UNITED NATIONS COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT

Working Group on Enhanced Cooperation

Contribution to the guiding questions agreed during first meeting of the WGEC

Submitted by

Mr. Nick Ashton-Hart

Response to the consultation of the working group for consideration at its second meeting

Submission of Nick Ashton-Hart, member from the technical community.

What are the high-level characteristics of enhanced cooperation?

I think this is one of the most difficult areas to gain consensus on and we should ask ourselves how much value addition our report can produce by trying to agree on a specific list of characteristics or principles. I think we should not try to do this, but instead to identify a selection of existing such documents. These would likely have many common elements which are generally agreeable and some which might be agreeable to some, but not others.

I think that would be a good compromise; it would illustrate where the gaps in agreement are and we can make clear that we don't all agree on all elements of all the principles in the listed documents, but we do agree that each of them embodies important perspectives.

This will allow us more time to spend on recommending areas for cooperation that could positively impact on the Internet everyone uses every day. Arguing about principles to find a common denominator is unlikely to have that kind of real-world impact. Wherever we can, we should prioritise spending time developing recommendations that will have a direct positive impact in the lives of others.

What kind of recommendations should the working group consider?

My view is that we cannot agree on what recommendations to develop before agreeing on some fundamentals. I suggest the following, and follow that with explanation and some ideas for specific areas we could explore.

1. We should agree that there are areas where the current level of enhanced cooperation as defined in Tunis have yet to deliver adequate results;
2. We should agree to focus on recommendations that relate to what is communicated, and avoid those related to the network as a

shared platform and resource that all communications rely upon – and further explicitly state that intra-national and international activities in relation to online communications should be least distortive or disruptive as possible to that shared platform. We should further identify some areas which impact this platform that all actors should avoid taking when pursuing public policy priorities related to content online;

3. We should identify areas where greater cooperation would be of general socioeconomic value, especially to developing and least-developed countries, and prioritize cooperation that is most likely to be effective in practical terms;
4. Within those areas we identify, we should further prioritize those which would have a direct positive impact on achievement of one or more of the SDGs.

Where more enhanced cooperation would deliver value

I think we all must accept that there are aspects of international Internet-related public policy where more action is needed and that governments have a role to play, just as Tunis states.

For example, it would be absurd to suggest that efforts to combat transboundary crime online are sufficiently effective at present. We ought to be able to say so.

We may differ about precisely how to deal with all aspects of crime online, but we ought to be able to agree on *some* venues and activities where greater cooperation is both needed and clearly within their mandate.

For instance, the two international organizations with a clear mandate to deal with transboundary crime are INTERPOL and the UN Office on Drugs and Crime (UNODC) – yet the latter has effectively no funding for activities related to crime online despite being the intergovernmental 'home' of the relevant international agreement with the largest number of states-parties, the Convention on Transboundary Organised Crime (three times as many as the Budapest Convention).

Nothing prevents member-states from providing more funding to UNODCs efforts – and our final report ought to call on them to do so. It is all very well to say – and it is clearly true – that enhanced cooperation is ongoing outside of the WSIS process, but member-states should go

further and ensure both adequate funding and a robust work programme at the venues they point to.

Other areas we could highlight are:

- The need to ensure the Human Rights Council and the Office of the High Commissioner for Human Rights can effectively advise on the development of cooperation in online crime interdiction, the evolution of the work of the UNGGE, the development of the Talinn Manual, and the like;
- How to take the principles of mutual legal assistance developed at UNODC and in other fora – like the Manila Principles – and operationalize them such that international human rights obligations are demonstrably respected *and* crime is more effectively and quickly prevented and criminals prosecuted;

Are there areas where member-states' national legal frameworks ought to be interoperable – not harmonized, but interoperable – to facilitate sustainable development and bridging of the digital divide? The answer is clearly yes. We should try and list a few areas, such as safe harbours for platforms, data protection laws (more than 100 countries don't have any data protection law at all), and consumer protection frameworks. We don't have to argue about what precise laws countries should have – this is a conversation states to have with their stakeholders and is a sovereign matter – but we could make clear that the Internet will work better for everyone if national legal frameworks in certain areas are interoperable with those of other countries.

The difference between the network and the data it carries

The working group should agree that the publicly-accessible Internet is two separate things *for the purposes of our work*:

1. The network that makes communications between any connected devices possible - the "network as a platform";
2. The data and associated services that use that network as a communications platform (or "data carried by the platform").

The data that the network carries are the applications and services that people use and the data that those applications and services create. The

network is the hardware, interconnections and essential communications between them.[1]

I propose that we agree that our outcomes should focus on measures related to the second.

Annexed to this document is a more complete elaboration on this concept and some thoughts for measures that we could recommend related to it.

[1] For the technically minded, the network as a platform corresponds to the lowest four layers of the OSI model and the lowest three of the TCP/IP (RFC 1122) model.

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"[2]– 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.

Keeping things simple, 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 which your mobile phone is one, and your desktop PC or laptop is another) of the network

[2] 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).

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.
- 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**.[3] 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

[3] Throughout this paper 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.

geographically complex to ensure the communication "performs" better.

- **Ensure that anyone may extend the public Internet** simply by connecting a router[4] 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)[5] 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; that our working group could usefully endorse:

- **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

[4] 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.

[5] 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).

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 should be avoided: aside from anything else, we 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 roads to be well maintained and 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.