Dangerous Democracy: State Power and Internet Governance

Aaron F. Brantly, PhD

“There is a proverbial war taking place and it affects everyone globally. It does not include guns and bombs, but rather control over bits and bytes that flow at light speed across national boundaries and influence the world in profound ways. The freedom of information is challenged by democratic processes and institutions that are at odds with the human desire for open and unimpeded access to information. The conflict contains a paradox in which democracy within the institutions that govern the Internet pose a threat to the freedom of information and to the citizens of states and regimes around the world. Internet governance is a challenge that pits corporations, states, institutions and individuals against one another in the pursuit of complex geopolitical ends. This chapter examines the complexity of internet governance and the challenges that democratic institutions pose to the global flow of information and communications.

There is also a tendency to be predisposed to the assumption that democracy is the penultimate form of governance. This chapter dispels that notion and presents the reader with a nuanced and complex world view in which democratic institutions are not representative but repressive. The global population has exceeded 7 billion persons, the number of individuals connected to the Internet globally falls just short of half the total global population. The number of internet enabled devices, constituting the Internet of things (IoT) is estimated to constitute 17 billion and will likely exceed 50 billion by 2020. The reality of the Internet and the devices that comprise it is not some amorphous construct beyond tangible physical reality, but rather they are physical and logical structures operating within the shared standards of a wide-reaching community of individuals, corporations, and states. Each of these entities have overlapping interests. Overlapping interests come in the form of dependencies, regulatory structures, policy frameworks and more. The Internet is more than a series of random tubes, is an example of technocratic bureaucracy with complex governance structures designed to ensure its technical viability and efficiency.

This chapter proceeds in three sections. First, it outlines the historical origins of both the technical and governance processes of what we broadly refer to today as cyberspace and provides a concise

---

2 http://www.internetworldstats.com/stats.htm
examination of the structure and function IANA, ICANN, W3C, the Internet Society and the International Telecommunications Union. Second, the paper examines the controversial nature of Internet governance. Third the paper establishes the framework for a robust discussion on the benefits and perils of democratic governance over the internet and its associated technologies.

As users of the Internet and cyberspace more broadly most individuals have little visibility into the inner workings of a complex environment that operates across dozens of jurisdictions both within and between states across the international community. The challenges of Internet governance are likely to persist for decades to come and likely to increase in difficulty in the face of competing interests and perceived threats. Democratic idealism in the absence of context is potentially ill-advised. Instead this work provides the reader with a thoughtful overview of many, but certainly not all, of the core issues at stake to facilitate more informed decision-making.

A brief overview of the Internet and its governance structures

Although common myth purports that the Internet was primarily designed as a mechanism for command and control survival in the event of nuclear war, the origins of this network of networks arose more from a need to share resources and information efficiently.\(^4\) Funded out of the Advanced Research Projects Agency within the Department of Defense, the primary objective of the ARPANET was connect expensive computing resources around the country to enhance scientific knowledge.\(^5\) The underlying concept that makes the Internet function, packet switching, was developed nearly simultaneously and independently in the United States by Paul Baran, and the United Kingdom by Donald Davies.\(^6\) The concept of packet switching revolutionized a nearly 100 year-old concept of circuit switching by removing the need for a single dedicated line to transmit a message in its entirety. The concept illustrated in figure 1 below was challenged from the start by stalwarts in the telecommunications industry. However, subsequent tests

---


\(^5\) Ibid.

\(^6\) Ibid
of packet-switched networks demonstrated network efficiency (both in speed and cost) and resilience compared to traditional circuit switched networks.

Packet-switched network

![Packet-switched network diagram]

Circuit-switched network

![Circuit-switched network diagram]

Figure 1: Packet vs. Circuit Switched Networks

By breaking digital information apart in to small pieces, identifying those pieces with specific information and allowing them to travel in the most efficient way possible from point A to point Z they were able to share limited infrastructure with other communications simultaneously and suffered less loss in transit. If a packet fell off the receiving computer would request retransmission of the missing packets. ARPA scientists facilitated the expansion of the network of networks across multiple institutions within the United States and even to Europe. The result was a robust network of computers able to share expensive processor time and able to facilitate communications. One of the first major forms of communications was the development of early iterations of electronic mail, or email.
As the connections between nodes within the network increased in complexity and as the number of programs available expanded there arose a need to focus on the technical and functional aspects of this technological evolution. The early methods of communicating the evolution of network structure and code was to write an “RFC” or request for comment. The first RFC was written by Steve Crocker at UCLA discussing the IMP (Interface Message Processor) in 1969. RFCs became a crucial aspect of both improving and maintaining the evolving network. The RFC process is still active and constitutes a core aspect of general technical governance associated with the continued development of the Internet.

Internet governance has increased in complexity in parallel with the increasingly connected nature of the networks it seeks to govern. RFC 584 establishes the charger for ARPANET Users Interest Working Group. The group, established on 23 May 1973 was designed to provide an institutional mechanism for the increasing number of technical and procedure needs of a burgeoning system. The original ARPANET working group morphed with the needs of the community and eventually became the Internet Working Group. In the late 1970s Vint Cerf, the then Program Manager for ARPANET (Under the renamed Defense Advanced Research Projects Agency), recognized the need for the creation of new coordination bodies. Cerf recognized the growing problems arising in a decentralized network. To further develop the network standards and protocols needed to be examined and agreed upon, rules and policies for behavior needed to be developed, and more. Two of the first governance bodies established were the Internet Cooperation Board (ICB), Internet Research Group (IRG) and the Internet Configuration Control Board (ICCB). In much the same way that driving requires agreed upon rules of the road for all cars to transit a city, the these boards established the agreed upon rules of the wires to ensure the functioning of a complex socio-technical system.

The heads of the ICCB and the ICB and other smaller groups worked together to form the Internet Activities Board (IAB). Early iterations of the ICB and the ICCB were unable to adequately address all of the challenges faced by the growing community. Barry Leiner, the DARPA Internet Research Program Director in 1983 disbanded the ICB and replaced it with the Internet Engineering Task Force (IETF). As funding for the burgeoning network shifted away from DARPA and towards the creation of NSFNET (National Science Foundation Network) IAB was without its primary sponsor. This necessitated the further reorganization the IAB and its sub-groups/task forces. The eventual outcome in the 1990s was the IAB, IETF and a new conglomeration of technical task forces called IRTF (Internet Research Task Force).

---

7 Interface Message Processor, a device at the edge of a local network designated with interpreting external requests for the network and broadcasting internal requests to other machines.  
8 RFC 1 https://www.rfc-editor.org/rfc/rfc1.txt  
Finally in 1992 the three main groups the IAB, IETF, and IRTF were placed under an overarching organization called the Internet Society (ISOC). ISOC was founded by Robert Khan and Vint Cerf with the following at the core of its charter:

The Society will be a non-profit organization and will be operated for international educational, charitable, and scientific purposes, among which are:

- To facilitate and support the technical evolution of the Internet as a research and education infrastructure and to stimulate involvement of the academic, scientific, and engineering communities (among others) in the evolution of the Internet.
- To educate the academic and scientific communities and the public concerning the technology, use, and application of the Internet.
- To promote scientific and educational applications of Internet technology for the benefit of educational institutions at all grade levels, industry, and the public at large.
- To provide a forum for exploration of new Internet applications and to foster collaboration among organizations in their operation and use of the Internet.¹¹

The Internet Society Controls a significant portion of core Internet functionality. However, in 1989, Tim Berners-Lee proposed the creation of a new information management system known as Hypertext Transfer Protocol (HTTP).¹² HTTP has become the core of what we know today as the World Wide Web. In 1994 Berners-lee founded the World Wide Web Consortium (W3C). W3C is a governance organization of the World Wide Web in much the same way that the Internet Society is for all the protocols that constitute the Internet Writ Large. W3C serves as a standards, education, outreach and development organization.

The continued advancement of the Internet further increased the need for governmental organizations to play a role in the development of standards, procedure and policies. ICANN has been historically the most controversial of all the governance organizations associated with the Internet. ICANN initially began in IANA (Internet Assigned Numbers Authority) and Jon Postel a computer scientist with the University of Southern California. It is hard to think of the Internet as a limited resource, but under the original IPV4 (Internet Protocol Version 4) structure first described in RFC 791 and later adopted into active use on the ARPANET in 1983. There are 4.294 billion possible unique IP addresses. Every devices

on the Internet requires an IP address for traffic routing purposes. While 4 billion seems like an inordinately large number, as indicated above, globally there are currently in excess of 17 billion devices. In the initial days of the Internet all request for IP address space were processed by a Postel and logged. As the network grew in size it became too complex for a single individual to manage. As IP addresses merged with the concept of Domain Names, names that reference numbers, the problem became even more complicated. The death of Postel severely affected the community. Vint Cerf proposed the establishment of an organization to take on the task previously managed by a single individual.

On 30 January 1998 the National Telecommunications and Information Administration, a sub agency within the US Department of Commerce proposed in a Green Paper the creation of a hybrid organization able to manage the increasingly complexity of the Internet.\textsuperscript{13} Later that year ICANN (Internet Corporation for Assigned Names and Numbers) was formally established. ICANN and its suburbanization IANA have been operating since under the oversight of the Department of Commerce. This oversight is set to expire following approval of the U.S. National Telecommunications and Information Agency in April 2016. DoC oversight officially ends in September 2016.

Among the many important tasks of ICANN and IANA are the allocation of address space under both IPV4 and the newer IPV6 protocols. ICANN manages the distribution and management of Top Level Domains (TLDs) such as .com, .org, .us., .ua and others. ICANN also facilitates domain name dispute resolution when two competing entities both claim the same domain name. ICANN has been the subject of significant criticism by a variety of domestic and international actors to deride the control the United States government possessed over a critical Internet resource.

Another organization that in recent years is increasingly weighing in on Internet governance is the International Telecommunications Union (ITU, Formerly the International Telegraph Union). Whereas most of the other major players in Internet governance are non-governmental or hybrid models, the ITU is an International Governmental Institution composed of United Nations member states. The ITU was found in 1865 and coordinates international cooperation on a variety of information communications technology related issues.\textsuperscript{14} However, while the other organizations are driven largely by individuals, corporations, governments all with proportional representation in largely consensus driven governance styles, the voting members of the ITU are exclusively states with all other types of actors acting at non-voting sector members. The role of the ITU within Internet governance has grown in importance since 1998 when

\textsuperscript{13} Improvement of Technical Management of Internet Names and Addresses; Proposed Rule. National Telecommunications and Information Administration. https://www.ntia.doc.gov/legacy/ntiahome/domainname/022098fedreg.htm

\textsuperscript{14} http://www.itu.int/en/about/Pages/overview.aspx
members voted on a resolution to hold a summit called the “world summit on the information society (WSIS).”

Complex Controversies

Internet governance is complex. The interests of those who have a stake in how the Internet operates are often in conflict because of economic, structural, technical, legal, policy, moral, and ethical issues that arise on a daily basis. Conflict over the rules governing the interactions of individuals in cyberspace are endemic to the very nature of an evolving system. The controversies associated with Internet governance are best broken down into groups by actor type. Five base categories, each constituting multiple sub-categories, include supranational actors, state actors, sub-state actors, corporate/business actors and individuals. Broadly interests can be examined as contests both across and within these categories.

Supranational actors are organizations or entities composed of states with policy responsibilities over large portfolios of issues. The most prominent supranational organizations include the North Atlantic Treaty Organization, The United Nations, the European Union etc. Supranational actors can facilitate cooperation and agreement amongst their member states but they also contain policy responsibilities outside of their state components. The International Telecommunications Union (ITU) is part of the supranational United Nations. The ITU as an agency within a supranational actor seeks to expand is policy relevance and control over various aspects of the Internet.

Supranational actors themselves can contain democratic structures for the inclusion of divergent state representation, however they are not necessarily wholly or purely democratic. Organizations like the United Nations are only quasi democratic in that they allow for state representation within the governing constraints imposed by its structure in particular the ability of permanent members of the Security Council to veto UN resolutions made in the more democratic General Assembly.

State Actors are nation states that constitute sovereign political bodies as broadly outlined by some recognized combination of de jure\(^\text{16}\) and de facto\(^\text{17}\) sovereignty. Sovereignty indicates state management of both their domestic and foreign affairs. Management of these affairs can contradict international norms and result in challenges to sovereignty, but generally sovereignty is an established mechanism by which states define both the limits of their physical and jurisdictional responsibilities. Cyberspace challenges many traditional notions of sovereignty through the creation of markets and information flows from external and

---


\(^{16}\) De jure, or legal, sovereignty concerns the expressed and institutionally recognized right to exercise control over a territory.

\(^{17}\) De facto, or actual, sovereignty is concerned with whether control in fact exists.
internal parties. State actors can be broken further into two more specific categories, democratic and authoritarian political systems, with highly divergent views on the role of the state. The open architecture of the internet challenges aspects of both types of political systems.

Democracies are generally more acceptant of unregulated sources of information, while autocracies are generally more constrained in their approaches. There are nuances between both categories and amongst states within each of these categories. State actors are considered representative of the interests of their citizens through the legitimacy of their sovereign power. For rules related to Internet governance to be made without state consent is to ignore sovereign government representation behalf of its citizens. However, as will be illustrated in the next section often the representation of states while democratic at the international and even supranational level can be wholly undemocratic domestically.

Sub-State Actors are groups or organizations that use, control, manage, engage or in some way interact with the Internet for a variety of purposes. Such groups can be non-governmental organizations (NGOs and INGOs) or they can be groups that reside outside of commonly accepted domestic and international laws such criminal or terrorist organizations. While the former set of groups can and often do participate in governance aspects of the Internet, the later do not. Many NGOs and INGOs are deeply involved in internet governance at various levels ranging from domestic involvement in human rights to international involvement in transit rights of data and a range of issues in between. Criminal and terrorist organizations are largely absent from formal discussions on Internet governance, but their actions heavily influence the subsequent development of laws and policies associated with Internet governance.

The sub-state actor category is extremely diverse, yet distinct from other actor categories. Many of the actors it contains are constitutive of selective or specialized interest groups engaged in activities outside of formal governmental responsibilities. The organizations identified in the first section to include, the Internet Society, WC3 and to a great extent ICANN are constitutive of INGOs and are highly specialized. While these organizations themselves might possess democratic qualities within their internal rule making and organizational structures they are not broadly representative of state or citizen interests across nations.

Corporate actors are business interests ranging from small to large. Interests within this category are extremely diverse and are generally reflective of willingness to accept exposure to global markets. Within the corporate actor category are two sub-categories with a disproportionate amount of influence on both domestic and international policy-making within the field of Internet governance. Technology companies generally want increased exposure to global markets through net neutrality rules. Telecommunications providers and ISPs in particular are often opponents of net neutrality due to losses in potential markets due to preferential pricing for speed, volume and service maintenance of certain customers.
The competition between these two groups led many US companies and technology related interest to engage in a day of protest in which they blacked out their sites or placed information relating to the value and importance of net neutrality.\textsuperscript{18} There are also strong debates within the corporate community over the classification of the provision of Internet as a utility.\textsuperscript{19} The two issues highlighted above are but two of hundreds of issues that come up with regards to the management and maintenance of cyberspace from a corporate perspective.

\textit{Individual actors} are citizens of different countries around the world. Currently there are more than 3.4 billion internet users globally. Every individual has economic and political incentives to engage and leverage the resources of cyberspace differently. Often interests can be as simple as accessing news about what is happening in the world or in their local community. The interests of individuals in Internet governance is understated largely due to a lack of comprehension of the causes and effects of policies. However, just as the above actors all compete or collaborate to influence the function of the core organizations that manage the technical and policy aspects of the Internet individuals are most commonly engaged through their usage and preferences for certain products, services, and protocols. Often individuals only fully grasp the importance of Internet governance when other actors interfere with their routines or in times of political, economic or social strife. A common challenge to individual usage of the Internet is the disruption of service by state actors during times of social unrest.\textsuperscript{20}

Multiple issues arise between the actors above that complicate traditional policy formulation. First, the groups are extremely diverse in both capacity and needs/wants. States have far more capacity than individuals, yet the Internet can be very important for both the state and the individual. Often individual needs in cyberspace are satisfied by actors external to the geographic confines of the state. For instance, Google, provides its Gmail service to users in Germany, a sovereign nation within the European Union. Google, however is an American company with its corporate headquarters in California. Rules on the storage of data associated with the account cross multiple jurisdictional boundaries. Moreover, the transit of the emails from one Gmail account in Germany to another might be broken into packets that cross dozens of sovereign boundaries based on the most efficient packet route. Can any country intercept that content while it is within their jurisdiction? Should a US company providing a virtual service without physical

\textsuperscript{18} For a fun look at the importance of net neutrality See “Net Neutrality: Last Week Tonight with John Oliver”: https://www.youtube.com/watch?v=jpb0EoRrHyU
goods be beholden to German or European law? Simply put, there are cascading policy implications related to decisions at the supranational and national levels on issues such as freedom to access information and the right of states to control information within their own societies.21

Additionally, there are often strong economic incentives on behalf of states and supranational organizations to control aspects of cyberspace for the purposes of taxation, regulation of certain markets and similar issues. Often the rules written to control the flow or storage of information, the economic implications of services or information can affect the protocols fundamental to the operation of the Internet. Harvard professor Lawrence Lessig is famous for his concept of “code as law.”22 Code is a logical structure and engineers and computer scientists are predisposed to elegant and efficient solutions rather than the nuances of varying jurisdictional boundaries.

Second, even when there is near-universal consensus on one area of governance associated with cyberspace, the applicability of sovereign rights is difficult to enforce in many instances or enforcement may conflict with other aspects of the function and use of the Internet. For instance the prosecution of pedophiles is a common area of consensus among states. Nearly all governments are in agreement that child pornography constitutes a violation of both national and international laws and should be prosecuted. However, when applying law to this area states each take a different approach with profound ramifications. To facilitate the capture of criminals some states have proposed or enacted requirements that include real name registration for various services, the use of digital IDs or the registration of system attributes to individuals users and more.23 These rules are not as clear cut as they seem and allow some states to surveil and censor behaviors often considered fundamental human rights by other states. The result is that while agreement on the protection against criminal behaviors is included within a general framework on governance, the implementation of the solutions receives opposition within the states themselves. It is great to track criminals and pedophiles, but do we want to allot the government to track everyone at all times? The debate over what is acceptable and not acceptable has been challenged across the groups of actors and in recent years has met strong challenges within the United States following the release of classified documents by Edward Snowden. Snowden’s document release led to the creation of a commission by

President Obama to examine the balance between what is and is not legal in cyberspace within the United States.  

Third, the cascading effects of policy decisions at various levels of governance subject each group of actors to significant information asymmetries. Asymmetries can occur between and within the actors above and amongst technical and non-technical communities broadly. Laura DeNardis addresses one of the more common misperceptions of online behavior that is dramatically affected by governance policies, anonymity. She writes: “On its surface, the Internet appears to be a public sphere in which anyone can anonymously participate. But entering this sphere usually requires passing through a gatekeeper that possesses personally identifiable information such as name, home address, credit card information, and even possibly social security number.” While many might fondly remember a time when The New Yorker published a cartoon by Peter Steiner with the quote “On the internet, nobody knows you’re a dog,” the reality of the Internet has come to be something far different.

Beyond anonymity, the failure to understand the consequences of policy actions can affect the general function of the Internet as was the case of Pakistan in 2008 trying to enforce domestic law and in the process caused all of YouTube’s global traffic to be siphoned into Pakistan Telecom. The feat was accomplished accidentally by broadcasting a false claim that the correct route to YouTube was something other than its actual route, the result propagated throughout the global network infrastructure and severely damaged global YouTube access. Here, a national policy of censorship affected global access to significant content provider largely due to a failure in understanding of the technical tools to achieve policy outcomes in cyberspace.

The issues highlighted are not all inclusive of the multitude complex issues and actors present within broader discussions on Internet governance. Together the historical, technical, organizational and actor relationships provide a starting point for understanding the dangerous nature of democracy and Internet Governance. The next section focuses specifically on the dangers that arise in push for democratic representation by one or another group of actors within Internet Governance.

Dangerous Democracy

Most students of history and politics are conditioned to believe democracy is the best form of government. We are told that representative democracies are able to mitigate complex disputes and facilitate

the best solution for the largest number of people. However, while this might be true at the national level it has proven to be a very difficult concept to extend outward to the supranational level as illustrated by scholars such as Andrew Moravcsik, Stanley Hoffmann and others.27 States are generally loathe to cede their powers to supranational entities where they are unable to control or significantly influence domestic policy outcomes. While intergovernmentalists and liberal theorists argue that states can establish regimes they also note they implementation and enforcement of the rules and policies established by those regimes remains difficult in many instances.

While in many domains of international interaction between states the implementation of policies in one or another state are reasonably isolated geographically or within specific economic or social sectors, the Internet spans across states and sectors and its protocols are dependent on interoperability and a large degree of trust that each party will implement common protocols. As in the Pakistan case in the previous section when one state violates the concepts of trust either intentionally or unintentionally the broader infrastructure can suffer consequences. There has been a great deal of movement in the last several years to subsume many of the governance functions of the Internet into the ITU. The last major movement occurred in 2012 at the World Conference on Internet Telecommunications (WCIT) in Dubai. At this conference a series of International Telecommunications Regulations were combined into a treaty that was

reviewed and voted on. Figure 2 below shows the distribution of votes on the treaty. There are clear patterns in the vote distribution.

The treaty would have provided states with a greater role in overseeing the telecommunications services within their countries. The treaty was opposed largely along the lines of political systems with authoritarian leaning regimes more supportive of the treaty and democracies opposed. Within the vote there were a number of non-voting interest groups involved including Google. A spokeswoman for Google was quoted in a 2012 Wall Street Journal article saying: “We stand with the countries who refuse to sign this treaty and also with the millions of voices who have joined us to support a free and open web.” Here we begin to see the complexities touched on in the previous section. State actors disagree on the role of states in managing the Internet. Some states are joined by corporate and other sub-state actors and the whole process was facilitated by a supranational organization.

Why is democracy dangerous? Democracy in Internet governance is dangerous because it is not inclusive of all the necessary interests and actor groups or compatible with the technical realities of the

---

29 The text of the treaty can be found here: http://www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf
network of networks as it was designed. Chris Demchak writes that the Internet is a socio-technical-economic system, one that does not lend itself well to single actor governance structures. The borders of the system are real, but the transit of data across borders is defined through protocols, not laws. The current structure of the governance is distributed by function and is inclusive in that any actor can participate given the time and resources available to engage the institutions that currently control its operation. The process is not purely democratic by actor type but rather managed and distributed in such a way as to include the concerns of various actor types. In this way the ultimate goal is not facilitation of interest one type or political system at the expense of the technical, social or economic interests of other participants in the network. Instead Internet governance as it currently stands comprises a unique combination of interests that are constantly in competition in a managed and segmented set of structures. Moreover, the norms associated with these institutions are robust and tend towards slow deliberate innovation and adaptation and discourage unilateral actions by any one actor or actor group. The lack of democratic processes is typically a complaint isolated to state interests who wish to increase their control over the development and management of the Internet both domestically and internationally.

Milton Mueller writes: “Internet governance is the simplest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies.” The debate over the coordination, management and development of the Internet is not likely to disappear anytime soon. As the number of connected devices increases and the number of individuals with access increases there is likely be an increasingly vigorous fight for control over the Internet. Understanding that democracy might not offer the best solution for Internet governance provides a starting point for robust discussions the direction of the Internet while still addressing the needs and concerns of various actors. The key for students and policy-makers alike is to craft robust governance structures able to incorporate disparate needs and wants while still maintaining Internet as a tool that has and will likely continue to profoundly shape the world.

Question to consider:
1. Is it possible to design a governance structure that incorporates a complex socio-technical-economic system that spans sovereign geographic borders?
2. Do democratic governance structures adequately address the needs and wants of actors at various levels?

3. Can democratic structures safeguard fundamental human rights in cyberspace as defined by the United Nations?

Recommended Readings

Articles/Treaties
http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=3170&context=cklawreview.


https://pdfs.semanticscholar.org/c0f3/bc9b6319f35bf6a89ad8bfe808f874991e72.pdf.

2012. Final Acts World Conference on International Telecommunications. WCIT. Dubai,

van Eeten, Michel JG, and Milton Mueller. n.d. “Where Is the Governance in Internet Governance?.” New Media Society,

http://fordham.bepress.com/cgi/viewcontent.cgi?article=1003&context=mcgannon_working_papers.

Websites
Internet Society: http://www.internetsociety.org
ICANN: https://www.icann.org
World Wide Web Consortium (W3C): http://www.w3.org
International Telecommunications Union: http://www.itu.int/en/Pages/default.aspx