UNITED NATIONS COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT

Working Group on Enhanced Cooperation

Revised recommendations submitted in preparation for the 4th WGEC meeting

Submitted by

NICK ASHTON-HART

TECHNICAL COMMUNITY

Proposal for a recommendation for inclusion in the final report of the Working Group on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet (WGEC) 2016-2018.

Proposed by Nick Ashton-Hart – Member for the Technical Community

Rationale:

The Internet's importance to economic and social development has increased dramatically since the WSIS outcomes were agreed and that trend is expected to continue as the number of people connected continues to grow. WSIS recognised that importance and so did its five and ten-year reviews.

It was understood even at WSIS that the public Internet was not monolithic as a policy subject. Many provisions of the WSIS outcomes make clear that its technical functioning was (and is) managed independently of the decision-making related to the software and services which leverage that technical infrastructure to operate.

In the period between 2005 and today disputes about how to implement national public policy priorities given the globalised nature of the communications and services which operate have grown. Disputes about transboundary policy priorities that are within the remit of "enhanced cooperation" continue to grow as well – law enforcement and cybercrime, the extent to which the laws of war extend to cyberspace, national security, measures that impact trade (local hosting, market access for services), and many others. Incidents of large-scale Internet disconnections or blocking of major consumer-facing services from reaching entire populations continue to grow[1].

Stakeholders and policymakers have very different views about measures that block the entire Internet or parts of it. What should be reinforced, especially when states engage in enhanced cooperation between themselves, is that they take into account the wider value of the Internet as a platform for all communications, including but not limited to its role as an enabler for the wider "bricks and mortar" economy, especially in developing countries.[2] It is in the interest of all states, and stakeholders, that the outcome of negotiations in enhanced cooperation ensure measures taken related to the content of certain communications don't damage, distort, or undermine the underlying platform all communications rely upon. This is especially important in respect of measures that have impacts, whether intentional or unintentional, on the public Internet beyond national borders – exactly the objective of enhanced cooperation.

[1] See West, Darrell, "Internet shutdowns cost countries $2.4 billion last year," Brookings Center for Technology Innovation, 2016, at https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

[2] UNCTAD estimated the size of Business to Business ecommerce at US$15 trillion in 2015, with rapid growth in developing countries. See UNCTAD, "Information Economy Report 2015," at http://unctad.org/en/PublicationsLibrary/ier2015overview_en.pdf.

Proposal:

The Working Group recommends that all stakeholders, especially governments, have a responsibility to ensure that actions taken and policies implemented in relation to communications and their content should 'build in' common concepts that are in the interests of all. These apply for equally for national and international policy agreed by states when engaged in enhanced cooperation:

- Measures related to content and communications online must not negatively impact the Network as a Platform for communications generally and its ability to operate efficiently at a technical level, and;
- Such measures do not apply to, or have any impact on, any communication which does not originate from, and is not destined for, a legal or natural person on the relevant territory or within the jurisdiction of a sovereign a communication is merely transiting through.

For the purposes of this recommendation:

- Communications covered include those within a territory which are transient or incidental and an integral and essential element of a technological process that enables communications to transit a territory and whose sole purpose is to enable relevant transmissions in a network between third parties by an intermediary, and;
- The "Network as a Platform" consists of:
  - Those standards-based unique identifiers integral to making interoperable communications possible in an Internet-Protocol-based network, and the licit allocation and use thereof[, *inter alia*, Internet protocol addresses of various kinds and domain names];
  - Licit (and/or where relevant, licenced) activities and operations of legal or natural persons [such as Internet Service Providers and Backbone providers] that are integral to the functioning of basic routing within a territory, and/or international interconnections between territories, which includes hardware and/or software integral to such activities and processes.

It is understood that these recommendations are entirely congruent with, and intended as a practical application of, the provisions of WSIS, *inter alia*, Tunis Agenda paragraphs 57, 47, 45, 42, and 30. This recommendation does not relate to the content of communications, but only those activities and related technical functions which make electronic communications between two or more points possible.

For further explanation about these concepts the text below is provided for the members of the Working Group but not intended as part of the recommendation. If the Members agree it is proposed to include it as an annex to the Report as explanatory information for those readers of the same who may not be acquainted with these concepts.

ANNEX: The Network as a shared platform

The network is an interrelated web of hardware and software that utilize common standards to ensure each component is interchangeable with other's performing the same function. This concept – referred to as "interoperability"[3]– is important because it allows maximum flexibility in designing networks and related systems.

The grouping of standards that make communications interconnection in the network possible are known as the "Internet protocol (IP) stack." IP-based networks are designed to operate with maximum efficiency, and a continuous process of evolution of these standards responds to the need for greater performance, interoperability, resiliency, trust and security over time.

What we call the public Internet is a "network of networks," the large majority of them privately owned and managed by corporations, whether for the use of their employees or, in the case of Internet service providers (ISPs), for the public to connect to the rest of the Internet.

There are three types of entity that collectively make basic connectivity, and therefore the public Internet, possible:

- Internet Service Providers (ISPs): entities that provide connectivity for end-users (ranging from single mobile devices to the largest corporations), of which most countries have from several to dozens
- Backbone providers: entities that connect ISPs to one another, but that do not have end-users as customers; these entities are often responsible for making connections between countries and continents possible
- The processes and institutions that manage those processes by which unique identifiers are allocated, such as IP addressing and the domain name system (DNS). These are analogous to telephone numbers or postal addresses in that they allow any "node" of the network (of which your mobile phone is one, and your desktop PC or laptop is another) to be identified and reached from any other node, and ensure that worldwide every single address is used only once.

Each ISP or backbone provider must do two things aside from connecting to its customers:

- Connect to other ISPs so the exchange of data between their respective customers is possible, and connect to backbone providers (either directly or indirectly) to allow international traffic exchange. Without these agreements (often known as "peering" or "interconnection" agreements), the Internet would cease to be a global platform and exist solely as ISP-specific "islands" that would only allow users to connect to the other customers of their own ISP.

[3] For a user-friendly overview of the Internet and the "network of networks" that it is comprised of, the Internet Society's "An Introduction to Internet Interconnection Concepts and Actors" (Internet Society, 2012) is recommended (see www.Internetsociety.org/sites/default/files/bp-interconnection.pdf).

- Acquire the various types of technical addresses necessary for its equipment and that of its customers to use to connect to others, and implement the related services (like DNS servers) that allow every single device on the public Internet to have a unique address and to allow its customers to be found and to find all others.

The result of all this is that these networks (if left to themselves and the web of stakeholders who operate and maintain them) can:

- **Automatically find the optimal (which is not necessarily the most direct) *route* between any two points at any given time**.[4] An important fact to remember is that the route between any two points may traverse third countries, and that route may pass through *different* third countries at different times of the same day. This is especially common in border areas where two countries have dense populations near a shared border.
- Create a communications connection between any two points in a way that optimizes *performance* in the networks through which that communication passes. This can result in a route being taken that is *geographically* complex to ensure the communication "performs" better.
- **Ensure that anyone may extend the public Internet** simply by connecting a router[5] to the "edge" of the network and applying for a unique address for that router. Acquiring that address is often automatic, though public Internet addresses are ultimately assigned by regional Internet registries (RIRs)[6] to ensure every single device on the public Internet has a unique address.

The public Internet as a platform is inherently blind to geography in a way that the "offline" world is not. Goods trade, for example, would generally be biased against shipping via third countries to deliver a package sent from, and bound for, destinations in the same country to avoid the potential "friction" of border measures such as customs, tax compliance and other formalities.

How to treat the network as a platform

Looking at the network as a platform suggests several policy objectives:

[4] Throughout this annex illustrations refer to connections between two points ("point to point"), to make key points easy to follow. There certainly are communications where a single origin is connecting to multiple endpoints simultaneously and each of these endpoints may be in different countries from one another.

[5] A router is a device that "talks" to other such devices to figure out how to forward requests from any device connected to it to any other part of the network. The standards used ensure that this can happen automatically, and as the network topology changes in real time these changes are "learnt" by those devices that need to know about them. Pretty much every business and residence has a router, in the latter case generally provided by the Internet service provider.

[6] These organisations are responsible for managing the key forms of addressing on the Internet, which are akin to the various types of addresses in the worldwide postal system in the functions they perform. All of them are ultimately linked to the Internet Assigned Numbers Authority (IANA), managed by the Internet Corporation for Assigned Names and Numbers (ICANN). IANA and the RIRs work together (more information is available at http://www.iana.org/numbers).

- Avoid actions that impede or distort basic functions such as addressing and traffic routing. Where a country needs to prevent some communication from taking place, or prevent access to certain information that the network carries for whatever reason (such as to block child pornography), it must do so in a way that does not affect the operation of the network that carries those communications.
- Avoid actions that might impact upon "transit traffic." As we have seen, traffic often – for very good reasons – transits a country for which it is neither the destination nor the source. This argues strongly for such transit traffic to remain untouched and unhindered – after all, failing to respect transit traffic of others could lead to reciprocal lack of respect for your own.
- **Avoid national or international policies that distort private-sector choices about how equipment or services integral to the functioning of the network as a platform are made**. Measures of this type – often called "local hosting" obligations – can refer to elements of the network as a platform (like submarine cables, routers or related equipment), but they are most often intended to influence where applications, data and related services are hosted. Obligations that distort investment choices that would otherwise seek to optimize performance and resilience in the network everyone uses as a platform can be counterproductive: aside from anything else, the International community cannot connect the unconnected 4 billion-plus people as quickly if individual countries' choices make the network more expensive for everyone. An example from the offline world is roads: we want well maintained roads with enough lanes to handle peak traffic, and ideally to have multiple connections between locations so that when traffic congestion affects one road we have alternative routes to take.