Key Issues in Internet Governance

George Raburu, Lawrence Dinga

***Abstract*— Internet is network of remotely or physically connected computers or computer devices that are able to interact. Numerous activities take place on the internet. The processes of decision making on what activities are to be implemented or not implemented on the internet depending on their impact on the immediate environment constitutes the internet governance. Hence Internet governance refers to processes that are designed to ensure accountability, transparency, responsiveness, legality, morality, stability, equity and inclusiveness, empowerment, and broad-based participation in the use of internet. Internet spurs digital transformation in unlocking the potential digital government into data-driven smart government capable of driving policies and services of public interest and public value (https://doi.org/10.1016/j.giq.2018.09.007). This paper analyses the key technical and public policy issues (rules, procedures and user expectations) that are considered relevant to users of internet. The paper is aimed at providing guide to organizations, researchers and individuals on the key issues that needs to be considered when striving for good internet governance.**

***Index Terms*— Internet Service Provider, Internet Protocol, Cyberspace, Internet Governance, Distributed Systems, Domain Names, World wide web(www), Internet Protocol, Cybercrime.**

I. INTRODUCTION

Internet Governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet (WGIG, 2005).

The prototype Internet was first rolled out by Advanced Research Projects Agency Network (APARNET) in the late 1960s sponsored by the U.S. Department of Defense. This was a distributed network aimed at facilitating communications between research centers. Even though ARPANET remained in the custody of the U.S. Government, its use soon spread to a larger community of users especially in the academia. The network eventually metamorphosed into the Internet and was launched to the public in 1983. In 1984, a board comprising various task forces was constituted to oversee the Internet activities. In 1986, the board gave birth to the Internet Engineering Task Force (IETF) in 1986, whose responsibility was to develop technical standards for the Internet. IETF became an open, cooperative and consultative body whose decisions were reached through consensus and embraced a wide range of stakeholders including individuals and institutions. As the Internet use became more and more and the world economy became reliant on its operation, many governments began to recognize the strategic importance of this new infrastructure and how it could contribute to the well-being of their citizens that led to the formation of Internet Corporation for Assigned Names and Numbers (ICANN) in 1998. The role of ICANN was to Manage Internet Protocol numbers and Domain Name System. Most developing countries did not support the formation of ICANN preference to the management by international organizations. This was the backdrop for the 2003 World Summit on Information Society held in Geneva in which Internet governance became the key issue addressed at the summit. It culminated in the establishment of the Working Group on Internet Governance (WGIG) whose mandate was to tackle the problem of Internet governance on a global level.

II. LAYERED ARCHITECTURE OF THE INTERNET

No discussion about Internet Governance issues can be progressed without discussing the layers principle as this is the foundation of the Internet's strength and that communications networks are categorized into three distinct layers (Yochai Benkler, 1998). "The *Physical infrastructure layer"* representing a pipe that carries information, *Logical layer"* that controls the infrastructure, and a "*content layer"*, that represents the content that flows through the pipes. Layer's principle is also drawn from the architectural engineering and design of the Internet in which TCP/IP protocol suit is structured into seven stacks. The Internet Governance related issues take place on each of the three layers. The physical infrastructure layer is considered the foundation layer of the Internet. The logical as well as content layers are built upon this physical infrastructure layer

Physical Infrastructure Layer

This is the foundation block of the Internet and consists of the copper wire, optical cables, satellite links and radio waves that transmit data from one point to another and are physically connected to our homes and offices. It provides the platform on which logical and content layers are built upon and therefore governance at this layer is critical to maintaining the seamlessness and viability of the entire network. Issues requiring governance at this layer include interconnection, universal access and deployment of next generation technologies to ensure that they work in harmony with the pre-existing legacy systems.

(i) Interconnection

The Internet is an amalgamation of various networks that interconnect to form one global network. In technical terms the Internet is a *"global, distributed system of hundreds of thousands of independently operated and interconnected computer communication networks"* using TCP/IP protocol suite. The interconnection between these networks is

George Raburu, School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya
Lawrence Dinga, Management Systems Limited, Nairobi, Kenya

however not being controlled by any institution nor are there clear governing laws or regulations. The ambiguity has led to high access cost particularly for remote countries in the developing world. The WGIG identified uneven distributed access cost as a significant issue that requires governance.

There are usually three levels of interconnection access. The first level, Tier 1 consists of large international backbone operators that provide access to high-speed data transmission lines and other related infrastructure to other operators that need it. Tier 1 can be considered as a superset of Internet Service Providers and include large telecommunications companies like AT&T, Sprint and Verizon. Tier 2 consists of national or regional operators while Tier 3 consists mainly of local Internet Service Providers. While there may be some regulation at national or local level (Tiers 2 and Tier 3 ISPs) regarding interconnection rates. Such regulations are not available at international level (Tier 1) and interconnection costs is always on the basis of negotiation and bargaining or is left for the market to determine efficient manner of interconnection. This presents a challenge to developing countries that normally lack ownership of Tier 1 infrastructure and find themselves disadvantaged to negotiate favourable access rates. It is also argued that the shortage of good content stored on local servers in developing countries is contributed to by the high international interconnection costs forcing users to access information from sites stored out of the country.

Lack of interconnection governance at Tier 1 has created some discontent and instigated initial move towards governance solution. International Telecommunication Union (ITU), proposed three solutions for governance mechanism which have not been wholly accepted by all stakeholders with big industry players that prefer market driven solution. On the contrary, the smaller industry players and developing world advocating for a system similar to the one used in international telecommunications (where the amount of traffic carried by operators) is measured in terms of call-minutes and reconciled using previously agreed-upon rate.

(ii)Universal Access and Service(UAS)

Within the internet, UAS traditionally focuses on basic voice communications. The principle goal of this concept was to promote the availability of quality telephone services to individual homes at affordable and reasonable rates. It was targeted to make telephone services ubiquitous to both rural and urban areas. While UAS policies target individuals and households to have access to telephone service either through wired or wireless devices, universal access policies focus on availing telephone services at publicly shared place or community. With the maturation of mobile telephony and lower rates, many countries are now capable of realizing their target of universal service and achieve more telephone penetration in both urban and rural areas. In the United States, the Telecommunications Act 1996 expanded the concept of universal service to include high speed internet while the EU in 2010 included functional internet in EU legislation on universal service. Both have recognized high speed internet as a basic human right and an enabler of the 21st century communications technology and have implemented policies geared towards making broadband as ubiquitous as voice. With these advancements in technologies, there is justification to use the generic term, *universal access and service* to denote the convergence of voice telephony, broadband and broadcasting technologies.

Universal access and service policies usually targets rural or a poor urban areas where private telephone services are not viable. Available Public payphone is always within a walking distance within the community and caters for a diminished population size. The Internet services should be made available and affordable regardless of location, gender or personal disabilities. Internet users should also ensure that universal access and service policy is forward looking and contains broadband growth, transition to a next-generation network atmosphere and address cases of convergence.

Many countries can reap a lot of benefits and dividends if they expand universal access policies beyond their traditional voice communication services to include ICT broadband, internet and broadcasting technologies. Initiating programs that include a mix of personal computers, mobile phones and other digital devices, broadband internet connections and local content can give citizens in remote rural and urban areas access to better education, healthcare, social support, agricultural extension services and many other economic opportunities. In most sectors of every country’s economy, ICT has brought significant growth and productivity, expansion to new markets and innovations of new products and services.

Traditionally, universal access involved fixed line telephone and this puts its governance under the ambit of national telecommunications regulators. However, at the international level, International Telecommunication Development Sector (ITU-D), plays a role of developing policies as well as providing training and capacity building to its member states. There is a Common desire and commitment to build a people-centered, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes(WIS, 2015)

(iii) Next-Generation Pathways

The rapid evolution of technology comes with great benefits to the Internet. However, the process of embracing new technologies can be confusing and therefore is an area that requires governance. Technical community often feels that implementing new technology is a matter that should be left at the decision of the consumer. However, the government may argue otherwise. A classic example is where some governments have opposed the use of Voice over IP telephony reasoning that it may lead to loss of revenue for the incumbent telecom operators. In other situations, many governments may refuse to license spectrum Wi-Fi networks citing issues of security. Therefore governments may choose to give priority to some technologies over others in an effort to pursue social or development goals. This basically means that decisions to introduce new pathways is a governance decision and is often an issue of the state and other involved stakeholders. It is therefore important that a comprehensive IoT Governance should include mechanisms to introduce new technology pathways in a smooth and effective manner. Next generation technologies also require governance to ensure that they are deployed in a manner that is harmonious with legacy systems. Such coordination should happen at every level of the network but it is especially critical at the infrastructure layer to ensure proper communication between the layers as it can be meaningless to implement new technology which cannot communicate with older or legacy systems. Governance is needed to ensure that standards and other technical specifications are compatible with legacy systems. Standard bodies such as IETF and ISO have the responsibility of ensuring that new technologies are compatible with legacy systems. For open source based standards, consumer and user groups sometimes have greater say over which technologies are adopted and how they can promote social and other values.

a) Logical Layer

The logical layer sits upon the infrastructure layer and consists of software programs and protocols that give life to the installed infrastructure and also provides an interface to the user. Issues that need governance at this layer include standards, domain name system (DNS) and IP allocation and numbering. Standards are important in order to make the Internet operate seamlessly over diverse operating systems, browsers, networks as well as different devices. Domain Name System maps IP addresses to domain names thereby allowing users to use memorable alphanumeric names to identify network services such as the World Wide Web and email servers. The DNS has been an issue of heated as well as interesting debate in Internet Governance due to the central role played by the Washington controlled Internet Corporation for Assigned Names and Numbers (ICANN) which the activity.

(i) Standards

Standards are important in order to make the Internet operate seamlessly over diverse operating systems, browsers, networks as well as different devices. Examples of such standards include TCP/IP protocol suite which is the heartbeat of the Internet as well as the Hypertext Mark-up Language (HTML) and the HyperText Transfer Protocol (HTTP). There is need for governance in standards because their effectiveness depends on ubiquitous acceptance which also depends on institutions to decide upon and publish specifications. There is also need for governance on standards so that they ca n be consistently updated to accommodate new technologies. This arises because of security concerns due to viruses, spam and other offensive content. Such issues have driven calls for new specifications for TCP/IP that would address more of these security risks. Likewise, some feel that the spread of broadband and the rise of applications relying on voice and rich media like movies, require the introduction of Quality of Service (QOS) standards to prioritize certain packets over others. There are various actors that control critical standards including:

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN was formed in 1998 as a private, non-profit organization and contracted by the U.S. Government to manage TCP/IP addresses and Domain Names. It was formed as a new model for governance of the Internet and was expected to be international, democratic and embrace all stakeholders from all sectors. ICANN through its assigned numbers authority, IANA allocates chunks of TCP/IP addresses to regional Internet registries who further distribute them to Internet Service Providers. It is also responsible for operating the Internet's root server system, creating policies to introduce new TLDs to the root system, allocating Domain Names through delegation to Internet registrars, assigning unique TCP/IP protocol parameters and administering the root zone file. However, it has proved to have many shortcomings and has been proven controversial from the start to the extent that has led many disfranchised stake-holders to suggest that a more conservative structure of Internet governance crafted around multilateral institutions such International Telecommunications Union or the United Nations could be more suitable for Internet governance.

The Internet Engineering Task Force (IETF)

IETF is the standards body for the Internet and is open to participation to all individuals and groups. It is the architect behind the development of TCP/IP protocol suite and such core protocols that are fundamental to Internet's operation. It main role is to develop prototypes that standardize Internet addressing scheme, establish standards for compression, encryption and security, mechanisms for error detection and correction as well as other crucial engineering attributes. IETF openness, participatory and consultative decision making processes coupled with relative lack of organization hierarchy has made it a model for an inclusive, yet highly effective, system of governance that is unique to the Internet. The IETF has been known to be open and transparent with its deliberations, documentations as well as standards. It publishes its history of meeting proceeding online as well as its mail distribution list. The IETF publishes the standards and supporting materials in archive known as the Request for Comments (RFC) series.

International Telecommunication Standardization (ITU-T)

International Telecommunication Union (ITU) is the UN agency charged with global coordination of information and communication technology and its standard setting wing is the ITU-T. ITU is charged with assigning radio spectrum, coordinating satellite orbital positions, establishing telecommunications standards and promoting information and communication infrastructure advancements in the developing world. ITU-T sets standards through study groups who give recommendations that are eventually supposed to be approved by member states. Its standards carry considerable weight by virtue of being one of the oldest standards body and a UN member. Its regulations influence most network operators given that data is carried over a wide range of communication media.

World Wide Web Consortium (W3C)

W3C was created in 1994 to enhance the World Wide by developing standards and protocols that usually sit on top of core Internet standards such as TCP/IP and it is also charged with ensuring interoperability.

(ii)Management of Domain Names

The Domain Name System is used to resolve human-readable hostnames like *www.Dyn.com* into machine-readable IP addresses like *204.13.248.115*. DNS also provides other information about domain names, such as mail services. DNS is like a phone book for the Internet. If you know a person's name but don't know their telephone number, you can simply look it up in a phone book. DNS provides this same service to the Internet. When you visit *http://dyn.com* in a browser, your computer uses DNS to retrieve the website's IP address of *204.13.248.115*. Without DNS, you would only be able to visit our website (or any website) by visiting its IP address directly, such as http://204.13.248.115. DNS management and coordination is another area that requires governance at the logical layer. Internet Corporation for Assigned Names and Numbers (ICANN) the body whose function is to control DNS and until 2000 the Internet had eight generic top level domains and because of the rapid Internet there were calls for more to be added. Currently the following generic top level domains (gTLDs) exist: .arpa, .com, .net, .org, .int, .edu, .gov, .mil, .aero, .biz, .coop, .info, .museum, .name and .pro. ICANN has recently announced another set of gTLDs which are yet to become operational. In addition to these gTLDs, the DNS has other top level country code domains (ccTLDs) which are representing individual countries such as .au (Australia), .uk (United Kingdom), .tz (Tanzania) and .ke (Kenya). The DNS has been an issue of heated as well as interesting debate in Internet governance as there is feeling that the U.S. Government has monopolistic of Internet Corporation for Assigned Names and Numbers (ICANN) to the exclusion of other countries.

(iii) Internet Protocol (IP) Allocation and Numbering

IP addresses are numerical set of four numbers, ranging from 0 to 255 separated by periods and assigned to each device connected to the Internet. IP address serves two main purposes of identifying the host or network interface as well as location addressing. The first IP address scheme is 32 bit number version 4 which is now almost depleted due to rapid Internet expansion. The next version is IPV6 which was developed in 1995 and standardized in 1998.

There are several governance issues that have been addressed in the IP numbering scheme. Under the current IPV4, there are 4.2 billion possible devices that can be connected to the Internet. However, with proliferation of Internet enabled devices such as cell phones and other Internet of Things that need unique IP address to communicate on the Internet, the existing IPV4 addresses are almost depleted. This issue has been addressed in two fronts: First, the technical community has developed the next version of IP addressing scheme known as IP version 6. This new version of IP protocol will have some 340 undecillion (3.4 × 1038) addresses that will essentially solve the shortage of IP addresses. Second, the technical community has introduced a process known as Network Address Translation (NAT) which enables the use of private IP addresses. In this arrangement, individual computers within a corporate network are assigned private IP addresses which are not unique and are not routable on public Internet. When these computers want to access the Internet, their private addresses are translated into public IP at the corporate network boundary using the NAT server. This process has enabled the extension of IPv4 addresses to accommodate more devices.

Currently Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the IP address systems. IANA allocates IP addresses from the pool of unallocated addresses to the Regional Internet Registries according to their needs and global policy. IANA also maintains a registry of all IP address blocks that have been allocated to each RIR.

b) Content Layer

The content layer is considered to be the place where an average user experiences the Internet. It contains the programs, services and applications users' access on their everyday life. Governance at this layer is of utmost importance to the user and includes issues such as Internet pollution, cybercrime and intellectual property rights.

(i) Internet Pollution

Internet pollution is the term that refers "*to a variety of harmful and illegal forms of content that clog or pollute the Internet*". These include spam or unsolicited emails, viruses, pornography as well as other spyware and phishing attacks (an email that solicits sensitive information such as bank account). Internet pollution epidemic has risen to unprecedented proportions over the last decade with spam messages accounting for 59.56 percent of email traffic worldwide in September 2017. Internet pollution causes huge economic damage and reduces users' trust in using the Internet. Trust is of paramount importance to the steady and continued growth of the Internet and when users begin shying away from the open nature of the Internet that has been a key factor for its success, this is likely to slow down the spread of the Internet and dim the prospects of online trading and e-commerce and would be very bad for the Internet economy. The main reason which has propagated the continued growth of Internet pollution is the difficulty in combating it. This is because spam and viruses usually take advantage of the Internet's anonymity and its end-to-end nature making them difficult to track using the existing conventional methods and tools. Pollution issue therefore presents challenge to the traditional governance mechanisms and new tools. Combating it therefore requires new structures and tools as well as new approaches. Technical approaches to spam control include junk mail filters that are currently implemented in many email clients. Other industry and civil society groups like the Messaging Anti Abuse Working Group which is a coalition of leading ISPs, including Yahoo, Microsoft, America Online, and France Telecom have been advocating for a set of technical guidelines and best practices to stem the tide of spam. Similarly, the *Spamhaus Project* is an international non-profit organization that collaborates with law enforcement agencies to track down the Internet's Spam Gangs, and lobbies governments for effective anti-spam legislation.

(ii) Cybercrime

Cybercrimes or computer related crimes are crimes that involve a computer and a network. These crimes can be divided into a number of different classifications. First, computers may be incidental to a crime. An example is where a drug trafficker uses a computer to store records of his transactions such as drug shipments and payments and therefore making the computer a tool of significant evidential value. The second classification involves a computer being used as a device for executing a crime. A case in point is the *United States v Osowski and Tang (2001)* in which the defendants fraudulently used their authorised access to a stock disbursals management system and transferred a stock valued at USD 6.3 million into their personal brokerage accounts. The above scenarios present old crimes being committed using new tools. The third classification is where a computer is the target of the crime. The classic example happened in Estonia in 2007, when a group of Kremlin sponsored hackers launched series of denial of service attacks that brought down internet services in the whole country. This synchronized attack against government agencies and banks using botnets prompted Estonia to seek assistance from NATO to restore services and urged the EU to criminalize cyber attacks. This is a typical example of new crimes using new tools.

Technological advancement has shown that many objects now have computing devices embedded in them and are capable of storing, processing and transferring data. This means that criminals can exploit these devices to create new opportunities for crime. With this in mind, we can expand the definition of cybercrime to include all offences that are committed against individuals or organizations with a criminal intent to harm the reputation of the victim or cause physical, mental or financial harm to the victim directly or indirectly, using computers as well as telecommunication networks such as the internet and mobile phones.

Computers and the internet are now emerging in many types of criminal investigations and their increasing use with ill intent by law breakers present challenges as to whether we have adequate legal tools and resources to investigate and prosecute cybercrimes.

One of the main challenges to combating cybercrime is that of jurisdiction. Jurisdiction relates to which law enforcement agency is authorized to investigate and adjudicate a cybercrime case and the extent of that authority. Any justice dispensing agency will only have power to investigate and adjudicate crimes that have occurred within their jurisdiction. This may include the geographic location of the criminal as well as that of the victim and the actual locality where the crime was committed. Law enforcement agencies are not allowed to investigate a cybercrime which has occurred beyond the borders of its jurisdiction without a formal and approved request. Cybercrime has no boundary and it is a kind of crime that does not need the offender to travel across country borders to commit a crime. This makes investigations and the prosecution of the perpetrator much harder.

(iii) Intellectual Property Rights(IPR)

IPR has become a major concern in Internet Governance in recent times. This is because the Internet, in large part has aided copyright violations using simple processes such as copy paste or through P2P networks like Kazaa and Napster which allow individuals to connect and illegally share digital music and video files in a massive scale. Music industry has emerged as perhaps the most hit and also the most important Intellectual Property Rights issue today. The rampant violation of Intellectual Property Rights has seen many governments strengthening copyright laws and extending their application to the Internet. Many governments have enacted a number of statutes and laws to strengthen provisions and this has resulted in downward trend in sales of copyrighted work.

The beginning of 1990s has seen introduction of domain names as new intellectual property in the online world and this has given rise to a new area of Intellectual Property law and policy emerging specifically due of the Internet. As the commercial potential of World Wide Web became apparent, a new trend known as cyber squatting emerged. This is the practice where websites containing company names or other forms of intellectual property are registered by users and, often, resold to unsuspecting companies in question for exorbitant sums. Resolving such disputes over domain names became very difficult as there were no precedents or case laws for references and also due to the fact that the Internet is international making determination of the relevant jurisdiction harder to identify. The ICANN responded to this through the help of WIPO and developed Domain Names and the Uniform Dispute Resolution Policy (UDRP). This is a series of guidelines that aimed to circumvent the often cumbersome, expensive and ineffective legal options available. It contains instructions for domain name registrars on when and how to cancel or transfer ownership of domain names in dispute.

(iv) Privacy and Data Protection

Privacy and data protection are closely interrelated Internet Governance issues. The terms privacy and data protection are closely related and are often used synonymously. Privacy is a valuable aspect of any human personal life and data or information protection safeguards the rights of a person to privacy. Data protection accords legal protection to a person in cases where his or her personal information is to be collected, stored, used or communicated by a third party. Data protection affords a person the right to know what information about them is held by the controller and ensures

that personal information is managed in confidentiality by the data controller and not arbitrarily disclosed without their consent. Put in another way, privacy can be seen as a legal issue while data protection is more of a technical issue. That is to say, to ensure privacy especially in reference to personal data and information, that data must be technologically protected. In other words, data protection safeguards a person's right to privacy. While the word privacy is commonly applied in the USA, the phrase data protection is more popular within the European Union member countries.
With the technological advancements and rapid proliferation of cross-border trade, compliance with international privacy and data protection legislations and standards is imperative and lack of adequate protection could hinder business operations and become huge barrier to international trade. The internet and e-commerce has led to huge free flow of information across international borders and therefore it is imperative that personal protection data and privacy laws be put in place to make sure that individuals enjoy their fundamental rights and freedoms.

III. Developmental Issues and Digital Divide

The issues of sustainable development should always at the forefront of Internet Governance debate because sustainable development cannot be achieved without global communications and knowledge exchange. This therefore effectively means that the outcomes of the Internet Governance debate will affect our ability to manage the social, environmental and economic factors of sustainable development. It therefore follows that access to the Internet infrastructure is an indispensable resource for general development and economic growth and a vector for sustainable development. However, the high cost of access to the Internet has major implications for developing countries who find themselves unable to compete on global level in economic sectors that are highly influenced by the Internet such areas as outsourcing industries or software production as well as areas of e-commerce that depend entirely on the Internet.

a) The Digital Divide

Digital divide is the term used to define the gap or rift between those who have got access and capabilities to use the Internet and ICT and those who do not. The term is always being used to refer to the rift between developed and the developing world. With the increased dependence on the Internet for business and economic development, lack of access to the Internet means lack of access to the world markets thereby hampering mainly developing countries from selling their products and services on a global scale and restricting the choice of goods and services available. Internet Governance impacts digital divide in the following areas:

(i) Internationalizing of Domain Names

Currently, domain names follow standard ASCII (American Standard Code for Information Interchange) characters which support Latin alphabet. This means that other international characters such as Asian are not supported and this has led to a feeling by developing countries that the exclusion of their languages from domain names limits their access to the Internet because users who are not familiar with English language have problem accessing English language URLs.

ii) Country Code Top-Level Domains(TLD)

This is also another issue that is likely to determine access in developing countries. Where governments are in charge, they have always mismanaged these valuable resources. This was witnessed in Cambodia when the government took over management of Cambodia's ccTLD from an NGO. This led to the ccTLD becoming less inefficient and more expensive. Poor management has led to missed opportunities as operators in developing countries have successfully marketed their ccTLD alternatives to ICANN's top-level names such as .tv for TV stations, .md for medical and health, .fm for radio stations and etcetera.

(ii) Standards

Decisions on technical standards can play big influence on digital divide. Standards play important role of making the global Internet connect seamlessly and affordably. However, problems comes when proprietary (i.e., whose intellectual property is owned by private entities) standards are used. This can make the costs of access to technology prohibitive by requiring expensive royalty payments, thereby limiting access by developing countries. It is also evident that developing countries do not only suffer from usage of propriety standards, but also from the process of "hijacking" open standards by private companies who make modifications to these standards and then turning them into de-facto proprietary standards. A classic example is the regular enhancements by private companies to HTML and XML. The result is that many features on certain web pages can only be fully accessible for example, using Microsoft Internet Explorer.

b) Overcoming the Digital Divide

Access to computers and the Internet and the ability to effectively use this technology are crucial for citizens to fully participate in economic, political and social development in order to bridge the widening gap of the digital divide. People should use the Internet to market and also to find lower prices for goods and services. The Internet allows people to work from home or start their own business, acquire new skills using distance learning, and make better informed decisions about their healthcare needs. The ability to use technology is becoming increasingly important in the workplace, and jobs in the rapidly growing information technology sector pay almost 80 percent more than the average private sector wage. Financial assistance, especially for the developing countries through bilateral and multilateral agencies like UNDP and World Bank can also help in bridging the digital divide. The importance of the financial aspect was clearly recognised during the Geneva phase of WSIS. One idea proposed at WSIS was the establishment of an UN-administered Digital Solidarity Fund to help technologically disadvantaged countries build telecommunication infrastructures.

IV. Conclusion

In the advent of the digital age and the new normal, internet usage has become part parcel of human life. The main advantage of strengthening internet governance is to create order in the cyberspace.

However the over reliance on the internet without a standardized rules of access and communication may downplay the importance of governance in the cyberspace. This is particularly true when management of intellectual property, affordability of the access equipment (hardware and software) are not bound by some global rules and procedures. In addition rules that ensure equitable sharing of services provided by the internet, needs to be fronted to all users. Some order is necessary to counter-act the information overload outage in the internet. Internet governance is therefore key in addressing the emerging challenges in the cyberspace. This paper addresses governance issues that would provide guidance to organizations, researchers and individuals on the key issues that needs to be considered when striving for good internet governance.

References

[1] Bell, R. (2002). The Prosecution of Computer Crime, *Journal of Financial Crime*, Vol. 9 Issue: 4

[2] Benkler, Y (2000) 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Common and User Access' *Federal Communications Law Journal* Vol 52 pg 561, 562-63 [Online] https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1242&context=fclj

[3] Birnbaum, M (2013) 'Germany looks at keeping its Internet, e-mail traffic inside its borders' *The Washington Post,* November 3 [Online] https://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html?noredirect=on&utm_term=.9359832b66bc Accessed 17 June 2018

[4] Château de Bossey (2005) ‘Report of the Working Group on Internet Governance’ [Online] http://www.wgig.org/docs/WGIGREPORT.pdf Accessed: 19 June 2018

[5] Franz-Stefan Gady (2016) 'The Wuzhen Summit and the Battle over Internet Governance'*The Diplomat* [Online] https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance/ Accessed: 26 June 2018

[6] Gelbstein, E. and Kurbalija, J., 'Internet Governance: Issues, Actors and Divides' *Diplo Foundation*, p. 62. [Online] http://www.unapcict.org/ecohub/resources/internet-governance-issues-actors-and-dividesAccessed: 18 June 2018

[7] Guerrini, F (2014) 'In Search Of A Governance. Who Will Win The Battle For The Internet?’ [Online]https://www.forbes.com/sites/federicoguerrini/2014/10/24/in-search-of-a-good-governance-who-will-win-the-battle-for-the-future-of-the-internet/#1056e14d321c Accessed: 24 June 2018

[8] Halder, et al (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. *Hershey, PA, USA*

[9] Internet Society (2016) ‘Why the Multi-stakeholder Approach Works’ [Online]https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

[10] Kapur, A (2005) ‘Internet Governance: A Primer’ *UNDP, Elsevier* [Online] http://www.unapcict.org/ecohub/resources/internet-governance-a-primerAccessed 17 June 2018

[11] Masters, J (2014) ‘What Is Internet Governance?’*Council of Foreign Relations*[Online]https://www.cfr.org/backgrounder/what-internet-governanceAccessed 17 June 2018

[12] Moore, R. (2005) Cyber crime: Investigating High-Technology Computer Crime, *Cleveland, Mississippi: Anderson Publishing*

[13] ITU (2003) ‘Declaration of Principles - Document WSIS-03/GENEVA/DOC/4-E’ [Online] http://www.itu.int/net/wsis/docs/geneva/official/dop.html Accessed: 29 June 2018

[14] ITU (2003) ‘Plan of Action- Document WSIS-03/GENEVA/DOC/5-E WSIS [Online] http://www.itu.int/net/wsis/docs/geneva/official/poa.html Accessed: 29 June 2018

[15] Olivier, S., (2009) Internet Governance and Democratic Legitimacy (September 30, 2009). *Federal Communications Law Journal,* Vol. 62, No. 2, 2010; *Fordham Law Legal Studies Research Paper* No. 1504159. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1504159

[16] Ray, K. R. S., ‘The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology’, *University of Chicago Law Review,* Forthcoming. Available at <http://ssrn.com/abstract=266964> Accessed: 29 June 2018

[17] Unknown Author (2017) ‘Global spam volume as percentage of total e-mail traffic from January 2014 to September 2017, by month’ [Online]https://www.statista.com/statistics/420391/spam-email-traffic-share/ Accessed: 19 June 2018

[18] UNESCO (2017) ‘Taking forward multi-stakeholder participation in Internet governance’ [Online]https://en.unesco.org/sites/default/files/msm_unesco_summary_30032017_2.pdfAccessed: 25 June 2018

[19] VON RONDA HAUBEN (2015)'Three Models for Internet Governance : Multi-Lateral, Multi-Stakeholder, or Netizen Model? Introduction to ACN Issue vol 26 No 1'Taz blogs [Online] https://blogs.taz.de/netizenblog/2015/11/23/three-models-for-internet-governance/Accessed: 26 June 2018