internet. This claim is difficult to substantiate on any basis other than belief in the tenet. Indeed, there is always a risk when a creating something new in the Internet, precautions would need to be taken in creating alternate roots or Internet naming systems to keep them from creating problems for the Internet.

As discussed in the first section of this paper, what holds Internet together as a single system is the set of protocols, designed according to the set of Internet technology principles allowing diverse networks to communicate with each other. What also holds the Internet together is a common addressing scheme as defined by the Internet Protocol (IP). If creating a new, incompatible addressing scheme, IPv6, did not fragment the Internet, it is hard to see how a new naming system could.

Stepping back, it is important to remember what the domain name system does. Its primary task is to create a set of people-friendly names to reference the IP addresses that identify various machines, services and locations on the Internet. There is nothing magical about the domain name system, it is sequential set of questions and answers for translating a name from one form, one friendly to human understanding, to another form, the pseudo-numbers used in IP addresses as a means of identifying systems and their location on the network. The fact that the Internet has names is important, not only for ease of use for the Internet's users, but for providing a means by which the same name can point to the same entity even if it moves to a new location. So the Internet needs names, and needs names to be reliable unique references.

Saying that an alternate root can kill the Internet is as reasonable as saying that the production of a new phone book will destroy the telephone network. Yes, if developers are careless in creating the new phone book it could confuse things, Who would use an erroneous phonebook? Likewise, if an alternate root did not give accurate information or made it impossible to reach systems that could otherwise be reached, who would use it? It is understood by everyone thinking about alternate roots that anything they created must work without making the Internet less stable.

The possibility of other naming systems brings up two questions: what are the requirements for an alternate root and if people have worked on alternate roots over the years, why aren't there any functional alternate roots in today's Internet?

To actually build a new domain name system would be difficult. Deploying one would be even more difficult. Some of the basic requirements that alternate root system developers have posited for their systems include:

- No overlap with any other domain system;
- Backward compatibility, so that the existing system continues to work;
- Security;
- Privacy;
- Scalability.

There have been over a dozen alternate root schemes over the years. Some are still in existence but many have ceased operations. Yet none of these alternate roots have ever reached any degree of acceptance on the Internet. The question is ″Why?″ Most of the speculation on "why" is that none of these have offered anything that the users weren't getting from the ICANN single root. With no motivation to switch, why would one switch?

Beyond the DNS to new naming architectures

One possible reason for not extending the current DNS system to support alternate roots is the fragility of the current DNS. With the addition of IPv6 record support, DNSSEC, domain names in languages and character sets other then English with its Latin script (called Internationalized Domain Names - IDNs) [RFC3490], and now the addition of an undetermined number of new names that may be filtered, some experts are cautious as to how many more changes the current DNS can take. This may be the actual liability with the DNS: it is not that alternate roots will be confusing, but rather that they may put extra stress on an old and fragile system.

For, as well as other, reasons, there have been various efforts to create other naming systems that can run parallel to the DNS and maybe eventually replace the current DNS. One of these is the Object Name Service (ONS) [ONS V1.0.1] system that is being deployed both as a federated model layered on the existing DNS system and as point-to-point (p2p) system using distributed hash tables. In the ONS there will be various peer roots instead of single root. The ONS is taking this approach because they are looking for a way to do naming in the Internet of Things, which exists on a multitude of networks, some of which are part of the Internet and some of which are not part of the Internet as currently defined. The ONS allows the network to grow beyond the Internet as we know it to become a greater synthetic network, a greater Internet. The ONS, therefore, may provide a key motivation for a new root.

The ONS is only one of the models developing a p2p based Internet naming system. Another is the GNUnet framework for secure peer-to-peer networking. Another example, in 2010, in response to seizure of 80 domains by the US government, an effort by Pirate Bay organizers was initiated to create "A free, decentralized, and open DNS system!"[43] [DOT-p2p] using p2p technology. This is but a few of latest of many efforts for new DNS systems or alternate roots that have been proposed in the last 10 years.

Another approach is related to the ICN and DTN technology described elsewhere in this paper. This proposal defines a DTN Uniform Resource Identifier (URI) [RFC3986] that could be used to define names under authorities in addition to ICANN for addressing within a network. An Internet draft using the Authority

[43] This particular effort has either gone dormant, or back underground, after a fair amount of media attention. It is just one effort in a long series of efforts.

component of Uniform Resource Identifiers (URI) [RFC2396] was produced to define a scheme for defining naming outside of the ICANN name-space for the use of Delay/Disruption Tolerant Networking (DTN)[44]. Work on this is still pending, but is being used experimentally.[ID URI]

One of the predictions for future technology is that there will continue to be work of new and alternate naming methods, including new DNS roots and non-DNS methods of naming. Will there be alternate roots that can become more than a hobby for some developers? This remains to be seen, but it is quite possible if the correct conditions occur. But, not only will there need to be a reason for users to want to use them, and an automatic way for these users to modify their computers to access these alternate roots, there will need to be some support from the Internet Service Providers. Additionally it will be necessary for these systems to show that they are not only compatible with the existing ICANN system, but they are at least as reliable as the ICANN system as it has proven itself to be a competent regulator of domain name services. For an alternate root to actually make it on the Internet, it will have to prove itself worthy of being deployed and used. This is not an easy path to success as the history of efforts since the late 1980's shows.

Will there be a replacement for the DNS system? Certainly at some point, the DNS will be replaced. It has been a critical component on the Internet since the late 1980's. It has grown and been stretched to support functions beyond any that were conceived of when it was created. It is a success. Can the DNS last another 10 years? Certainly - there is an army of brilliant and dedicated engineers keeping it going. Can the DNS last another 20 years or more? That is difficult to answer. When one considers the number of different names that will exist with the addition of new TLDs and the requirements of mobility and security, it is difficult to imagine that that the current DNS system will remain adequate to the task for more than another decade or two.

[44] http://tools.ietf.org/id/draft-irtf-dtnrg-dtn-uri-scheme-00.txt

Given today's policy focus on ICANN as the one naming authority, with governments, intergovernmental groups and multi-stakeholder policy groups focusing on how to control and/or work with ICANN, the creation of a new, and pervasive, method of naming would throw much of that policy effort into confusion. In fact the 'killer app' for the creation of a new naming system might just be the response to ICANN and the desire so many governments and intergovernmental organizations have to replace it. The 'killer app' might also be the fear technologists have of a government gaining control of the ICANN managed naming system. The root and its construction is one of those cases where it is difficult to tell which will be the driver: the availability of new technology, or the two contravening influences, the drive to control the internet and the drive to keep the Internet from being controlled.

Evolutionary Technology

Herbert Simon was among the first to argue convincingly that the design of artificial systems should, and often is, subject to the same principles with natural and biological systems. [Simon 96] Among biologists, an evolvable system has been understood to require several attributes, including robustness and modularity. [Dovrolis 10] Robustness in the biological sense is related to the stability of the system and requires an invariance in the way a particular function works. This is one of the properties expected in a protocol; once it is standardized it does not change and designers can depend on that invariance. In terms of modularity, there is a parallel to the layer structure of the Internet were every system is built out of a layer of protocols, where one can change without causing changes in the others. While it is possible that the invariance of protocols would appear to be contradictory to the evolution of a system, combined with modularity, it is what actually enables the evolution of a system. The stability of some modules allows other modules to change in the face of environmental pressure. The tendency of a system to remain static for a while and then change is called "punctuated equilibria"

[Gould 02]. An example of punctuated equilibrium in the Internet is the TCP protocol. Despite the fact that numerous other, more powerful and specialized, transport layer protocols have been developed in the last ten years, none of them has significant use in the Internet compared to TCP. The same can be said for IPv4 at the network layer. It is this equilibrium that has allowed other protocols to evolve. [Dovrolis 10]

All of the examples in this section run over TCP/IP. They involve changes in the Internet that occur at the speed at which the users of the network adopt them, but they are relatively easy to adopt as they do not require any structural change to the network. This is markedly different from the examples in the section on clean-slate development that requires changes in many parts of the Internet.

Cloud Computing and software-as-a-service

Some writers consider cloud computing to be a "fundamental shift in the delivery of information technology services that has permanently changed the computing landscape" [Srinivasan 11]. This may be hyperbole, as the architectural model bears some resemblance to the model of centralized computing and storage that existed before the introduction of the Personal Computer in the 1980's. It has, though, been transformed through technology and the Internet. And instead of working on a central computer, it is marketed as Software-as-a-Service (SaaS) [Narasimhan 11]. Additionally, a large number of corporate road warriors have been using Virtual Private Network (VPN) access to data services for at least a decade. Nonetheless it is a significant change from the way work has been done by most people for most of the past two decades. And certainly the underlying technology is different.

In contrast to many, though by no means all, of the technical advancements reviewed in this study and discussed in this report, cloud research as been largely driven by industry, such as Microsoft, Amazon, Google and others. The resurgence of centralized data storage in the cloud has taken place rather quickly, within less than a decade. One of the drivers for cloud computing is said to be economies of scale. [Srinivasan 11]

Among the leading Cloud/SaaS applications today are: [Narasimhan 11]

- Google Gmail/Calendar
- Microsoft Dynamics: Enterprise Resource Planning (ERM) and Customer Relationship Management (CRM)
- NetSuite: ERM and Financial Software Suite
- Oracle CRM on Demand
- RightNow: CRM
- Salesforce.com: CRM
- SuccessFactors: Business Execution Software
- Workday: Enterprise Business Management
- Custom applications of Force.com, Google App Engine or Windows Azure

It is clear that the main use today of the Cloud and SaaS service, are business applications. Among business users, the biggest concern seems to be the dependability of the service (e.g. the outcry over the recent service outage of Microsoft's services), its features and the ability of one cloud to integrate with another. [Narasimhan 11]

Of these applications only Google Gmail and Calendar are used largely by individual users. Not included in survey were applications such as Google Docs that are beginning to see more use, but still do not approach the degree of use found in commercial Cloud/SaaS applications.

Data Confidentiality in the Cloud

While business may, and perhaps should have, privacy and confidentiality concerns about cloud usage when not using a private cloud, individuals most certainly do. In a cloud, as in the centralized services of the past, the service provider has access to all of the data and could misuse that data. One of the concerns is accidental or deliberate disclosure of data in the cloud. [Ryan 11]

Various technological solutions are being developed to aid in securing the data within the cloud. One set of solutions rests on the virtualization of the systems storing the data in a virtual machine environment. A virtual machine gives a user unshared access to the resources they are using. In using virtual machines[45], mechanisms can be set up such as whitelisting[46] and blacklisting[47] of guest kernel processes[48] that can be used to make sure no one other than authorized processes of the subscribed user has access to the data, eliminating many of mechanisms normally used in viral attacks on the Internet. Of course this does nothing to prevent access by the service provider who always has access by having access to the actual hardware and its data storage. [Anthes 10]

Encryption is often described as a solution for the confidentiality problem. While the technology is being developed, it is still very difficult and computationally very expensive to encrypt and decrypt all of a users data locally, especially when using a netbook[49] or a tablet. Since the problem of encrypting data as it crosses the Internet is a solved problem, research has worked on ways to encrypt the data in the storage systems while maintaining a structure that allows ease of access by the remote user. Some of the research involves encrypting data in place using a method called "fully homomorphic[50] encryption". While this is still more research than a practical solution at this point, it is the type of solution that will be seen in the next decade. A recent development that appears to have promise is a called 'Cryptographic Cloud storage,' which is being defined by Microsoft Researchers. They "describe a virtual private storage service that aims to provide the security of a private cloud and the cost savings of a public cloud. Data in the cloud remains encrypted, and hence protected from the cloud provider, court subpoenas, and the like. Users index their data, then upload the data and the index, which are both encrypted, to the cloud. As needed, users can generate tokens and credentials that control who has access to what data."[Anthes 10]

[45] A virtual machine is either an emulation (software) or virtualization (hardware) of a computer system. It is a method used to sub-divide a single physical computing device into a number of private smaller computing devices.

[46] Whitelisting is an access control method that relies on a list of which users or processes are permitted to access data.

[47] Blacklisting is an access control method that relies on a list of which users or processes are not permitted to access data.

[48] Kernel processes are, generally, those process that run in the most protected parts of an operating system and that have access to the physical parts of the system.

[49] Small lightweight, low power laptops.

[50] homomorphic means that even after something is transformed as through cryptography, it maintains the same structure.

As secure as cryptographic cloud storage sounds, it is hard to imagine a world where such a technology would not be met by political and legal demands for the deposit of a token in the hands of law enforcement, eliminating the desired security. The issue of government demand for cryptographic keys, tokens and credentials is one of the policy areas that will need to be discussed in the next decade. As cryptographic methods improve, government demands for methods to circumvent privacy will be demanded. Yet, if any government can demand the ability to bypass cryptographic security and any government can decide for itself, as a sovereign matter, who it gives access, it might be argued that there is no such thing as cryptographic security.

Do you know where your data is?

Given government sovereignty issues, one of the major policy issues of cloud computing is a cross border issue. When data crosses a border, it becomes subject to different privacy and other regulations. A user may not even know where their data is stored and under what rules that data can be accessed by authorities. Among the issues that governance policy may look at is whether there should be an obligation to extend a user's control of their data to include control of its location. At the very least policy may require user notification of where their data is stored and what laws and regulations it is subject to.

Several countries are looking at becoming data havens, i.e. places where data can be stored safely. This has, however, turned out to be more difficult than it might seem as many countries have signed treaties that oblige them to reveal data content under certain conditions. Resolving the issues surrounding data havens will also be a topic of policy discussion during the next decade.

Internet of Things

The Internet of Things (IoT) refers to the possibility of interconnecting objects in common use to each other and to other network elements. It is a network where an object and its subcomponents can be tracked for their entire lifecycle from manufacture to distribution, through personal use to disposal. It is a global network of networks, traverses the Internet, and has many individual private network segments. [Doria 10]

The term Internet in Internet of Things requires interpretation. It does not refer to a network that includes infrastructure as the Internet does. It refers instead to a network overlay[51] on other networks. While the IoT may use the existing Internet as an access substructure, it is not restricted to using only the Internet substructure. It may be also be implemented on new yet-to-be developed network infrastructures.

Research on the IoT is global with part of the network already in existence, though currently largely layered over the Internet as we currently know it. While the IoT is beginning as something that is overlaid on the Internet infrastructure and is using Internet names and addresses, there is no reason to believe that it will remain a strict overlay.

The IoT is based on the associations between objects in the world and not on the association of computer nodes or users. Yet at the same time, it is still subject to one of the operational principles of the Internet, its addressing and naming. Currently the IoT is using the Internet addressing scheme and naming system, which is governed by ICANN. Some experts on the subject of IoT governance have gone so far as to state: "Governance of the IoT will not/should not replicate the ICANN model or the ICANN debate" [Cute 09].

As with other new emergent networks, a different naming/addressing architecture may be developed and deployed in time. There would be good reason for this to happen, given the IoT's existence beyond the bounds of the Internet, as it is currently defined. This new naming and addressing architecture would bring with

[51] An overlay network is one that uses another network, but has its own architecture and often includes elements such as a unifying data abstraction, protocols and interfaces. Often an overlay network is capable of being run over a variety of other network infrastructures. Among the well known overlay networks is the IP network, which is an overlay network over a variety of hardware transport networks, such as the Public Telephony network or a specialize Fiber Optic network, each of which has its own architecture.

it a new set of governance policy issues. Yet, when looking at the IoT, there is not yet sufficient evidence to know in what ways the governance would/should differ. One industry group, EPC Global [EPC] which has a focus on the RFID (Radio Frequency Identification) technology that is a major strand of the current concept of IoT, has already shown an interest in having a role in the governance of IoT; in fact they claim that the IoT is not an overlay of the Internet, but rather that the Internet is an overlay of the Internet of Things[52].

The European Commission has been concerned about the form IoT governance will take for several years. They have started to look into the needs for IoT governance, specifically [EC-IOT]:

> According to the European Commission, policymakers should also participate in the development of IoT alongside the private sector. Some challenges are indeed policy-related, as highlighted by the World Summit on the Information Society, which encourages IoT governance designed and exercised in a coherent manner with all the public policy activities related to Internet Governance.
>
> Many questions concerning the implementation of the connection of objects arise such as:
>
> - object naming;
> - the authority responsible for assigning the identifier;
> - ways to find information about the object;
> - how information security is ensured;
> - the ethical and legal framework of IoT;
> - control mechanisms.

The European Commission also released an action plan for Europe on the Internet of Things [EC-IOT 09] indicating the need for "promoting a shared and decentralized network governance" and committing to follow WSIS principles in the governance of the IoT.

Privacy and the IoT

While the IoT, refers to things, these things can be associated with a time and place. When a thing is obtained by a person, usually though purchase, that information can be linked to the person and their activities. There are various proposals for

[52] This claim was made during an IGF workshop on the Internet of Things on 29 September 2011. The workshop transcript will eventually be made available on the IGF website: http://www.intgovforum.org/cms/

linking each object in the IoT with a permanent globally unique identifier. While technically useful and within the bounds of the technical principles of the Internet, this is seen as a risk to people's privacy. The research community has been discussing the privacy and security issues related to having the object carried by individual identified and tracked. Most of the proposals rely on the creation of governance policy for protecting the privacy of individuals, however, there are many who worry that if something can be tracked, it will eventually be tracked for security or other reasons. There is pressure on the community to find ways to satisfy the technical and commercial requirements for tracking objects through their entire life cycle without creating yet another privacy and security threat.

The Internet of Things is one of the future developments that currently lies at the cusp of technology and policy and is a good subject for longitudinal study within the Institute.

Filtering, Inspection and Circumvention

Filtering and packet inspection, the ability to read inside a packet at line speed, is not a new development, though the hardware being produced by systems vendors does improve with every year to satisfy customers in nations that require filtering for their notions of a harmonious state. The struggle against packet inspection and filtering in support for freedom of expression, freedom of information and freedom of association is not new either.

The developments worth watching for their effect during the next decade are the efforts to circumvent the measures instituted by those who wish to control the Internet and to control the populations in their countries by controlling the Internet. After the Iranian blocking and then misuse of Twitter and Facebook, as well as the Egyptian government's shutdown of the Internet, a research was funded in the US to create public domain software systems that could be used to circumvent a localized shutdown of the Internet. The project, encouraged in part by the US State Department [Clinton 11],

> We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship. We are providing funds to groups around the world to make sure that those tools get to the people who need them in local languages, and with the training they need to access the internet safely.
> ...
> We want to put these tools in the hands of people who will use them to advance democracy and human rights, to fight climate change and epidemics, to build global support for President Obama's goal of a world without nuclear weapons, to encourage sustainable economic development that lifts the people at the bottom up.
>
> That's why today I'm announcing that over the next year, we will work with partners in industry, academia, and nongovernmental organizations to establish a standing effort that will harness the power of connection technologies and apply them to our diplomatic goals. By relying on mobile phones, mapping applications, and other new tools, we can empower citizens and leverage our traditional diplomacy. We can address deficiencies in the current market for innovation.

One project, the Commotion Wireless Project [Commotion] has the following mission:

> democratic activists around the globe need a secure and reliable platform to ensure their communications cannot be controlled or cut off by authoritarian regimes. To date, technologies meant to circumvent blocked communications have focused predominantly on developing services that run over preexisting communication infrastructures. Although these applications are important, they still require the use of a wireline or wireless network that is prone to monitoring or can be completely shut down by central authorities. Moreover, many of these technologies do not interface well with each other, limiting the ability of activists and the general public to adopt sophisticated circumvention technologies.

The Commotion Wireless project focus is to take existing software systems and combine them into what they have been calling Internet in a Suitcase. They do not plan on the creation of new software or hardware except in so far as it is needed to bring the divergent elements of the system together. Their plans are described as follows [Commotion]:

> For over a decade, developers here have pioneered the development of "device-as-infrastructure" broadband networks. By utilizing cell phones and best-of-breed open source projects from around the globe, OTI's[53] implementation strategy integrates already existing hardware (and extensions to currently available open source initiatives) to dramatically increase the security and robustness of telecommunications. Specifically, this project proposes the following five-point solution:
>
> - Create a robust and reliable participatory communications medium that is not reliant

[53] Open Technology Initiative: http://saschameinrath.com/2011/jun/22/new_york_times_covers_oti_work_u_s_underwrites_internet_detour_around_censors

upon centralized infrastructure for local-to-local (peer-to-peer) and local-to-Internet communications;

- Design ad hoc device-as-infrastructure technologies that can survive major outages (e.g. electricity, Internet connectivity) and are resilient during emergencies, natural disasters, or other hostile environments where conventional telecommunications networks are easily crippled;
- Secure participants' communication to protect data integrity and anonymity through strong end-to-end encryption and data aggregation;
- Implement communications technologies that integrate low-cost, pre-existing, off-the-shelf devices (e.g. cell phones, laptops, consumer WiFi routers) and maximize use of open source software; and,
- Develop an open, modular, and highly extensible communications platform that is easily upgraded and adapted to the particular needs and goals of different local users.

At this point in time, given the semi-mythic description of the Internet as a system that could withstand nuclear attack, the image of a group of developers, mostly students, developing an open system that can withstand authoritarian interference is a development worthy of observation, analysis, and support. It is interesting to note that the Iranian government has announced that they are ready for the Internet in a Suitcase and will be able to stop the circumvention[54]. [Memarian 11]

Another project worth watching for its effect on policy developments is the ToR project[55], which aims to allow users to achieve online anonymity and to protect the freedom of association on the Internet.

> Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

The Tor project, originally a US navy project, provides software for most operating systems, including Microsoft Windows, Apple OSX and IOS, and Linux, that allows people to surf the Internet in anonymity and without surveillance by either the state or anyone else. It blocks not only the identity of the users, but also blocks statistical analysis that can be used in decisions of which site to block. One of the major

[54] http://english.peopledaily.com.cn/90001/90777/90854/7425779.html

[55] https://www.torproject.org/

features of Tor is it ability to block traffic analysis. Even in cases where users encrypt their data, the packet headers are in cleartext[56]. The fact that the packet information is sent in cleartext allows surveillance systems to monitor a traffic stream and analyze it. While the surveillance system may not what is contained in a message, it can determine the association between the user and those the user communicates with. In many situations this information is as dangerous to the well being of an individual or a business proposition as the data itself. Use of the Tor network allows a user, through the use of multiple proxies, to mask the information needed in traffic analysis.

A wide cross-section of people and institutions use ToR on the web both for website publication and surfing. According to the ToR website, it has not only been used by individuals who want to avoid surveillance, but has also been used by the US government when it want to keep its monitoring activities secret.

In terms of policy, while democratic countries support the creation of circumvention methods when they are directed at authoritarian regimes, it is uncertain how they will react when used to allow for the free dissemination of leaked documents such as was the case in Wikileaks. The area of filtering, blocking and circumvention is certain to be involved in many of the governance policy areas over the next decide.

Social Media, Multimedia and Communities

Social networking and virtual communities are not a new development

> I expect these tools to develop into a common new genre on the Web. Real Life is and must be full of all kinds of social constraint - the very processes from which "society" arises. Computers help if we use them to create abstract *social machines* on the Web: processes in which the people do the creative work and the machine do the administration.
>
> ...
>
> People are already experimenting with new social machines for online peer review,

[56] For discussion purposes, a data packet can be divided into 2 parts, the data, and the meta-information, including packet headers, that encapsulates the data and defines what the network should do with the data. While the data can be encrypted, the meta-information cannot be encrypted. Data that is sent over the Internet without encryption is referred to as cleartext.

> while other tools such as chat rooms developed quite independently and before the Web. MUDDs[57] are social tools derived from multiuser games of Dungeon and Dragons where thousands of people take on roles and interact in a global online fantasy world. By experimenting with these structures we may find a way to organize new social models that not only scale well but can be combined to form larger structures.[Berners-Lee 00]

The explosion of social media and virtual communities that is seen today and that can be expected in the future has gone beyond what could have been envisioned a decade ago. Social media is at once seen as a tool of liberation, economic revitalization, a solution to social problems and a threat. In terms of political effects one only needs to point to Iran and Wikileaks, to see the importance of social media and the worldwide communities that are created. When looking at the phenomena called the Arab Spring, "a study on network theory finds that the tipping point needed for a committed minority to win over the majority is just 10 percent" in the age of social media [Atlantic 11]. Wiki sites have been created where governments solicit comments and collaboration on agency directions and regulatory plans. At the same time, social media has presented dangers such as polarizing discussions where users only get feedback from those who agree with them, and the amplification of societies' ills, such as loss of privacy and personal security and identity theft. [Shneiderman 11].

Currently there is an explosive near-ubiquity of personal network devices, e.g. the varieties of smart phone, tablets and other networked devices. They are becoming phenomenologically linked to human life and well being and to public policy. In the past, social media was something that someone engaged in when they were at their desks or at home in the evening. Now it is becoming an integral part of human life, part of the commons. An interesting aspect of this is that because the smart devices are spreading beyond the developed world to the developing world, this is the first technically inspired social change that is happening as much, if not more, in the developing world than it is in the developed world.

[57] MUDDs: Multi User Dungeons and Dragons

To date, policy in this area has come from the providers of the social media tools. Internet policy governance organizations, e.g. the IGF, may have had some discussions about social media as an emerging issue, but have not really caught up with the issue. Currently, the social media providers, such as Facebook, Linkedin and Google Plus, define the policies that users are subjected to. What is not clear is whether this is accepted by society as a norm or whether there is an expectation that governments or the Internet governance policy organizations should have some degree of influence over the policies of these services. While some users argue willing to accept that the agreement between the user and the media provider is sufficient with the user having the ultimate choice of whether to use the service or not, other argue that the service social media provides have become integral to full social existence that there is no real choice about participating in social media.

Given the power of new technology to provide multimedia, social media is evolving into a new area being called Social Multimedia [Tian 10]. As with most of the social media fields, this is seen as a multidisciplinary field juxtaposed between Computer Science and the Social Sciences that involves disciplines such as signal processing, information retrieval, social psychology, cognitive psychology computing theory and others. The interactions in social multimedia are described as having several dimensions [Tian 10]:

- Creates an environment that promotes community sharing of ideas and content
- Content involves a variety of media types that are linked contextually and not necessarily collected in the same time and place, or by the same people.
- The relationship between the participants in the social media go beyond the text that is shared in social media to include video and tagged images.
- Real world social interaction is often captured in social multimedia.

It can be expected that the discussions concerning policies related to social media and social multi-media will be complicated by the issues inherent in the distribution of multimedia, especially when the images depicted in the media include people engaged in activities they would prefer kept private.

IT ecosystems for healthcare

In both the developed world, because of cost, and the developing world, because of availability, information technology is being applied to help contain cost and provide timely medial interventions. In the last 2 years alone, there have been over 2000 distinct articles, as listed in the ACM Digital Library, on topics in healthcare, the Internet and communications networks (this out of over 30,000 articles on Healthcare and computing).

Web 2.0 technology and multi-media, social networking among physicians, other medical specialists and their patients are playing a part in this trend. [Computer 10] Other technology needed for medical informatics, especially with regard to patient care is either undergoing research or is still in development. Improvements in system reliability and in the storage and access of patient data are brought on line all the time. Finally there is research in finding reliable ways for the various medical information systems to be linked so that information about a patient is accessible to all those who have an appropriate reason to access that information in order for a patient to be well served by medical informatics. [Cantrill 10]

Policy issues that arise in e-health include protecting the privacy of patients while sharing the information as needed to reach appropriate medical professionals, authentication so that physicians can trust their information sources and so that patients can be sure they are getting advise from a qualified professional, and the storage and eventual use of patient information. There is a direct conflict between the need to link all of a patient's information in order to provide the best care possible and the need to protect the privacy of a patient that needs to be overcome in both the technical and policy spheres before this field will be able to make appreciable progress. but the work to solve these issues continues and is well funded.

Delayed innovations

This section looks at some of the innovations predicted from previous decades that have not yet lived up to their promise. Some of these innovations may begin to appear and have policy effects over the next decade.

Artificial Intelligence in the network

For over 40 years artificial intelligence (AI) has been 'just around the corner'. And since the early days of the Internet there have been people expecting that AI would have an effect on the Internet. Predicting that AI will have an effect on the Internet in the next decade is, therefore, not a very safe prediction. Knowledge systems on the other hand are beginning to appear in almost all areas of Internet operations. There were over 40,000 articles in the last year listed in ACM Digital Library dealing with knowledge systems in Internet architectures and protocols. Since knowledge systems are a very advanced sub-field of computer science, many of these articles are quite theoretical. What does seem to be happening is that these theories are being put into effect by companies developing Internet applications for business.

One of the areas that has been enabled by knowledge systems is data mining[58]. By applying high level abstractions, grid services[59] can be used "as an effective cyber infrastructure for implementing and deploying geographically-distributed data mining and knowledge discovery services and applications." [Talia 10]

> Software frameworks and technologies for the implementation and deployment of knowledge services, (...), provide key elements to build up data analysis applications on enterprise or large-scale Grids and Clouds. Those models, techniques, and tools can be instrumented in Grids and Clouds as decentralized and interoperable services that enable the development of complex systems such as distributed knowledge discovery suites and knowledge management systems offering pervasive access, adaptivity, and high performance to single users, professional teams, and virtual organizations in science, engineering and industry that need to create and use knowledge-based applications.

That is, using these system elements allows anyone to data mine any and all

[58] Data mining is a subarea of computer science that involves using artificial intelligence, statistics and database management techniques to discover patterns in data. Data mining is a fundamental method used in any intelligence activity.

[59] Grid services related to service provided by grid computing resources, which are highly distributed in terms of type and geography, heterogeneous, and loosely couples systems.

information that currently available on the Internet.

One example of a company applying data mining and knowledge systems techniques is Cataphora, which produces behavioral modeling and monitoring systems .The purpose of the system is to "replace armies of expensive lawyers with cheaper software". [Markoff 11] The Catephora systems are capable of discovering all of the writings of a person on the Internet and then analyzing them to give an employer a complete picture of someone's viewpoints on any subject they have ever written about. This is done in a way that is provable and thus actionable in a court of law. It is arguable whether such analysis is legitimate within the workplace, it most likely varies according to the laws of the country where the workplace is situated. This set of tools however, is not limited to the workplace. These tools can be used on any individual in any circumstance. This sort of offering brings the tools of intelligence organizations, e.g. the CIA, to the corporate and eventually to the user level.

The privacy issues created by the proliferation of such tools in the age of social networks is an issue that will affect the discussions regarding ongoing Internet governance policy and the control by a user of their data.

Automatic reprogramming of the networks

For years, network management professionals have considered using automatic programming to manage the network. Within some enterprises, management systems are already in use doing this, but few systems have begun to do so across the network. That is with the exception of viral technologies, that have been reconfiguring nodes within the network for their specific, normally illegal, requirements for years. Several researchers have also looked into the use of viral technologies for beneficial purposes. One application is the use of viral technologies to combat malicious viral technologies. Another such application is the use of a pruned epidemic tree for routing in a DTN. If computer viruses had not gotten such a dangerous reputation in the network, it is possible that there may have been greater non-malicious use of viruses by this time to do network maintenance as the technology is well developed - though it may only be well developed because of its usefulness in crime. It is possible to believe that network maintenance will indeed happen in the not too distant future. One use that has been spoken of is the use of viruses in the service of a right of anonymity. It is well understood that once information about a person has been put on the Internet, it cannot be removed because the spread of data is very pervasive. While a viral program to remove references to a person from the network would not be 100% effective, because of off line storage and encrypted storage, and would need to be carefully controlled and monitored, such uses are possible. The next decade is likely to bring many unexpected uses of viral technology and other automatic reprogramming technique into use. Each of new use of Internet reprogramming techniques is likely to initiate some degree of governance policy discussion.

New TLDs

Given all of the Internet governance policy activity that there is surrounding new gTLDs, a reader of this report might question why new gTLDs aren't listed as one of the new technologies that will drive future Internet governance policy. The reason is that New gTLDs involve very little new technology. While they are predicted to be a business revolution,[60] they do not, at this point, represent a technical revolution, though there is work to be done to adjust some Internet software due to the policy decisions to add many new gTLDs. During a 2010 US National Science Foundation workshop on future networking, David Clark said the following: "While governance will be an issue in 15 years, the current and short term future of ICANN is not relevant, I don't think anyone said 'ICANN' the whole time. Those are today's arguments, not tomorrow's" [Kroeker 10] while there will be policy discussions related to new gTLDs, these are not defined as being due to

[60] The author must admit that she really doesn't have a clear understanding of what a business revolution might be. Perhaps it is a way to make money without exploiting anyone.

technological or architectural change.

One area, however, that is somewhat new is the area of internationalized top level domain names (IDN TLDs). While implementing domains names in written forms other than the basic English/Latin (IDNs) the Internet is accustomed to as top level domain names is new, there have been IDNs in the Internet for years at the second level. In the last year, improvements were made to the IDN protocols so that they would be more useable[61] than in the past. One issue that is introduced by IDN TLDs has to do with Whois, the service discussed earlier in this report by which the registrants of TLDs are made public and tracked. Currently the Whois service is only capable of using basic English/Latin characters and numbers[62]. In communities that use written methods other than Latin script, requiring an English/Latin based Whois is not only confusing and misleading, it is quite possibly impossible. There is an effort ongoing in ICANN to try and untangle the technical and policy issues involved in developing a new Whois system that is adequate to serve the IDN TLDs. This is a very focused area that touches on many of the topics outlined in this report and may be a good subject for further academic research.

Conclusions

As mentioned earlier in this report, one thing that can be predicted with certainty is that the dynamic tension between technology's tendency to enable the various human rights and freedoms, by opening up an ever increasing set of opportunities for expression and sharing, and governance policy's drive to protect and limit danger, will continue. The logic of this dynamic will give rise to a number of adjustments to both technology and policy and "one cannot speak of a balance of forces in an actual or static sense but only of a system of compensations related to the operations themselves" [Piaget 95]

[61] There are those who think this effort was too conservative, e.g. <http://iucg.org/wiki/IDNS_Common_Glossary> This report makes not comment on this, other than to point to it as an ongoing tussle over the proper way to handle IDNs

[62] The are known technically as ASCII LDH - for the American Standard Code for Information Exchange - Letters, Digits and Hyphen

Some of the leaders in Internet governance have in the last years (re)discovered the work of Elinor Ostrom on "governance and management of common-pool resources." Ostrom defines "common-pool resource" to refer "to a natural or man-made resource system that is sufficiently large as to make it costly (but not impossible) to exclude potential beneficiaries from obtaining benefits fro its use." [Ostrom 90] While her name has been frequently invoked in the last year, her work has not yet been integrated into discussions of Internet governance. The application of Commons Theory to the issues of of Internet governance policy could provide another research area for the Institute.

One of the fundamental changes to policy making over the next period will be its multi-stakeholder model. While this can be seen as somehow separate from the Internet technology, especially from new developments in technology, it is a reflection of the Internet's emerging power to influence society and norms. It is only in the past few year's that organizations outside of those involved with the governance on Internet resources, have begun accepting the necessity of including other stakeholders in making policy, something that used to be considered the role and responsibility of just one stakeholder. This is a trend that will not abate, though of course we can expect that its progress will be in fits and starts with occasional setbacks. This will affect not only the policy that governs the Internet, but will also affect the technology that is created.

References

[Anthes 10] Security in the Cloud, Gary Anthes, Communications of the ACM, Novemeber 2010, page 16

[Atlantic 11] From Sushi to Tunisia: A Guide to Swaying Majority Opinion http://www.theatlantic.com/life/archive/2011/09/from-sushi-to-tunisia-a-guide-to-swaying-majority-opinion/244589/

[Berners-Lee 00] Tim Berners-Lee (2000). Weaving the Web, page 172

[Bled 08] The Bled Declaration: Toward an European approach to the Future Internet", http://www.future-internet.eu/publications/bled-declaration.html, March 2008

[Cantrill 10] Computers in Patient Care: The Promise and the Challenge, Stephen V. Cantrill, M.D., Communications of the ACM, September 2010, page 42

[Clark 02] Tussle in Cyberspace: Defining Tomorrow's Internet, David D. Clark, John Wroclawski, Karen R. Sollins, Robert Braden, 2002, SIGCOMM'02

[Clinton 11] Remarks on Internet Freedom, http://www.state.gov/secretary/rm/2010/01/135519.htm

[COE 11] Internet Freedom, from principles to global treaty law, Draft 2.0, http://www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/Internet%20Governance%20Principles.pdf, April 2011

[Commotion] http://tech.chambana.net/projects/commotion

[Computer 10] Computer issue on e-Health, July 2010

[Crowcroft 10] FIE, Future Internet Enervation, Jon Crowcroft, ACM SIGCOMM Computer communications Review, July 2010, page 48

[CSISAC 11] Statement on OECD Communiqué on Principles for Internet Policy-Making http://csisac.org/CSISAC_PR_06292011.pdf

[Cute 09] http://twitter.com/bcute17/status/2189966433

[Doria 10] "Governance of the Internet of Things ," A. Doria, M. Fiedler, R. Herkenhöner, W. Kleinwächter, G.F. Marias, and G.C. Polyzos, (submitted to Communications Law, Bloomsbury Professional)

[Dot-p2p] http://dot-p2p.org/ also at http://www.myce.com/news/dot-p2p-promises-a-free-decentralized-open-dns-system-37216/

[Dovrolis 10] Evolvable network architecture: Waht can we learn from biologu, Constantine Dovrolis, J. Todd Streelman, ACM SIGCOMM Computer Communications Review, April 2010

[Drake 05] William Drake (ed, 2005), Reforming Internet Governance

[EC IOT] Internet of Things, http://europa.eu/legislation_summaries/research_innovation/research_in_support_of_other_policies/si0009_en.htm

[EC-IOT 09] Communication From The Commission To The European Parliament, The

Council, The European Economic And Social Committee And The Committee Of The Regions, http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

[EPC] http://www.epcglobalinc.org/home/

[G8 11] G8 Declaration- Renewed Commitment For Freedom And Democracy, G8 Summit of Deauville - May 26-27, 2011, http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html

[GAC 07-1] GAC Principles regarding new gTLDs', March 28, 2007, https://gacweb.icann.org/download/attachments/1540128/gTLD_principles_0.pdf?version=1&modificationDate=1312358178000

[GAC] GAC maintains a website where all of its advice to the ICANN Board can be found: https://gacweb.icann.org/

[GDP 03] Geneva Declaration of Principles

[Gould 02] Stephen Jay Gould (2002). The Structure of Evolutionary Theory

[Haraway 97] Donna Haraway (1997), Modest_Witness@Second_Millenium.FemalMan@_Meets_OncoMouse(TM)

[ICANN 11] Bylaws For Internet Corporation For Assigned Names And Numbers, 24 June 2011 http://www.icann.org/en/general/bylaws.htm

[ICECSR] International Covenant on Economic, Social and Cultural Rights, http://www2.ohchr.org/english/law/cescr.htm

[ICCPR] International Covenant on Civil and Political Rights, http://www2.ohchr.org/english/law/ccpr.htm

[ICN 11] Information-Centric Networking -Dagstuhl Seminar, http://drops.dagstuhl.de/opus/volltexte/2011/2943/pdf/dagstuhl_icn_proceedings.2943.pdf

[ID-URI] The DTN URI Scheme, http://tools.ietf.org/html/draft-irtf-dtnrg-dtn-uri-scheme-00

[Kroeker 10] Future Internet Design Summit, Kirk L. Kroeker, Communications of the ACM, January 2010, page 29

[Kroes 11] Blog, http://blogs.ec.europa.eu/neelie-kroes/i-propose-a-compact-for-the-internet/

[LaRue 11] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[Leavitt 11] IPv6: Any Closer to Adoption, Neal Leavitt, Computer, September 2011, page 14

[McCarthy 11] European Commission calls for greater government control over Internet, http://news.dot-nxt.com/2011/08/31/ec-greater-government-control

[Memarian 11] Take That, Tehran, Omid Memarian, Slate, July 12. 2011 http://www.slate.com/id/2299037/

[Merleau-Ponty 64] Maurice Merleau-Ponty (1960, 1964). Signs

[Narasimham 11] State of Cloud Applications and platforms: The Cloud Adopter's view, Balakrishma Narasimhan, Ryan Nichols, Computer, March 2011, page 24

[Markoff 11] Armies of Expensive Lawyers Replaced by Cheaper Software, John Markoff, New York Times, http://www.nytimes.com/2011/03/05/science/05legal.html?_r=2&pagewanted=1&ref=science

[OECD 11] Communiqué on Principles for Internet Policy-Making, http://www.oecd.org/dataoecd/40/21/48289796.pdf

[ONS V1.0.1] Open Naming Service Standard, http://www.gs1.org/gsmp/kc/epcglobal/ons, http://www.gs1.org/

[Ostrom 90] Governing the Commons: The Evolution of Institution for Collective Action, Elinor Ostrom, 1990

[Paget 95] Piaget, J. (1995). Six Sociological Studies

[Post 09] David G. Post In Search of Jefferson's Moose: Notes on the State of Cyberspace, 2009 Note: I have not actually quoted from this book. But I read it while researching this paper, and the feeling I had was that half of what I thought had already been said by Mr. Post.

[Rexford 10] Future Internet Architecture: Clean-Slate Versus Evolutionary Research, Jennifer Rexford, Constantine Dovrolis, Communications of the ACM, September 2010, page 36

[Ricoeur 92] Oneself as Another, trans. Kathleen Blamey, Chicago: University of Chicago Press, 1992

[Rodrigues 10] Peer-to-Peer Systems, Rodrigo Rodrigues, Peter Drushel, Commuications of the ACM, October 10, page 72

[RFC791] Internet Protocol, http://tools.ietf.org/html/rfc791, Jon Postel (ed), September 1981

[RFC793] Transmission Control Protocol (the TCP of TCP/IP), Jon Postel, September 1981

[RFC1034] Domain Names: Concepts and Facilities; Paul Mochapetris, http://tools.ietf.org/html/rfc1035

[RFC1035] Domain Names: Implementation and Specification; Paul Mochapetris, http://tools.ietf.org/html/rfc1035

[RFC1591] Domain names system structure and delegation, Jon Postel, http://tools.ietf.org/html/rfc1591, March 1994

[RFC1918] Address Allocation for Private Networks, Yakov Rekhter, Robert G Moskowitz, Daniel Karrenberg, Geert Jan de Groot, Eliot Lear, http://tools.ietf.org/html/rfc1918, February 1996

[RFC1930] Guidelines for creation, selection, and registration of an Autonomous System (AS), John Hawkinson, Tony Bates, http://tools.ietf.org/html/rfc1930, March 1996

[RFC1958] Architectural Principles of the Internet, Brian Carpenter, http://www.rfc-editor.org/rfc/rfc1958.txt, 1996

[RFC2396] Uniform Resource Identifiers (URI): Generic Syntax, Tim Berners-Lee, Roy T. Fielding, Larry Masinter, http://www.ietf.org/rfc/rfc2396.txt

[RFC2460] Internet Protocol, Version 6, Stephen E. Deering, Robert M. Hinden, http://tools.ietf.org/html/rfc2460, December 1998

[RFC2775] Internet Transparency, Brian Carpenter, http://tools.ietf.org/html/rfc2775, February 2000.

[RFC2993] Architectural Implications of NAT, Tony Hain, http://www.rfc-editor.org/rfc/rfc2993.txt, November 2000

[RFC3439] Some Internet Architectural Guidelines and Philosophy, Randy Bush, David Meyers, http://www.rfc-editor.org/rfc/rfc3439.txt, December 2002

[RFC3490] Internationalizing Domain Names in Applications (IDNA), Patrick Fältström, Paul Hoffman, Adam M. Costello, http://www.ietf.org/rfc/rfc3490.txt, March 2003

[RFC3593] Internet Protocol Version 6 (IPv6) Addressing Architecture, Robert Hinden, Steve Deering, http://tools.ietf.org/html/rfc3513, April 2003

[RFC3986] Uniform Resource Identifier (URI): Generic Syntax, http://tools.ietf.org/html/rfc3986

[RFC4632] Classless Inter-domain Routing (CIDR):The Internet Address Assignment and Aggregation Plan, Vince Fuller, Tony Li, http://tools.ietf.org/html/rfc4632, August 2006

[RFC4838] Delay-Tolerant Networking Architecture, Vint Cerf, Scott C. Burleigh, Robert C. Durst, Kevin Fall, Adrian J. Hooke, Keith L. Scott, Leigh Torgerson, Howard S. Weiss, http://tools.ietf.org/html/rfc4838, April 2007

[RFC5890] Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework, John Klensin, http://tools.ietf.org/html/rfc5890, August 2010

[RFC5891] Internationalized Domain Names for Applications (IDNA): Protocol, John Klensin, http://tools.ietf.org/html/rfc5891, August 2010

[Ryan 11] Cloud Computing Privacy Concerns on Our doorstep, Mark D. Ryan, Communications of the ACM, January 2011, page 36

[Saltzer 84] END-TO-END Arguments In System Design J.H. Saltzer, D.P. Reed and D.D. Clark* M.I.T. Laboratory for Computer Science http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.txt.

[Shneiderman 11] Realizing the Value of Social Media Requires Innovative Computing Research, Ben Schneiderman, Jennifer Preece, Peter Pirolli, Communications of the ACM, September 2011, page 34

[Simon 96] The Sciences of the Artifcial, Herber A. Simon, The MIT Press, 1996; as quoted in [Dovrolis 10]

[Srinivasan 11] Navigating the Cloud Computing Landscape - Technologies, Services and

Adopters, Savitha Srinivasan, Vladimir Getov, Computer, March 2011, page 22

[Talia 10] How distributed data mining tasks can thrive as knowledge service, Domenico Talia, Paolo Trunfio, Communications of the ACM, July 2010 page 132

[Tian 10] Social Multimedia Computing, Yonghand tian, Jaideep Srivastava, Tiejun Huang, Noshir Contractor, Computer, August 2010, page 27

[ToR] The ToR project https://www.torproject.org/about/overview.html.en

[UDHR] Universal Declaration of Human Rights, http://www.un.org/en/documents/udhr/

[WSIS] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316|0

[Zittrain 08] The Future of the Internet and How to Stop it, Jonathan Zittrain, Yale University Press 20089