IGF Internet Governance Forum

# Best Practice Forums: Handbook 2015

## CONTENTS

BPF summaries:

# INTRODUCTION

The Internet Governance Forum (IGF), which was called for in section 72 of the Tunis Agenda for the Information Society,[1] brings people together from various stakeholder groups as equals, in discussions on public policy issues relating to the Internet.

The tenth annual meeting of the IGF was held from the 10th to the 13th of November 2015 in João Pessoa, Brazil. More than 2,400 registered participants from over 116 countries attended the meeting, while thousands more actively participated online. These participants discussed, exchanged information and shared good practices with each other with the aim of facilitating a common understanding of how to maximise the Internet's opportunities and to address risks and challenges that have arisen and that may occur in the future.

Output-oriented debates and discussions during the four-day meeting addressed both opportunities and challenges under the sub-themes of cybersecurity and trust; the Internet economy; inclusiveness and diversity; openness; enhancing multistakeholder cooperation; Internet and human rights; critical internet resources; and emerging issues.

The meeting hosted more than 150 sessions throughout the week and also enabled the IGF's various community-driven intersessional activities to continue and promote the collaborative work they have been delivering throughout the year. One such intersessional activity, best practice forums (BPFs), also had the opportunity to present the findings of their community-driven work over the past year in order to gather broader stakeholder input on each of the six BPF topics concerned.

This handbook collates summarised versions of each BPF's output with the aim of providing the community with a snapshot guide on the important topics covered by these diverse BPFs.

*Acknowledgements:*

*The 2015 BPF outputs represent a truly bottom-up and collective effort from the global IGF community. A special thanks goes out to all contributors to the processes and those who made comments on the various drafts. The work would not have been possible without the leadership of the IGF MAG, including, but not limited to, Jānis Kārkliņš, Constance Bommelaer, Benedicto Fonseca, Lynn St-Amour, Avri Doria, Virat Bhatia, Carolyn Nguyen and Baher Esmat.*

[1] World Summit on the Information Society (WSIS) (18 November 2005). *Tunis Agenda for the Information Society* (WSIS-05/TUNIS/DOC/6(Rev. 1)-E). Available: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html. [Accessed 28 October 2015].

# THE IGF AND BPFs

BPFs offer unique platforms for multistakeholder communities to not only discuss topics relevant to the future of the Internet, but to also investigate, compare, collect and compile good practices, strategies and/or approaches on these topics. In the section below, the reasons for adopting BPFs to address certain topics and the characteristics of BPFs are briefly described.

## Why does the IGF have BPFs?

In 2012, the UN General Assembly (UNGA) Economic and Social Council (ECOSOC) Working Group on Improvements to the IGF published a report that called for the development of more tangible outputs to 'enhance the impact of the IGF on global Internet governance and policy'.[2] To enrich the potential for IGF outputs, the IGF's Multistakeholder Advisory Group (MAG) consequently developed an enhanced intersessional programme intended to complement other IGF activities, such as regional and national IGF initiatives, dynamic coalitions and BPFs.

## What are BPFs?

BPFs are working groups created by the IGF with the aim of facilitating dialogue and collecting emerging and existing practices to address specific issues or themes. By nature multistakeholder environments, BPFs and the IGF offer unique platforms to bring together diverse stakeholders – including civil society, the technical community, governments, intergovernmental organizations, academia, users and young people, for instance – to address pertinent topics in a holistic manner using these dedicated working groups.

BPFs also offer substantive ways for the IGF to produce more tangible and substantial outcomes. Like other intersessional activities, BPF outcomes are designed to become robust resources, to serve as inputs into other pertinent forums, and to evolve and grow over time. While BPF outcome documents have already been useful in informing policy debates, they are also iterative materials that acknowledge the need for flexibility in light of the pace of technological change faced by Internet policymakers.

[2] See page 4, UNGA ECOSOC (16 March 2012). *Report of the Working Group on Improvements to the Internet Governance Forum* (A/67/65-E/2012/48). Available: http://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf. [Accessed 28 October 2015].

## How do BPFs work?

BPFs have the freedom to define and delineate the parameters of their work in consultation with their respective multistakeholder communities; to define their own methodologies; and to tailor their work to the requirements of their theme's specific needs and requirements.

As is clear from the summaries contained in this book, the methodologies adopted by BPFs differ greatly and are highly dependent on the theme(s) and participants involved in each BPF's work. In general terms, however, all BPFs use open and transparent working approaches with the aim of encouraging and gathering broad stakeholder input. The outcomes of each BPF are intended to be community-driven, bottom-up and a true reflection of the multistakeholder nature of the IGF's intersessional activities.

## When and where do BPFs do their work?

BPFs do much of their work in the year between annual IGF meetings using primarily online and virtual platforms that are accessible to stakeholders from all over the world. While some BPFs do their work for approximately one term – or the year between annual IGF meetings – other BPFs have been operational for two consecutive years.

Each BPF has a unique platform on the IGF's website that it updates with relevant information, a dedicated mailing list on which it can communicate to and with participants, and most BPFs hold regular virtual meetings that anyone is welcome to attend. In addition, BPFs may choose to use the opportunity of multistakeholder advisory group (MAG) meetings (in 2015, these meetings were held in Geneva and Paris) to hold face-to-face meetings to further its work, although online participation at each such meeting is always facilitated and encouraged. Each BPF also has a 90-minute session at the annual IGF meeting at which it has the opportunity to present its preliminary findings and to further dialogue and debate about the topic(s) concerned.

## Want to learn more about the IGF and BPFs?

Read more about the IGF and BPFs on the IGF's website, which has a dedicated page for each BPF, hosts the video material from each BPF's session(s) at annual IGF meetings, and also offers a wealth of other information about the IGF's work: http://www.intgovforum.org/cms/.

## INTRODUCING THE 2015 BPFs

Six topics formed the focus of the 2015 BPFs, namely:

1. **Fostering enabling environments to establish successful IXPs;**
2. **Creating an enabling environment for IPv6 adoption;**
3. **Online abuse and gender-based violence against women;**
4. **Strengthening multistakeholder mechanisms;**
5. **Establishing and supporting CSIRTs for Internet security; and**
6. **The regulation and mitigation of unsolicited communications.**

Of these topics, the first three were new topics in 2015 whilst the last three in the list were continued from the previous term (or year) and were therefore in their second year of operation.

## HOW TO USE THIS HANDBOOK

In the sections below, the outcomes of each of these topics or themes are briefly summarised in the order of the list above.

For each BPF, the coordinator(s), lead experts (if applicable) and rapporteurs are listed and an approximate number of participants is listed. Where possible and for the purposes of illustration and practical application, BPF rapporteurs highlighted case studies, comments from participants and examples from their full reports for use in this handbook. Because each BPF adopted a different methodology, however, the content of each BPF's summary is also different.

To read the BPFs' full reports, visit the IGF website:

http://www.intgovforum.org/cms/best-practice-forums/2015-bpf-outs

## LIST OF ACRONYMS

| | |
|---|---|
| BPF | best practice forum |
| CEDAW | Committee on the Elimination of Discrimination against Women |
| CGN | carrier grade network address translation |
| CERT | computer emergency response team |
| CSIRT | computer security incident response team |
| DoS | denial of service |
| DDoS | distributed denial of service |
| ECOSOC | Economic and Social Council |
| ICT | information and communication technology |
| IETF | Internet Engineering Task Force |
| IGF | Internet Governance Forum |
| ITU | International Telecommunications Union |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| ISOC | Internet Society |
| ISP | Internet service provider |
| IXP | Internet exchange point |
| IXPA | Internet exchange point associations |
| LAP | London Action Plan |
| LBT | lesbian, bisexual and transgender |
| LEA | law enforcement agencies |
| MAG | multistakeholder advisory group |
| M$^3$AAWG | Messaging, Malware, Mobile Anti-Abuse Working Group |
| NAT | network address translation |
| NGO | non-governmental organization |
| OEC | Organisation for Economic Co-operation and Development |
| RIR | regional Internet registries |
| UN | United Nations |
| UNGA | United Nations General Assembly |
| WSIS | World Summit on the Information Society |

## FOSTERING ENABLING ENVIRONMENTS TO ESTABLISH SUCCESSFUL IXPs

**Coordinators: Gaël Hernández, Jane Coffin, Malcolm Hutty**

**Rapporteur: Wim Degezelle**

**Period of activity: one term (2015)**
**Approximate number of contributors: 100**
**It was possible to contribute to this BPF during virtual meetings (10+), on the mailing list, to the BPF survey, via the public review platform and during the BPF session at the IGF 2015 meeting.**

**Read the BPF's full report:** http://www.intgovforum.org/cms/documents/best-practice-forums/creating-an-enabling-environment-for-the-development-of-local-content/582-igf-2015-bpf-ixps

## INTRODUCTION

The BPF on Enabling Environments to Establish Successful Internet Exchange Points (IXPs) brought together experts and stakeholders in an open and collaborative process to develop a useful and tangible best practices outcome document. Stakeholder input was collected via discussions on an open mailing list, regular virtual meetings, public input via the IGF review platform and during the in-person session at the IGF 2015 meeting in João Pessoa, Brazil.

The best practice document explains why IXPs matter and focuses on ways to create enabling environments that allow IXPs to develop and flourish. The information and examples provided are meant to serve as the foundation of a flexible framework – useful regardless of the country or continent – for creating an environment that fosters IXP success and development. This summary is an abbreviated version of the BPF outcome document that was published at the end of November 2015.

Note that the BPF is not about the technical details of how to establish, operate and sustain an IXP. Those seeking technical guidance and technical best practices are advised to visit specialist meetings and forums and to consult technical manuals and check lists. A non-exhaustive list of technical forums and reference documents can be found at the end of this document and in the appendices of the BPF outcome document.

## BACKGROUND

### What are IXPs?

The Internet is a large network of networks, a global communication network composed of thousands of individual networks. To effectively be part of the Internet, each network needs to be able to send and receive traffic to and from any other network. IXPs are physical locations where Internet networks are connected at a common point to exchange data. Different networks can interoperate because they all speak the same language: the Internet Protocol (IP).

The practice of exchanging data between networks at an IXP is called peering. Peering is largely based on voluntary agreements by both networks as a result of acknowledging the value of being directly connected: IP packets are routed directly using the shortest and cheapest path between both networks. By exchanging traffic at an IXP, Internet service providers (ISPs) do not have to build out their networks to all their "peers," which cuts costs, frees up money, labour, and resources, and allows for a more competitive market environment. Peering is in a majority of the IXPs a cost-neutral transaction.

The IXP model of network interconnection and traffic exchange is a widely-adopted industry practice with over 500 known IXPs in 120 countries. The location and distribution of IXPs in the world can be explained by looking at factors such as country demographics, market conditions, and global economics.

Table 1: The number of IXPs by region[3]

| Region | Number of IXPs | Number of countries | Number of cities |
|---|---|---|---|
| Africa | 37 | 28 | 31 |
| Asia | 99 | 25 | 49 |
| Europe and the Middle East | 214 | 49 | 142 |
| Latin America and the Caribbean | 60 | 16 | 49 |
| North America | 102 | 2 | 57 |

## What are the benefits of having an IXP?

- Using cost-neutral transactions for the exchange of traffic between networks at an IXP reduces the network's operational cost. This means that it becomes cheaper for the network to be part of the Internet and to provide services to its clients.

[3] Packet Clearing House (n.d). *IXP Directory, Euro-IX*. Available: https://www.euro-ix.net/ixps/list-ixps/. [Accessed September 2015].

- The direct interconnection of networks at an IXP allows the networks to keep local traffic local and to deliver the traffic destined for each other with the lowest possible latency (latency is the time elapsed between the transmission of IP packets from the originator and reception of those IP packets at the receiver).

- Using IXPs gives networks more autonomy and control over the network's own resources, including routing and traffic management, because it decreases a network's dependency on third-party networks.

- Increasing the number of direct paths and routes furthermore between networks increases the stability and robustness of the Internet in the case of network outages, denial of service (DoS) attacks, and other related circumstances.

- Evidence suggests that IXPs can enable competition by facilitating the entry of new service providers and content delivery networks (CDNs) in a cost-effective way. For instance, new entrants do not have to build out their networks to all the other networks that are exchanging traffic at the IXP. Additionally, an IXP generally provides a neutral traffic exchange point whereas bilateral interconnection can be expensive and include other barriers to entry.

> *Slowly, due to the presence of the IXP, certain operators started new projects to host local content and developed a new business.*
>
> African IXP comment in response to BPF survey

## Main stakeholders of an IXP

The different stakeholders that participate in the IXP ecosystem can be grouped according to their role, interest, and involvement in the establishment and operation of an IXP. The role stakeholders play does not necessarily depend on their belonging to one of the traditional Internet governance stakeholder groups (governments, civil society, the private sector, and academia), but rather on the function they fulfil at the IXP or in its environment. A particular stakeholder can also play multiple roles. The main roles involved in the creation and operation of an IXP can be classified as:

- IXP members/ participants
    - network operators
    - providers of other services
- IXP operator
- regulator/ ministry/ other government body
- community/ facilitators
- building/ facilities operator

The main stakeholders and their respective roles are further described in the BPF outcome document.

## CREATING AN ENVIRONMENT TO ESTABLISH SUCCESSFUL IXPs

### Bringing together the peers, setting up the IXP, and forming a community

The first step in establishing an IXP is to bring potential peers around a table to take the decision to start the IXP. There needs to be a minimum number of network operators interested and willing to interconnect their networks before it makes sense to invest in equipment and facilities for the purpose of setting up an IXP. It is generally assumed that the presence of five networks – less in case of small islands – can justify the establishment of an IXP.

There are several ways IXPs can operate, and IXP models vary across regional markets. Most European IXPs grew from non-commercial ventures between network operators, while most IXPs in Africa were established by ISP associations and universities. Commercial IXPs, in turn, are more typically found in the USA and parts of Asia. Each IXP model carries with it certain advantages, and some IXP approaches are better than others depending on the economic and policy conditions in the region.

Finding peers and agreeing on how to run the IXP are the first steps in launching the IXP. Meanwhile, the process of building a community around the IXP occurs in parallel. IXP community support is almost indispensable for establishing an IXP, and is essential if one wants the IXP to become a success. "Setting up an IXP is 80% human and 20% technical" is a common expression. Developing this supportive community in which the IXP's members and other stakeholders are involved is one of the most important tasks of the IXP operator – apart from the purely technical aspects of running the IXP. Building an IXP community is work and time intensive.

*The main reason [to establish the IXP] was the high cost of transit. To lower the*

> *costs, we started to interconnect multiple entities (i.e., bandwidth users) and buy transit [in] bulk (price per Mb [megabit] goes down when the number of Mb goes up). It became obvious that we had a local IXP. The next step was to gather more people to build a community and help grow the local IT [information technology] economy.*
>
> European IXP, BPF survey
>
> ”

Most IXPs have mailing lists and organize networking events, member and stakeholder meetings. IXP events and mailing list discussions tend to cover a variety of topics, not strictly limited to technical or organizational issues related to the IXP and, as such, often become local discussion forums on Internet-related issues.

Capacity-building, getting the technical expertise, and learning to run and manage the organization are major challenges for a starting IXP. IXP associations (IXPAs) play an important role as platforms for knowledge and best practice exchange within the IXP community; also supporting their members in addressing the challenges they face. The IXPAs are knowledge centres and can be a first point of contact for governments that look for advice on IXP development. The IXPAs[4] are AFIX, APIX, Euro-IX, LAC-IX. They formed the Internet Exchange Point Federation (IX-F)[5] to build a global IXP community and help the development of IXPs throughout the world.

### A supportive government and an enabling (regulatory) environment

Governments can play a motivating role as supporters, co-initiators, or sponsors of IXP projects. They have responsibilities for the development of the country's infrastructure and can intervene to avoid market distortion (for example, on the wholesale market for international connection). Governments can also support IXP development as part of their strategy to create a more competitive local market of Internet services.

In some countries, the existing regulatory regime and policies may hinder the growth of the IXP. For instance, policies that inhibit competition on broadband terrestrial infrastructure may limit the options available for local interconnection. Raising awareness and providing clear information to governments on the role and benefits of an IXP is an important step to address resistance or lack of interest. Successful projects spearheaded or initiated by governments or regulators include the Argentina-

[4] See the Reading List at the end of this summary for the websites of these IXPAs.

[5] See: http://www.ix-f.net/.

Conectada project, the Bolivian IXP, the IXP in Lesotho and UAE-IX (Dubai).

Decision-makers, however, should be very cautious if they plan to operate the IXP, regulate the IXP, or enact laws about IXPs or the interconnection at IXPs. Not all government involvement will accelerate the development of IXPs and some decisions – even when taken in good faith – may have a counterproductive effect.[6] Should the legal regime still require a "measure" to be taken to allow for the IXP, this measure should be kept as flexible as possible.[7]

## High cost of domestic and international connectivity

Joining an IXP will be attractive if the cost of exchanging traffic locally is cheaper than purchasing international bandwidth (IP transit) from an upstream provider for routing traffic overseas and back. Otherwise there is no incentive for network providers to connect to the IXP.

For example, prior to an IXP being established in Quito, Ecuador, the cost of international transit was USD 100 per megabits per second (Mbps) per month. After the IXP was established, the cost of exchanging traffic at the IXP was USD 1.00 per Mbps per month.[8] Furthermore, high prices for domestic connectivity and a poor availability of flexible cost-effective services like Ethernet, can limit the development – and therefore the benefits – of the IXP.[9]

The high investment required to build the infrastructure (networks, cross-border connections, etc.) and exchange traffic (transit through other countries, access to and capacity rights on submarine cables, etc.) are entry barriers and may increase the market power of the incumbent operators and give monopoly rights to operators of international infrastructure. Such market power can lead to above-cost prices for international connectivity. For example, after Kenya agreed to liberalise its undersea cable market, the cost of international connectivity started to drop, and more investors became interested in Kenya.[10]

[6] Dawit Bekele (November 2014). *The role of Governments in Creating an enabling environment for establishing and developing IXPs*. Available: http://www.itu.int/en/ITU-D/Regional Presence/ArabStates/Documents/events/2014/IXP/Presentations/Panel%201_ISOC_Role%20of%20governments.pdf [Accessed October 2015].

[7] Sofie Maddens (November 2014). *National Legal Frameworks for the Establishment of IXPs*. Available: http://www.itu.int/en/ITU-D/RegionalPresence/ArabStates/Documents/events/2014/IXP/Presentations/Panel%202_ISOC_Tunisia%20presentation%20Sofie%20Maddens%20November%202014.pdf [Accessed October 2015].

[8] Hernan Galperin (November 2013). *Connectivity In Latin America and the Caribbean: The Role of Internet Exchange Points*. Available: http://www.internetsociety.org/doc/connectivity-lac-ixp-study [Accessed October 2015].

[9] R. Schuman and M. Kende (May 2013). *Lifting barriers to internet development in Africa: Suggestions for improving connectivity*. Available: http://www.internetsociety.org/doc/lifting-barriers-internet-development-africa-suggestions-improving-connectivity [Accessed October 2015].

[10] *Ibid.*

Landlocked countries, sealocked countries and small islands are faced with specific challenges and often depend on expensive satellite technology to bring bandwidth to the country.

## Location, equipment, and technical capacity

Modern IXPs can cost very little to set up and run. Establishment and operational budget estimates range from 5,000 to 8,000 USD or less[11] (low-end) to a maximum of 50,000 USD.[12] Finding an adequate location that is both neutral and low-cost to host the equipment is very important. When considering possible locations, the following elements need to be taken into account: space, environmental control, security, reliable and redundant power, access to terrestrial infrastructure, cabling, and support. In addition to these practical and technical considerations, all members of the IXP must perceive the location as neutral and trust that no member of the IXP will benefit more than another.

In many cases, and in particular for the non-commercial IXPs, the founders compiled the initial resources and equipment, and then developed mechanisms for the funding of the IXP. Other IXPs received funds or equipment from the local ISPA; could count on the support of a university network; received donations in the form of money, equipment, or technical expertise from organizations such as the Internet Society (ISOC), Packet Clearing House (PCH), Network Startup Resource Center (NSRC); or were sponsored by private companies. Development agencies and institutional donors such as the World Bank, the African Union, and the Latin American Development Bank also have track records of supporting initiatives to create IXPs.

Starting IXPs can count on external expertise to set up and install the equipment but have to develop the technical knowhow to run the IXP. Technical capacity-building is needed at the IXP's operational level and on the side of the IXP member/ network operator. Finding and training the technical staff is a challenge for new IXPs.

> *We had no real technical clue how to run an IXP – this took time to develop.*
>
> European IXP, BPF survey

[11] Some argue that starting up an IXP should not exceed 3000 USD; even less with donated equipment. These calculations, however, do not include, for example, the travel cost of experts brought in to give the needed training, which, in developing countries, easily mounts up to 3000 USD.

[12] Comment on BPF mailing list exchange.

The Internet community has a tradition of sharing first-hand experiences, teaching, and helping each other by sharing practices and solutions. Organizations such as ISOC, PCH, and the NSRC, along with most of the regional Internet registries (RIRs), provide crucial support and training to IXPs; especially those in the planning and developing stages or newly established ones. Meetings of network operator groups (NOGs) and of the RIRs often have special IXP workshops where experts from the IXP community give presentations. The IXPAs are another resource that provides information, training, networking, and business opportunities. An overview of related organizations and venues can be found at the end of this document and in the appendices of the BPF outcome document.

## INDICATORS OF A SUCCESSFUL IXP

There is not one indicator to measure the success of an IXP and too easily one is tempted to only take into account the volume of traffic that passes through the IXP. The assessment of an IXP needs to take into account a whole list of diverse indicators; of which traffic volume is only one metric. To obtain the whole picture, factors such as local transport costs, building space, power, port speeds and peering policies need to be included and it is important to consider to which extent the IXP is successful in generating sufficient funding to operate and grow. The assessment will be incomplete if it ignores the IXP’s community-building role.

## CASE STUDIES

The BPF outcome document contains four case studies that are particularly worth reading:

Case study 1 explains how, due to the lack of locally-stored content, the Kinshasa Internet Exchange point (KINIX) grew slowly and struggled to attract new operators to connect to the IXP. KINIX took initiatives to deploy added services at the IXP, to conclude partnerships with content providers to host a local cache, to promote local hosting and the creation of local data centres, to encourage the government to handle administrative matters over the Internet (e.g. online tax service), and was involved in the re-delegation of the .cd domain name servers. KINIX's actions had a positive impact on the development of the IXP.

**Case study 2** describes the successful development of NAP.EC in Ecuador and explains how different actors benefited from the existence of the IXP. The installation of local caches by content providers, for example, led to a significant increase in traffic and a dramatic decrease of latency experienced while accessing local content.

**Case study 3** tells the story of Costa Rica's first IXP (CRIX) and demonstrates how important the good cooperation between ISPs and government institutions was for the creation of CRIX in 2014. The IXP is based on cooperation, with no regulation involved, and keeps growing stronger due to the active participation of new members and of all the involved parties.

**Case study 4** shows how a national ccTLD manager can be a neutral and trusted player in the process to promote and establish local IXPs. The Canadian Internet Registration Authority (CIRA), the manager of the .ca ccTLD, encouraged and assisted communities to form local groups to develop their IXP. In just over two years' time, five new IXPs have been established in Canada.

## KEY POLICY MESSAGES

The BPF discussed and formulated some key policy messages:

### *IXPs do not provide international transit connectivity directly*

IXPs provide the infrastructure and support for networks to interconnect at a common place. While IXPs can be a good location to distribute international transit connectivity, IXPs do not typically offer this service themselves. Doing so could put an IXP in competition with its members, and might also have licensing implications.

### *The need for an IXP is driven by market conditions*

IXPs typically emerge in response to unsatisfied demand for network interconnection, often due to the high cost of alternatives (e.g. transit). A top-down approach to multiply the number of IXPs in a geographic region will not necessarily multiply the benefits, and may even be counter-productive. Having too many exchanges can fragment the market and increase the overhead cost for networks to peer.

### *IXPs need time to mature*

Establishing an IXP is only the first step. It can take significant additional time to promote the IXP, attract additional network operators, and build a community. It is important to manage expectations about the time it takes for IXPs to be successful.

### *Neutrality is vital*

IXPs typically function best when both their ownership and governance system are neutral and do not directly or indirectly favour one or more exchange participants. Neutral access policies are also important for facilities that host IXPs.

### *IXPs are only one piece of the puzzle*

Effective approaches to cross-border infrastructure, data centres, content, and licensing are also important components of any national broadband strategy.

### *Traffic is not an accurate measurement of success*

Measuring the success of an IXP by pure traffic numbers is very much region-focused and not representative for many other indicators (i.e. local transport costs, building space/ power, port speeds, peering policies, etc.). Other indicators of the success of an IXP are, for example, sufficient funding to operate the IXP (and grow in the future) and frequent social events between participants.

### *Licensing-related issues must be resolved*

IXPs should work with local governments to understand local licensing requirements. While many countries do not require a license, some do require authorisation.

## CONCLUSION AND NEXT STEPS

How can we accelerate and speed up connecting the next and last billion Internet users and provide solutions for the development that the Internet enables by using the good practices and experiences collected in this document?

Building connectivity (infrastructure); building communities (people and stakeholders); capacity development (training, face-to-face and online); and the policies that enable them (bottom-up governance and local and international governmental and environmental factors) are the ingredients of a formula that has proven to work. This formula works through partnerships: people that work together and build human trust networks for targeted sustainable development. We have an opportunity to strengthen, amplify and accelerate this formula to connect the next billion and final billions.

The BPF collected and described a range of good practices in its outcome document from which novel and developing IXPs can select useful practices depending on their local situation and needs. The practices in this document are not static but can be improved and completed based on new experiences as more IXPs deploy around the world.

More work can be done on IXPs moving forward by focusing on some of the key issues that have been raised during the BPF, for example the special situation of landlocked countries relying mostly on satellite connectivity; problems that established IXPs encounter; and the question when and how a community could reboot or revive a dormant IXP.

## FURTHER READING:

### Public and reusable data on IXPs

Packet Clearing House Report on IXP locations:
https://prefix.pch.net/applications/ixpdir/summary/
EURO-IX list of IXPs: https://www.euro-ix.net/ixps/list-ixps/
EURO-IX IXP map: https://www.euro-ix.net/ixps/ixp-map/

### Non-exhaustive list of community-organized IXP training

*Network operator group (NOGs) meetings are key places to obtain technical training, connect with experts, and build a community and human networks of trust:*

African Network Operator Group (AFNOG): https://afnog.org/.
Asia-Pacific Regional Internet Conference on Operational Technologies (APRICOT): https://2014.apricot.net/.
Caribbean Network Operator Group (CaribNOG): http://www.caribnog.org/.
Eurasia Network Operator Group (ENOG): http://www.enog.org/.
Latin-American Network Operator Group (LACNOG): http://www.lacnog.net/.
Middle East Network Operator Group (MENOG): http://www.menog.org/.
North American Network Operator Group (NANOG): http://www.nanog.org/.
South Asian Network Operator Group (SANOG): http://www.sanog.org/.

*RIRs offer key training sessions at their meetings, and work with ISOC and others to conduct trainings around the world:*

AfriNIC: http://www.afrinic.net/
AfriNIC mailing lists: http://www.afrinic.net/en/community/email-a-mailing-lists

ARIN: https://www.arin.net/
ARIN mailing lists: https://www.arin.net/participate/mailing_lists/

APNIC: https://www.apnic.net/
APNIC mailing lists: http://www.apnic.net/community/participate/join-discussions

LACNIC: http://www.lacnic.net/en/web/lacnic/inicio
LACNIC mailing lists: http://www.lacnic.net/en/web/lacnic/lista-de-discusion

RIPE: http://www.ripe.net/
RIPE mailing lists: http://www.ripe.net/ripe/mail

*IXPAs provide training, networking, and business opportunities:*

Asia-Pacific Internet Exchange Association (APIX): http://apix.asia/
African Internet Exchange Association (AFIX): http://www.af-ix.net/
European Internet Exchange Association (Euro-IX): https://www.euro-ix.net/

Latin American and Caribbean Internet Exchange Association (LAC-IX): http://lac-ix.org/index/

## Non-exhaustive list of technical forums and reference documents

IXP construction checklists
https://wiki.pch.net/pch:public:ixp-construction-checklist
https://wiki.pch.net/pch:public:basic-ixp-guide
https://www.euro-ix.net/ixps/set-up-ixp/ixp-models/
https://www.euro-ix.net/ixps/set-up-ixp/ixp-infrastructure/

IXP toolkit (ISOC)
http://www.ixptoolkit.org
http://www.internetsociety.org/internet-exchange-points-ixps-0

IXP best current operational practices (Euro-IX)
https://www.euro-ix.net/ixps/set-up-ixp/ixp-bcops/

Open-IX: OIX1 IXP standards and certification
http://www.open-ix.org/standards/ixp-technical-requirements/

More resources can be found in the appendices of the BPF's outcome document.

# CREATING AN ENABLING ENVIRONMENT FOR IPv6 ADOPTION

**Coordinators: Susan Chalmers, Izumi Okutani**
**Rapporteur: Wim Degezelle**

**Period of activity: one term (2015)**
**Approximate number of contributors: 100**
**It was possible to contribute to this BPF during virtual meetings (10+), on the mailing list, to the BPF survey, via the public review platform and during the BPF session at the IGF 2015 meeting.**

**Read the BPF's full report:** www.intgovforum.org/cms/documents/best-practice-forums/creating-an-enabling-environment-for-the-development-of-local-content/581-igf2015-bpfipv6-finalpdf

## INTRODUCTION

The BPF on Creating an Enabling Environment for IPv6 Adoption explored, on a global, open, participatory, and multistakeholder basis, different "best practices" that have been used in relation to increasing Internet Protocol version 6 (IPv6) adoption.

The BPF outcome document is the result of an iterative discussion process conducted on the BPF's open mailing list, over several virtual meetings, comments provided by the community at large on the IGF public review platform, and discussions during the BPF session on IPv6 at the IGF 2015 meeting in João Pessoa, Brazil. Best practice examples were collected by means of a public survey, through email correspondence, and public mailing list discussions.

The best practice document intends to assist others in their efforts to support IPv6 adoption in their locality, region, industry, or network.

## BACKGROUND

Generally speaking, devices connect to the Internet via numerical Internet Protocol (IP) addresses. The first pool of IP address numbers was created in the 1970s and contained approximately four billion unique numbers. This is the Internet's legacy addressing system - Internet Protocol version 4 (IPv4). The growth and expansion of the Internet has virtually exhausted the IPv4 address pool.

A new addressing system, IPv6, was developed in 1995 to deal with IPv4 exhaustion.

IPv6 addresses are longer in length: An IPv6 address is represented by eight (8) groups of hexadecimal values, separated by colons (:). The IPv6 address size is 128 bits, opposed to 32 bits in an IPv4 address. A bit is a digit in the binary numeral system and the basic unit for storing information.

The preferred IPv6 address representation is: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x is a hexadecimal digit representing four (4) bits. "X" ranges from "0-9" or from "a-f."

The IPv6 space is huge in comparison to the IPv4 pool. The adoption of IPv6 went very slow during the past decade. Today the global uptake of IPv6 compared to IPv4 is still relatively low and the availability of IPv4 addresses is now severely limited.

## Why adopt IPv6?

The Internet's sustainable growth depends on IPv6 adoption; the booming mobile market and the Internet of Things (IoT), alone, will require much more IP address space than is available with IPv4.

Anyone running the old protocol needs to adopt the new one in order to support the increasing demand on the global network as more people – and more machines and "things" – come online. IPv4 and IPv6 are two different protocols. IPv6 is not backwards compatible with IPv4. Devices that communicate using only IPv6 cannot communicate with devices that communicate using only IPv4.

Technologies – for example Network Address Translation (NAT) and Carrier Grade Network Address Translation (CGN) – have been developed to extend the life of IPv4. Unused IPv4 address blocks are being traded on so-called secondary or after markets. These efforts should be considered only as temporary solutions and come with their own costs and downsides. They are sometimes relied upon to forestall what should be considered as ultimately inevitable for a business, a government, or end users: IPv6 adoption.

Until recently, there has been little immediate benefit in deploying IPv6 and, in competitive terms, there was no "early adopter" advantage. However, now that more Internet users are connecting via IPv6,[13] the immediate benefits of deploying the new protocol are gaining visibility, for example:

- Content providers and publishers can see a direct performance benefit if traffic is delivered directly to the end user over IPv6 and no longer has to flow through

[13] Google measurements, for example, indicate that 25% of the end users in the USA now use IPv6 and that globally, nearly 8% of Google's traffic is delivered via IPv6.

NAT or CGN devices.

- Network operators will save on the operating and maintenance cost of NAT and CGN infrastructure.
- End users with IPv6-enabled devices can access content from IPv6-ready content providers with improved performance (provided that their ISP offers IPv6 services).

> *Facebook says it has seen users' Newsfeeds loading 20 percent to 40 percent faster on mobile devices using IPv6. Tests at Time Warner Cable show a 15 percent boost.*
>
> Dan York, Internet Society[14]
>
> ”

## HURDLES TO IPv6 ADOPTION

The cost associated with the transition from IPv4 to IPv6 is one of the hurdles to adoption. IPv6 needs to be deployed throughout the network by all players and this requires reconfiguring networks, providing training, and upgrading or purchasing new equipment. Hurdles to IPv6 adoption should be taken into consideration when developing IPv6-related policies or planning to deploy IPv6.

A number of specific hurdles have been identified by the BPF:

- Deploying IPv6 in a network requires solid planning, as usually networks need to keep operating while undergoing upgrades.
- Retailers (ISPs) that depend on access wholesalers that only support IPv4-based services are unable to provide IPv6 to their end customers.
- Lack of perceived demand and return on investment are a hurdle for hardware and software vendors to prioritise IPv6 development.
- Websites and applications may require updating in order to support IPv6.
- Engineering, operations, and customer support staff will need to be trained on IPv6.

[14] Dan York, Internet Society's (ISOC) Deploy360 Blog, *Facebook News Feeds Load 20-40% Faster Over IPv6* (April 2015). Available: http://www.internetsociety.org/deploy360/blog/2015/04/facebook-news-feeds-load-20-40-faster-over-ipv6/. [Accessed September 2015].

*Removing [hard-coded assumptions about IP addresses from older websites and systems] and preventing any new systems from making the same mistake is a key best practice.*

Ross Chandler; contribution on the IGF review platform

”

## CREATING ENABLING ENVIRONMENTS FOR IPv6 ADOPTION

The contents of the BPF's outcome document are based upon best practice examples from all continents collected by means of a public survey, which launched in mid-July 2015 and closed the following November[15] and were completed with expert insight. The BPF also drew from the discussions that unfolded on the open mailing list and during the BPF's virtual meetings. The comments received on the drafts published on the IGF website and during the face-to-face session at the IGF 2015 meeting in João Pessoa, Brazil, have been another source of input.

Readers need to be well aware that the different examples are situated in their own contexts and that success in terms of growth of IPv6 use in a certain region or environment will almost always be the result of a combination of initiatives, practices and other factors.

### IPv6 task forces, a platform for best practices

IPv6 task forces work to promote IPv6 deployment in their country or region. They are organized at national, regional, and global levels and are useful meeting places for different stakeholders to meet and collaborate on IPv6 adoption. As such, the IPv6 task force is not only a best practice in itself, but as well a platform where other initiatives and best practices are created.

Task forces can be organized ad hoc, by the community, or supported by government. They conduct various activities and serve various purposes, from raising awareness about IPv6, to providing advice on how to deploy it and conducting outreach, to developing fully-informed policy recommendations to the government that should result in their country seeing higher IPv6 use.

Examples of active IPv6 task forces[16] can be found in Australia, Belgium, Canada,

[15] The compilation of survey submissions is available in the Appendices section of the BPF's full report.
[16] See the Further Reading list at the end of this summary for the websites of these IPv6 task forces.

Chad, Colombia, Indonesia, Mexico, Spain, Switzerland, Thailand, The Netherlands, or the United Kingdom. Larger countries can have region- or state-specific task forces such as the Rocky Mountain or Texas IPv6 Task Force in the USA.

National IPv6 task forces often collaborate on a regional basis. Regional meetings enable participants to exchange information with members of other task forces who, while from different countries, may operate in similar cultural, economic, and regulatory environments.

Examples of regional task forces[17] are APIPv6TF (Asia-Pacific), LAC IPv6 TF (Latin America and the Caribbean) or the North America IPv6 Task Force (Canada, US, Mexico).

Common challenges cited by task force leaders include funding, coordination and lack of participation by key stakeholders, and in particular the local industry. Those involved continue to seek ways to alleviate these challenges. Raising awareness should help.

## Capacity-building

> *[IPv6 training is] a key area if the rate of IPv6 deployment is to be accelerated. Not only is the training of engineers important, but [also] the training [and] awareness of upcoming engineers is important.*
>
> Kasek Galgal, contribution on the IGF review platform
>
> ”

Capacity-building on IPv6, both in terms of technical training for engineers and operators, and raising awareness for non-technical policymakers, law enforcement, and business decision-makers, is fundamental to creating an enabling environment for IPv6 adoption. Many different organizations, for profit and not-for-profit, provide IPv6 training, including the Regional Internet Registries (AFRINIC,[18] APNIC,[19] ARIN,[20] LACNIC[21] and RIPE NCC[22]) and national research and education networks.

Having conducted IPv6 trainings since 2010,[23] AFRINIC offered a number of insights in its

[17] *Ibid.*

[18] See: http://afrinic.net/.

[19] See: https://www.apnic.net/.

[20] See: https://www.arin.net/.

[21] See: http://www.lacnic.net/web/lacnic/ipv6.

[22] See: https://www.ripe.net/.

[23] For more information on AFRINIC's training programmes, visit: http://learn.afrinic.net/en/.

survey response, suggesting that others interested in organizing their own IPv6 capacity-building workshops consider the following:

- an effective IPv6 foundations training session requires at least two full days;
- participants must be pre-screened for requisite knowledge before attending;
- content must be 50:50 theory/ practice; and
- rigorous feedback must be required and used to update the content.

Over the course of her work as RIPE NCC IPv6 programme manager, Nathalie Künneke-Trenaman has seen how many people who are new to IPv6 approach the idea of deployment. She offered the following advice:

> *"One of the big problems with IPv6 deployment is that people think they have to do everything at once and that too much new knowledge is needed. It is of vital importance to break a deployment into smaller tasks and evaluate them step-by-step."*

In addition to the trainings for network operators, there are a number of commercial providers of IPv6 trainings that mainly gather to do business. Offerings normally include general technology training on IPv6 and vendor-specific training on how to configure IPv6 on specific equipment.

While most of the capacity-building focuses on network operators, IPv6 training for law enforcement officials, policymakers, and corporate-level (C-level) business decision-makers (e.g., CEOs, COOs, CFOs, etc.) is also very important for creating an enabling environment for IPv6 adoption.

> *It should be more than just "understand the importance of IPv6 deployment". In consulting with decision-makers, I try to make them understand that, actually, they have no choice; IPv6 is the current Internet Protocol, while IPv4 is the legacy protocol. So, investing in IPv4 means investing in a end-of-life technology while investing IPv6 is investing in current technology. Their choice is actually in how they want to deploy it – carefully, with time, laying a clean foundation for their future network, or quick and dirty, creating extensive unnecessary operational cost in the future or even having to redesign at some point.*
>
> Silvia Hagen, Swiss IPv6 Council, comment on IGF review platform

”

A few recommendations from BPF contributors for business decision-makers in building capacity included the following:

- build confidence at the decision-making level that IPv6 is "proven technology" and (perceived) risks are manageable;
- work with decision-makers directly to help them understand the importance of IPv6 deployment, at a level where they can make a meaningful risk assessment for their business;
- ensure that non-technical staff understand the long-term, positive effect of IPv6 deployment on their business goals (for example, enabling growth and the potential for reducing costs); and
- for product developers and marketing staff, clarify the benefits for organizations that adopt IPv6.

## Lessons from the private sector

Discussions relating to best practices in the private sector – for ISPs and content providers in particular – resulted in a set of high-level suggestions. Planning for IPv6 deployment might begin with a review of existing infrastructure and an assessment of vendor IPv6 readiness.

Employee training is necessary; particularly in the case of technical employees but, depending on the business, for some non-technical personnel as well (e.g. customer service representatives).

As for IPv6 deployment, businesses should consider working from the outside in: deploying IPv6 via dual stack technology[24] for public-facing services first, and then migrating to IPv6 on internal networks, second. To make the transition easier, they should set internal deadlines and engage with customers, keeping them notified, if not engaged, during the deployment process.

Other approaches are also possible, as the following example shows:

> *Telekom Malaysia´s deployment of IPv6 was driven by two factors, namely; the responsibility to propagate IPv6 adoption as the nation's*

[24] Dual stack involves running IPv4 and IPv6 at the same time.

> *leading communication service provider, and to ensure business continuity for our customers in view of the global IPv4 address exhaustion. Taking the inside-out approach, our deployment of an IPv6-compliant network began years ago by first enabling the core IP network and moving outwards to the edge and customer endpoints. The biggest challenge was in going full swing for the mass adoption of dual-stack Internet broadband services, circa 2013.*
>
> Azura Mat Salim, Telekom Malaysia, text contribution
>
> ”

One policy option for encouraging IPv6 adoption that was suggested was for ISPs to use cost incentives, for example raising the price for IPv4, a scarce resource that is becoming costly to maintain, and providing IPv6 to the customer without extra charge. Finally, collaboration with others in deploying IPv6, as happened during the 2012 IPv6 World Launch,[25] has shown to be effective.

### Research and education networks and tertiary institutions

National research and education networks (NRENs) and tertiary institutions (like universities) conduct valuable research on IPv6. They are important resources for information and knowledge on the subject. NRENs are often ISPs themselves and provide IPv6 services. They also participate at the IETF and work to develop RFCs. Universities can help promote IPv6 by supporting student research projects.

### Government initiatives

Governments are in a powerful position to create an enabling environment for IPv6 adoption. They can lead by example by requiring the public administration to adopt IPv6. They can require IPv6 in ICT procurement policies which, in turn, obligates businesses tendering for government contracts to provide IPv6-capable products and services. The development of IPv6 profiles (Germany[26]) can assist public administration in its own procurement processes and evaluation of tenders, and requiring vendors to

[25] See: http://www.worldipv6launch.org.

[26] See: http://www.bva.bund.de/EN/Themen/Information_technology_bit/IPv6/node.html.

themselves use IPv6 (USA[27]) results in businesses needing to be able to "walk the walk" – not only providing IPv6 services to their clients but running IPv6 themselves.

Submissions to the BPF on national deployment strategies feature different approaches, from working with the private sector on pilot projects that showcase best practices for the benefit of all (Saudi Arabia[28]), to organizing a national IPv6 launch with IPv6-ready groups (Finland[29]), to creating a national IPv6 mandate across the public and private sectors (India[30]). Governments can help industry by publishing an IPv6 adoption guide that tailors relevant information to different stakeholder groups (Singapore[31]). Collaboration with industry through government-supported national working groups (Norway), study groups (Japan[32]), or outsourcing experiments to the private sector (Japan) has yielded successful results:

> *The reasoning [for a government to require their vendors to use IPv6 themselves] is twofold. First, vendors should consider actively demonstrating their commitment to fully supporting IPv6. Second, in the long-term, vendor websites that are only accessible over IPv4 will force their customer to keep supporting IPv4 as well, thereby hindering the ultimate decommissioning of IPv4.*[33]

## The role of the end user

End users and consumers play a role in IPv6 adoption by purchasing IPv6-enabled products, a growing market in light of the IoT. Voluntarily-adopted IPv6 certification standards, or even new "indicators" showing the customer he or she is using an IPv6 product or service (like the "LTE" indicator in the case of mobile phones) can help raise consumer awareness.

## IPv6 measurements – tracking success

IPv6 measurements are useful, illustrative tools that IPv6 advocates can use when engaging with policymakers. Measurements can also be used, of course, to gauge the effectiveness of a best practice. Measuring IPv6 usage before and after the implementation of a policy can help reveal that policy's impact.

APNIC has done extensive work on IPv6 measurement, conducting "a broad-based,

[27] See: https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf.
[28] See: http://ipv6.sa/ipv6-strategy-for-saudi-arabia-2/.
[29] See: https://www.viestintavirasto.fi/en/ipv6now/index.html.
[30] See: http://www.dot.gov.in/sites/default/files/Roadmap Version-II English _1.pdf.
[31] See: https://www.ida.gov.sg/~/media/Images/Infocomm Landscape/Technology/IPv6/download/IPv6AdoptionGuideforSingapore.pdf.
[32] See: http://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/.
[33] Reference made to Dan York, ISOC's Deploy360 blog (11 September 2014). *US DoD's DREN Will Only buy Products With an IPv6 Website.* Available at: http://www.internetsociety.org/deploy360/blog/2014/09/us-dods-dren-will-only-buy-products-with-an-ipv6-website/. [Accessed September 2015].

long term measurement of the level of uptake of IPv6 across the Internet."[34] Outside of providing valuable data for reference, APNIC's website also visualizes the data it collects, making it easy for visitors to see IPv6 deployment rates on a country-by-country basis. Google also measures IPv6 activity, tracking user use of IPv6 on a worldwide basis.[35] Cisco's 6Lab[36] was also mentioned during the BPF as another resource for IPv6 measurement, as well as the website of World IPv6 Launch.[37]

## CONCLUSION AND NEXT STEPS

The BPF explored different best practices that have helped to create an environment that promotes and supports the adoption of IPv6. Amongst other topics, the BPF looked at IPv6 task forces, capacity-building initiatives, best practices in the private sector, and the role that governments, national research and education networks, and tertiary institutions can play.

The BPF outcome document intends to be a source of information and examples for people and organizations in their various efforts to promote, deploy and spread IPv6.

Within the timeframe of the 2015 intersessional work it was necessary to limit the scope of the document to certain 'best practices' and to be selective in the examples. Ideally, work continues, so that this BPF document becomes a living document, and is continuously completed and actualised.

Moreover, a continuation of the BPF on IPv6 would allow the Internet community to broaden the scope and focus on areas that have not yet been looked at, for example the economic decision-making process that sits behind the decision to deploy IPv6, as was suggested during the IGF Main session on Intersessional activities in João Pessoa, Brazil.

*We feel that the potential financial impact of IPv6 adoption is a key factor for the decision many businesses and other stakeholders have to make and further studying and documenting these mechanisms could be a great contribution to achieve our goals of the global deployment of IPv6 and finally in connecting the next billion users to the Internet.*

[34] See: APNIC's IPv6 measurement page, available at: http://labs.apnic.net/measureipv6/.

[35] See: Google's IPv6 Statistics, available at: http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[36] See: http://6lab.cisco.com/stats/.

[37] See: http://www.worldipv6launch.org/measurements/.

Marco Hogewoning, RIPE NCC at the main session on intersessional
work at the IGF 2015 meeting in João Pessoa, Brazil

”

## FURTHER READING:

### Non-exhaustive list of IPv6 task forces:

APIPv6TF (Asia-Pacific): http://www.ap-ipv6tf.org
IPv6 Forum (Australia): http://www.ipv6forum.com.au
IPv6 Council (Belgium): http://www.ipv6council.be/
IPv6 Canada (Canada): http://www.ipv6canada.ca/
IPv6 Forum (Chad): https://www.facebook.com/pages/IPV6-FORUMCHAD/341444906009204
IPv6 Council (Colombia): http://www.co.ipv6tf.org/
LAC IPv6 TF (Latin America and the Caribbean): http://portalipv6.lacnic.net/flip-6-lac-ipv6-tf/
IPv6 Forum (Mexico) http://www.ipv6forum.com.mx ; http://www.ipv6summit.mx/
North America IPv6 Task Force (North America: Canada, US, Mexico): http://www.nav6tf.org/
Spanish Chapter of the IPv6 Task Force (Spain): http://www.spain.ipv6tf.org/html/index.php
Swiss IPv6 Council (Switzerland): http://www.swissipv6council.ch
IPv6 Forum (Thailand): http://www.thailandipv6.net/
IPv6 Task Force (The Netherlands): http://new.ipv6-taskforce.nl
IPv6 Council (United Kingdom): http://www.ipv6.org.uk/
CAv6TF (USA – California) http://cav6tf.org/
Rocky Mountain IPv6 Task Force (USA - Colorado, etc.): http://www.rmv6tf.org/
IPv6 Task Force Hawaii (USA – Hawaii): http://ipv6hawaii.org/
MidAtlantic IPv6 Task Force (USA): http://midatlanticv6tf.org/
TXv6TF (USA –Texas) http://www.txv6tf.org/

### Examples of training and capacity-building resources:

AFRINIC training programmes: http://learn.afrinic.net/en/
APNIC training programmes: https://training.apnic.net/home
RIPE NCC training and education: https://www.ripe.net/support/training
Network Startup Resource Center (NSRC): https://nsrc.org/about

### Examples of IPv6 requirements in ICT public procurement policies:

The Netherlands:
https://lijsten.forumstandaardisatie.nl/open-standaard/ipv6-en-ipv4 (in Dutch)

Spain:
http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Transicion_a_IPv6.html#.VmmWjjbYxVI (in Spanish)

Sweden:
http://www.regeringen.se/contentassets/6136dab3982543bea4adc18420087a03/it-i-manniskans-tjanst---en-digital-agenda-for-sverige-n2011.12 and http://www.pts.se/ipv6 (in Swedish)

USA:
https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf

### Examples of IPv6 measurements:

APNIC's IPv6 measurement page: http://labs.apnic.net/measureipv6/

Google's IPv6 Statistics: http://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption

Cisco's 6Lab: http://6lab.cisco.com/stats/

More resources can be found in the appendices of the BPF's outcome document.

## ONLINE ABUSE AND GENDER-BASED VIOLENCE AGAINST WOMEN

**Coordinator: Jac SM Kee**
**Rapporteur: Anri van der Spuy**

**Period of activity:** one term (2015)
**Approximate number of contributors:** 150
**It was possible to contribute to this BPF during virtual meetings (15+), through the BPF's dedicated mailing list, by completing a survey, by submitting case studies, and by contributing via the public review platform and during the BPF session at the IGF 2015 meeting.**

**Read the BPF's full report:** http://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women

### INTRODUCTION AND OVERVIEW

The BPF on Online Abuse and Gender-Based Violence Against Women gathered a variety of views and inputs on its multidimensional theme and problem through the use of an open, inclusive and transparent process. As a result of this community-driven approach, the BPF's findings reflect a rich diversity of responses from various stakeholders and regions regarding online abuse and gender-based violence.

The work of this BPF is aimed at being one step in the direction of getting stakeholders to take proper cognisance of this complex issue. The process has also demonstrated the need for more work to be done to understand and address online abuse and gender-based violence and to develop effective responses, as will be discussed in more detail below.

This summary is an abbreviated version of the 185-page report that was published by the BPF in December 2015. For illustrative purposes, a few examples, case studies, and comments from participants have been extracted from the report, but for a more thorough and comprehensive understanding of the issue, please read the report.

## Why focus on online abuse and gender-based violence?

Human rights and freedoms apply both offline and online;[38] not only endowing Internet users with certain freedoms, but also imposing certain obligations for users to respect the rights and freedoms of other Internet users. Although great strides have been made to improve connectivity and Internet access around the world, resulting in expanded opportunities for advancing rights, growing access has also resulted in the increased use of technology to perpetrate acts of abuse and/ or violence against users; often resulting in the infringement of human rights online.

While violations of users' rights online may affect all users in differing ways, incidents of online abuse and gender-based violence have roots in existing structural inequalities and discrimination between genders; and disparity in access to, participation in and decision-making over the Internet. As such, online abuse and gender-based violence disproportionately affect women in their online interactions.

Women do not have to be Internet users to suffer online violence and/ or abuse (e.g. the distribution of rape videos online where victims are unaware of the distribution of such videos online). On the other hand, for many women who are active online, online spaces are intricately linked to offline spaces; making it difficult for them to differentiate between experiences of events that take place online versus events offline events.

## What is online abuse and gender-based violence?

Online abuse and gender-based violence refer to the range of acts and practices that either occurs online, or through the use of information and communication technologies (ICTs). It also falls within the definition of gender-based violence under General Recommendation 19 of the Committee on the Elimination of Discrimination against Women (CEDAW) convention, namely:[39]

> *violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty.*

Many of the examples of online abuse and gender-based violence that the BPF collected from participants, case studies, and survey respondents were similar or

[38] For example: United Nations Human Rights Council (UNHRC) (29 June 2012). *The Promotion, Protection and Enjoyment of Human Rights on the Internet* (A/HRC/20/L.13). Available: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280. [Accessed 28 October 2015].

[39] CEDAW (1992). *General Recommendation No. 19 (11th session, 1992): Violence against women.* Available: http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm.htm#recom19 [Accessed 2 November 2015].

overlapping. The examples most frequently identified related to infringements of privacy, harassment, surveillance and monitoring, and damaging reputation and/or credibility. Direct threats of violence, blackmail and attacks against communities were less frequently listed as examples of abuse. Some respondents also felt that excluding women from accessing the Internet and/ or certain online services because they were female amounted to violations of their human rights.

### Example 1: the changing face and nature of abuse

As part of a practice called 'Top 10' in at least two peripheral neighbourhoods of São Paulo, profile pictures of girls aged between 12 and 15 are mixed with phrases describing the girls' alleged sexual behaviour, and the girls are then ranked according to 'how whore they are'. The practice has reportedly led to school dropouts and suicides. BPF participants from the InternetLab, an independent research centre that has done extensive research on the practice, believe the practice to be quite widespread in Brazil.

Online abuse and/or gender-based violence is impacted by the context and ways in which it occurs, as well as other factors such as cultural norms, socioeconomic status, the ordinary level of violence in the community concerned, the rate of Internet adoption and accessibility. It is also important to note that such actions are often an extension of existing gender-based violence, such as domestic violence, stalking and sexual harassment; or tends to target a victim on the basis of her gender or sexuality.

### Example 2: the importance of identity when targets are concerned

During the BPF's session at IGF 2015 meeting in João Pessoa, Brazil, one of the participants, a female member of the European Parliament, relayed some of the experiences of abuse she faced once she was elected:

> *"…as soon as… I made my first speech in the culture committee, actually defending the Erasmus programme (which should not be particularly contentious), I was subjected to Twitter hate by an extreme right party... Because I was a woman and I dared to speak up, the abuse that I got was actually sexual abuse."*

Recognising the rapidly changing landscape of ICTs that affect the expression of online abuse and/or violence, the flexible working definition used by this BPF was not intended to be exhaustive or definitive, but facilitative; to gather best practices and emerging research and analyses in understanding the issue. As will be noted in the findings section below, however, more work should be done to better define and understand the problem in the future.

### Why does the problem have to be addressed?

Online abuse and gender-based violence can, among other things, limit women's ability to take advantage of the opportunities that ICTs provide for the full realisation of women's human rights, act as a barrier to access that can exacerbate the gender digital gap, often violate women's human rights, and reaffirm and reproduce gender stereotypes.

> *I have been online for just over 20 years [and] never in my life have I experienced the kind of abuse and harassment that has been following me around online for the past few years. It has made me stay offline, no longer engage in open conversations, become very distrustful of people generally, I've had problems sleeping, I've been afraid the individuals who have harassed me will turn up where I am in public...*
>
> Anonymous BPF survey respondent
>
> ”

The problem is aggravated by various obstacles that prevent women from exercising their right to access justice in both online and offline environments, including a lack of effective and timely remedies to address online abuse and gender-based violence experienced by women, and obstacles faced in collecting evidence relating to such abuse and violence.

Taking effective action to counter the problem is therefore not only important in ensuring that the Internet fulfils its potential as a positive driver for change and development, but also in helping to construct a safe and secure environment for women and girls in every sphere of life. While increasing attention has been paid over the past few years to understanding the nature, harm and consequences of the problem by some, the importance of addressing online abuse and gender-based violence has arguably not been adequately taken up by several of the stakeholders within the Internet governance ecosystem.

### Example 3: the potential impact of online abuse and/ or violence

A pilot study conducted by a BPF participant in Suriname to gather country-specific information amongst a sample of young female Internet users indicated that respondents believe the effects of online abuse and gender-related violence to be serious. The contributor notes:

> *"It was very revealing that the majority of respondents felt that one of the consequences of online violence against women would be women/girls contemplating suicide or even acting on the thought of suicide. In most other cases the respondents felt that the women and girls would become depressive and may use the Internet less or not at all."*

## How did the BPF approach the problem?

Due to the nature of the Internet as a distributed network of networks, addressing the online abuse of women and gender-based violence requires considerable input and cooperation from, and trust among, a multitude of stakeholders, including the technical community, private sector, civil society advocates and organizations, governments, international organizations, academic community, users, and young people.

For this reason the BPF prioritised the importance of engaging stakeholders from diverse fields in the BPF's work in order to have vibrant discussions informed by multiple perspectives. The BPF investigated the types of conduct that potentially constitute online abuse and gender-based violence, the underlying factors that contribute to enabling environments for the problem, the variety of rights and interests involved in addressing the problem, the impact that online abuse and/or violence has on individuals and in communities, other related contentious issues, and emerging solutions, responses and/or strategies that constitute good and/or best practices and provide insights and lessons to inform future work aimed at countering the problem.

Regular virtual meetings were scheduled using online polls to encourage stakeholder participation from diverse regions. When necessary, for instance in mapping the BPF's scope of work or encouraging input on various drafts, the BPF made use of open, editable and accessible online platforms like Etherpad, Google docs and the IGF's review platform. The BPF's mailing list was furthermore used to elicit and gather input on various aspects of the BPF's work; and social media platforms were used to encourage further participation.

In addition to gathering stakeholder input on these platforms, the BPF also designed and distributed a survey (which received 57 responses from stakeholders in 25 different countries); collected case studies from companies, individuals, civil society organizations, governments and intergovernmental organizations; and designed a social media campaign to gather more input on one aspect of the BPF's work, namely impact. The BPF's final output document, Draft F, was produced as a reflection of this open, iterative and bottom-up process. To read more about the BPF's methodology, see Part II of Draft F.

### Case study 1: the BPF's social media campaign as an example of online abuse

As a part of the BPF's objective of engaging as many stakeholders as possible in its work, BPF participants decided to use Twitter to gather responses to the question:

> *What impact does online violence have on women and girls? Use #takebackthetech to contribute examples to #IGF2015*

On the day before the Twitter campaign was scheduled to commence, BPF participants started receiving tweets and emails warning and threatening them of a concerted effort by a small group of individuals to derail the BPF's planned social media campaign. In the following two days, over 25,000 tweets and retweets were gathered on the Twitter hashtag #takebackthetech, and some BPF participants received direct tweets that were often threatening and misogynistic in nature. 15,225 tweets included links (pictures or weblinks), while 835 tweets were replies (indicating actual attempts at a conversation rather than just 'mobbing' the hashtag).

Besides Twitter, the attack also occurred on platforms like Facebook, email, blogs and minor publications, and the IGF's review platform, where Draft II of the BPF's outcome document was published for public comment at that stage. Besides tweets, the attack included messages, images, memes, 'opinion' pieces and videos. Some of the actors involved in the attack also attended open and freely accessible BPF virtual meetings using false names and/ or impersonating other people.

A significant percentage of the content appeared to be aimed at intimidating, silencing and exposing private information about some BPF participants; contained language and imagery that was misogynistic in nature; contained content that was race-related and/ or potentially xenophobic in nature; contained content that was homophobic and transphobic in nature; and/or contained graphic images and content of sexualised violence.

#### *How did the BPF deal with incidents of online abuse?*

The BPF and its participants not only took precautionary steps to ensure the safety of its participants as far as was reasonably possible, but also ensured that its working methods remained transparent and inclusive so as to give the actors involved in the attack an opportunity to reasonably contribute and improve the BPF's work. In incidents where violent threats where directed at specific users, BPF participants notified Twitter. At the same time, individual users who were not associated with the BPF started reporting many of the most violent tweets. Twitter acknowledged the attack and reported that it was giving moderation priority to the reports made in relation to the hashtags concerned in order to ensure a faster response.

### *Consequences of the attack*

As a result of the attack, some participants disengaged from the IGF's open and inclusive, transparent platforms because they felt unsafe and had concerns related to their privacy being infringed. For example, actors associated with the attack indicated a proclivity to using video and audio material out of context with the aim of distorting the actual purpose and context of the participants' work. The attack therefore had the unfortunate effect of chilling free speech and silencing and intimidating individuals who were previously actively involved in the BPF's work.

The attack also exposed the BPF to one particularly difficult challenge in multistakeholder policymaking, namely when certain actors choose not to engage using existing and designated channels but engaged in a negative campaign-like manner with the aim of derailing a process; despite the existence of other ways for them to interact reasonably and in bona fide manner. While there were indications that most of the attack derived from a small group of individuals, the attack was furthermore characterised by mob-like actions that appeared to be informed by inaccurate understandings of the BPF's work and purpose.

On a positive note, the attack alerted more individuals and organizations to the importance of addressing the challenge of online abuse and gender-based violence. It led to substantial support from a multitude of individuals and organizations and raised awareness of the importance of addressing the challenge. It also provided the BPF with substantially more input and data with which to improve its work – as is discussed in the section below.

## SUMMARY OF BPF's FINDINGS

Over a nine-month work period, the BPF used an open, iterative and bottom-up process in which people from diverse regions and stakeholder groups participated by completing a survey, attending frequent virtual meetings, commenting on four consecutive draft documents, responding to mailing list questions, participating in a social media campaign, and submitting both formal and informal case studies.

In the section below, some of the BPF's main recommendations and lessons are summarised in three categories – the problem definition; the rights and interests involved; and responses. For a more thorough and contextualised discussion of the results, please read the BPF's outcome document.

### *Towards a proper acknowledgment of the complexity of the problem*

### Definitions:

The complexity of the problem of online abuse and gender-based violence starts with the definition. Whilst some BPF stakeholders called for clearer definitions to prevent abuse and the violation of rights, the BPF's work showed that the issue is not only interpreted and approached differently in diverse regions, but also that the terminology used for it is inconsistent, and that the nature and pace of technological development, especially online, demand flexibility in defining related issues.

**Recommendations**

Greater clarity with regards to definitions, in particular ones that can comprehensively and clearly encapsulate its range and need for flexibility, could go a long way to helping advocates address the issue. A starting point could be linking online abuse and/or violence to, and expanding the manifestation of, existing and recognisable forms of abuse and gender-based violence, and identifying new abusive/ violent practices that are specific to ICTs and the Internet.

*I think it's really important for us to have definitions of the problem that don't over regulate, because very often the tools that we would want to use in order to counter harassment will be the same tools that are used to censor.*

Comment by David Kaye, UN Special Rapporteur on the Promotion and Protection of the Right to

Freedom of Opinion and Expression, during BPF session at the IGF 2015 meeting in João Pessoa, Brazil

”

## Contexts and environments:

The importance of comprehensive and flexible definitions is also evident when investigating the impact of diverse contexts and environments on online abuse and gender-based violence. Girls and young women, for instance, may be particularly vulnerable to especially some forms of abuse and/ or violence (as discussed in example 1 above); as will women of diverse sexualities and gender identities (see case study 2 below); women with disabilities (see the recommendation for future research below); and prominent women or women in technology and gaming fields (see example 3 above).

Various underlying factors also play a role in enabling online abuse and gender-based violence, and can also have a compounding effect on the impact of such abuse and violence, as well as the allocation and effectiveness of resources to ensure women gain access to justice and redress. Such factors often relate to specific contexts and/or circumstances, including (for example), when women find themselves in rural areas (see Example 4 below); and the impact of religion, culture and perceptions about morality.

### Example 4: The importance of context

In a remote Pakistani village, a tribal assembly reportedly sentenced women who had been filmed with a mobile phone while dancing and singing together with men at a wedding ceremony to death. In this area, strict gender segregation beliefs do not permit women and men to be seen socialising together. The video was disseminated without their knowledge or consent, and had a far-reaching consequence by transmitting a private moment into a more public space.

The BPF also found that the issue must be studied whilst keeping offline environments, and potential repercussions (including physical, emotional and psychological harm) in offline/ physical environments, in mind. Online violence and gender-based violence often compete with other forms of violence against women in priority agendas, making it important that definitions of abuse of and violence against women take clear cognisance of online forms of abuse and/or violence against women.

### Further research suggestions

In respect of contexts and circumstances, further study and research is required for better understanding the specific challenges that women with disabilities face in this issue, as well as how online abuse and gender-based violence affect girls (below 18 years of age).

## Promoting understanding and awareness:

As closely related to contexts and circumstances, a lack of awareness about women's rights and the impact of the issue on individuals and communities contribute to an inability to make claims for the fulfilment and enforcement of such rights.

### Recommendations

Responses, programmes and mechanisms aimed at addressing the issue cannot be developed in a vacuum and need to similarly address specificity in contexts and relevant circumstances, whilst recognising the broader framework of online abuse and gender-based violence as an issue of gender-based discrimination and a violation of women's human rights. This reinforces the importance of awareness and literacy and education programmes tailored to the needs of specific communities, along with substantial investment in research and statistics on the incidence of the issue.

## *Rights and interests involved: towards a better understanding*

Whilst the fact that 'offline' human rights apply equally online is widely recognised, there appears to be a discordance when the related obligations on stakeholders to protect and uphold these rights are called for where online abuse of women and gender-based violence are concerned. Responses and strategies to counter online abuse and gender-based violence also face significant challenges in sometimes requiring the limitation of certain rights when multiple rights are involved in order to protect other rights – as is discussed in case study 2 below.

### Recommendations

Measures to address online abuse and/or violence must consider, include and balance multiple rights, and should take into account existing inequalities and discrimination that may affect how rights are protected and recognised. Emerging areas of policy work around delineating hate speech online, as well as the right to privacy in the digital age can be opportunities to expand this issue.

### Further research suggestions

Tensions that arise when issues related to multiple rights and interests are involved (including freedom of expression, privacy and anonymity) need further study.

### Case study 2:
### Walking a tightrope? Anonymity, encryption and online abuse/ violence

The protection of and right to encryption and anonymity online are often protected by freedom of expression and other human rights defenders. But while these rights are invaluable in enabling more people to express themselves online, they also enable and protect the perpetrators of online abuse, violence and crime.

For women who face existing discrimination, stigma and other challenges that make it difficult for them to access critical information that is often otherwise restricted or censored, the Internet is an invaluable space to exercise their fundamental human rights. One example is women who are lesbian, bisexual and transgender (LBT) and who may use the Internet to access information, to organize for the advancement of their interests and human rights, and to form communities in relative safety and, if so required, anonymity. Despite this positive potential for LBT women to realise their human rights online, however, studies show that LBT individuals and advocates tend to face more threats and intimidation online – often from users who are anonymous.

The loss of privacy and the disclosure of personal information may subject women to significant threats and attacks, both online and offline. At the same time, as in the LBT community example, perpetrators often use anonymous accounts to perpetuate abusive behaviour and violations online. This presents a challenging context for addressing the issue of online violations of women's rights whilst balancing other fundamental rights. As noted during the BPF's session at the IGF 2015 meeting in João Pessoa, Brazil by David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: 'all tools are subject to abuse, and that's certainly the case with respect to anonymity.'

To address the issue, Kaye argue during the BPF's session that the "default option" for technologies should be anonymity; followed by an investigation of the problems that anonymity may cause. As he also wrote in a report on the topic in May 2015:[40]

> *Encryption and anonymity [...] provide individuals with a means to protect their*

[40] Office of the High Commissioner for Human Rights (May 2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (A/HRC/29/32). Available online, along with other background resources: http://daccess-ods.un.org/TMP/668197.572231293.html.

> *privacy [...], and enabling [...] those persecuted because of their sexual orientation or gender identity [...] to exercise the rights to freedom of opinion and expression.*

Company policies on anonymity and real name policies may furthermore contribute to the manifestation of online abuse and gender-based violence. For example, in one case a survivor of domestic violence managed to avoid her ex-husband for 20 years until a social media platform's "real-name policy" allowed her abuser to track her down. Similarly, LBT women have also faced difficulties as a result of the same real-name policy, which failed to acknowledge their need to use pseudonyms.

## *Considerations in developing responses*

Abuse and gender-based violence against women, whether perpetrated online or offline, is difficult to address because of the attitudes, stereotypes and beliefs that underpin the issue. In an online context, such efforts are further complicated because responses need to be implemented within the global context of the Internet and with the cooperation of a multitude of stakeholders. Efforts to develop, encourage and implement practices to counter online abuse and gender-based violence therefore vary significantly around the world.

Whilst the BPF did not have the scope to investigate all relevant strategies and approaches to the issue, it highlighted many examples of responses taken in the public and private sector, as well as by multistakeholder and community-driven communities. It also extracted various lessons that could be learnt from such approaches and ideas that can be explored in further work.

### Recommendations

The BPF found that it is critical that public and private sector approaches to the issue be developed transparently in due consultation with current users (including victims and survivors of online abuse and/ or violence) and civil society organizations, and to also consider the needs of future users as Internet access and adoption expand globally.

Many strategies also fail to consider the potential impact of certain approaches on other rights, making a better understanding of the rights and interests involved in addressing the issue (discussed above) vital. Consultation with civil society organizations working on human rights, women's rights as well as violence against women is an important measure for this consideration.

Where countries consider developing legislative responses to the issue, it is important that relief and redress be prioritised over criminalisation. Not only do governments need to prioritise the access that victims and survivors of online abuse and gender-based violence have to justice, but flexible and informal (yet also transparent) measures that can more easily, quickly and effectively respond to online behaviour need to be investigated in future research. This does not only include improving law enforcement agencies' responses and awareness of the issue, but also demands an evaluation of entire judicial systems' ability to respond effectively to victims' and survivors' needs. Where possible, the creation of specialised and fast-tracked agencies and courts (including such online measures) to help victims and complaints with complaints should be explored.

There is also a need for the public sector to evaluate its relationship with intermediaries in addressing and countering the issue, including the level of obligations it can realistically impose on intermediaries. Any duties imposed upon intermediaries, however, need to be both flexible to account for technological change, and workable to account for the nature and speed of content distribution. Internet intermediaries can explore clearer and more explicit commitments to comprehensive human rights standards to better address the issue of online abuse and gender-based violence. Existing legal frameworks can provide guidance on the actions they can take to ensure that women's rights online are promoted and respected in compliance with international human rights standards.

Lastly, while the responsibility of educating users and improving digital literacy levels arguably lies primarily with the public sector, BPF participants also suggested that the public sector should consider cooperating more closely with the private sector (particularly digital intermediaries) to ensure education also continues on relevant platforms.

### Further research suggestions

There is a need for further research and investigation into technical community responses (e.g. CSIRTs) to the problem of online abuse and gender-based violence.

## NEXT STEPS

The work of this BPF is both timely and instructive considering the increasing effort by different stakeholders at national and global levels to understand and address the issue of online abuse and gender-based violence. It has showed that there are no one-size-fits all solution to this multidimensional and complex problem, and that greater study is needed to further investigate the range of acts, underlying causes, diversity and breadth of impact, and potential responses that can be developed for the issue.

The BPF's work has facilitated diverse stakeholder engagement on the issue, and as such, benefitted from different views and perspectives. This is, however, only a first step towards a more comprehensive understanding and response. It is hoped that some of the findings and areas for further exploration can inform continued discussion and efforts: both at the IGF as a critical platform for multistakeholder engagement on key internet policy, governance and human rights issues, and in other policy discussion spaces.

## FURTHER READING:

**For more examples, resources, case studies and full citations, see the BPF's report:**
http://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women

## STRENGTHENING MULTISTAKEHOLDER PARTICIPATION MECHANISMS

**Coordinators: Avri Doria, Cheryl Miller**
**Rapporteur: Brian Gutterman**

**Period of activity: two terms (2014 and 2015)**
**Approximate number of contributors: 100+**
**It was possible to contribute to this BPF both during the 2014 work cycle and again in 2015 during virtual meetings (20+), through the mailing list, via a public call for inputs, via the public review platform and during the BPF session at the IGF 2015 meeting.**

**Read the BPF's full report:** http://www.intgovforum.org/cms/documents/best-practice-forums/developing-meaningful-multistakeholder-participation-mechnisms/580-igf-2015-bpf-strengthening-multistakeholder-participation-mechanisms-1

### INTRODUCTION

The 2015 BPF on Strengthening Multistakeholder Participation Mechanisms output report reflects two years' work on the same subject. This report is a working document and builds upon the foundation of work of the 2014 BPF, which produced this output document.

The report, developed through an iterative process with active members of this BPF and the broader IGF community, presents both reflective and forward-looking viewpoints on the 2014 exercise from stakeholders participating in 2015. It also incorporates content and examples received from a call for input to further analyse much of the normative analysis of important issues raised pertaining to strengthening multistakeholder participation mechanisms; both during the 2014 work cycle as well as in 2015. Much of the content of the report also derived from the discussions on the group's open mailing list.

The BPF's 2014 work focused on definitions and explored some of the theory behind multistakeholder models. In 2015, the group documented a number of existing practices and attempted to extract some practices that can be considered when working within a multistakeholder model. Some notable issues encountered and explored in depth in the report and throughout open discussions include the nature of consensus in multistakeholder organization and decision-making, the 'bad actor' problem, the relationship between multistakeholder models and democratic models, and both best practices and obstacles to building trust and lowering barriers for participation.

## SUMMARY

Key findings and views of the community in its 2015 work, while building on its 2014 work, include:

### Building trust

Many participants in the 2015 BPF agree that a key factor in facilitating productive outcomes through multistakeholder mechanisms is the presence of trust among stakeholders. It was noted that transparency and accountability are two critically important components of building trust, and that trust is developed over time by stakeholders acting oftentimes in accordance with previous statements – as judged by other stakeholders. In the context of Internet governance multistakeholder mechanisms, many stakeholders have had previous interactions that bear on the initial level of trust they bring with them.

Enhancing trust among stakeholders is a challenging, time-consuming process. While educational and participatory resources to facilitate participation exist, there are few resources for building trust among stakeholders.

#### Recommendations

Developing and making available tools and methods for building trust among stakeholders would be an important contribution to the enhancement of multistakeholder mechanisms. In addition to increased efforts among all stakeholders to build and establish such trust, there should also be targeted efforts to identity where trust is lacking and needed.

#### Examples

Some useful analyses and examples of multistakeholder mechanisms being used in fields other than Internet governance can be found in a 2015 paper from the Berkman Center for Internet & Society at Harvard University, titled "Multistakeholder as Governance Groups: Observations from Case Studies".[41] This paper synthesizes a set of twelve case studies of real-world governance structures and examines existing multistakeholder governance groups with the goal of informing the evolution of – and current debate around – the future evolution of the Internet governance ecosystem in light of the NETmundial Principles and Roadmap, discussions at local, regional, and global IGF meetings, and the NETmundial Initiative, as well as other forums, panels, and

[41] See: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549270.

committees.

## Participation and resources

The 2014 BPF found that while many advocates of multistakeholder mechanisms seek to be expansively inclusive, their efforts are frequently inadequate in terms of educating potential stakeholders about Internet governance and enabling them to make an informed choice about participating. Similarly, some stakeholders who wish to participate may be unable to do so due to a shortage of resources. While some resources are available from certain organizations to alleviate this situation, they are insufficient for the current needs and are not increasing comparably to the growth of the Internet.

### Recommendations

The 2015 BPF community advocates for the exploration of possible solutions to the variety of obstacles that hinder participation in multistakeholder Internet governance processes and mechanisms. Some participants emphasized that more transparency around the funding of stakeholders participating in multistakeholder processes is needed; as is an overall increase in public funding of participants, since funding can often determine who gets to influence Internet governance spaces.

### Example from an African context

A report[42] from Research ICT Africa[43] submitted to the BPF illustrates some notable observations about the lack of education regarding multistakeholder mechanisms and processes as well as its implications within the context of Internet governance in Africa. This analysis is particularly relevant when examining the successes and/or failures of multistakeholder models and mechanisms in the context of the ten-year review of the World Summit on the Information Society (WSIS+10). Inclusive participation in multistakeholder mechanisms and processes is certainly a strength of the model in general. However, as the abovementioned report describes, the necessary outreach and promotion of multistakeholder participation methods is lacking – particularly in civil society, developing countries, and industries where diverse stakeholder engagement is necessary.

## Bad actors and bad conduct

[42] See: http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Discussion_paper_-_Mapping_Multistakeholderism_in_Internet_Governance_-_Implications_for_Africa.pdf.

[43] See: http://www.researchictafrica.net/home.php.

One significant and problematic issue raised by participants in both 2014 and 2015 is the prospect of so-called "bad actors" and "bad conduct" by individuals or organizations in multistakeholder mechanisms. Many multistakeholder mechanisms and processes assume that stakeholders have an interest in reaching outcomes supported by consensus or 'rough consensus'.[44] Some consequently define 'bad actors' as being individuals or organizations that seek to damage trust in the process and its outcomes through obstructive participation. Therefore, some BPF participants fear that multistakeholder mechanisms are vulnerable to bad actors because it explicitly places trust in and asserts balance among stakeholders.

A number of participants in the BPF shared views on the mailing list regarding what they believed constituted a bad actor in the context of multistakeholder decision-making mechanisms and processes. It was said also that many of the traits of a 'bad actor' can similarly be defined as being 'bad conduct' in multistakeholder processes.

### Who are 'bad actors' and what constitutes 'bad conduct'?

The following list of traits/ indicators of an individual 'bad actor' or 'bad conduct' was compiled verbatim from participants on the BPF's mailing list. Indicators of participants that might be acting as bad actors or might be displaying bad conduct include a participant who:

- is abusing the process to delay or deform substance;
- is making veiled threats;
- has undisclosed conflicts of interest, including contingent fees, etc.;
- is engaged in 'astroturfing';
- is inflating their value artificially;
- does not want to enable or engage in fact-based and reasoned, respectful disagreement;
- engages in attacking and disparaging comments, attacks individuals or organizations or states with hostile and disparaging remarks, and seeks to disrupt civil discourse;
- make remarks that are detrimental to active participation of some other people and/or to reaching a consensus in multistakeholder discussions;
- participate in a process with the effect of scuttling the process;
- persist in arguing a position after it has been discussed in detail and found to not be part of the consensus, and use that position to block the continuing work of the rest of the group;
- persist in raising out-of-scope issues that act as roadblocks to a group-making process;
- whose primary form of argument is personal attack, intimidation and/or bullying.

[44] The issue of the various definitions of 'consensus' and 'rough consensus' when it comes to multistakeholder processes and decision-making is explored in more depth throughout this paper.

## Working definitions

Through the 2014 BPF process on this subject, the IGF community was able to draft some important working definitions (below), which were refined and built upon in the BPF's 2015 term. The working definitions below are the result of these discussions over the past two terms.

### 'Multistakeholderism'

Multistakeholderism[45] as defined in the 2014 BPF is:

> *… the study and practice of forms of participatory democracy that allow for all those who have a stake and who have the inclination to participate on equal footing in the deliberation of issues and the design of policy. While they may assign implementation to a single stakeholder group, implementers are accountable to the decision-making stakeholders.*

Another definition proposed was:

> *In our context, a multistakeholder model is a framework or an organizational structure that adopts the multistakeholder process of governance or policy development, which aims to bring together key stakeholders such as business, civil society, governments, research institutions and non-governmental organizations [NGOs] to cooperate and participate in the dialogue, decision-making, and implementation of solutions to problems and common goals.*

One contributor in the 2015 process emphasized that an alternative definition could be:

> *Multistakeholder mechanisms in the realm of Internet governance is one where all relevant stakeholders are engaged in discussing issues that affect their interests and exploring possible policy approaches.*

As identified through 2014 BPF process, the key attributes of a multistakeholder mechanism are that it:

- is democratic,
- open,

[45] One participant suggested that the BPF should avoid using the word "multistakeholderism", even if alternatives like "multistakeholder cooperation" are more verbose. The "ism" stirs the response that it sounds analogous to a faith, creed, or ideology that potentially biases the way the issues are framed, proposed, and opposed.

- known to the relevant stakeholders,
- accessible,
- works iteratively,
- achieves rough consensus (as opposed to unanimity); and
- achieves balance between all stakeholders.

Note that "equal footing" is not sufficient – although often necessary – if some stakeholders are funded and can participate intensively and others are not funded and cannot participate. Even remote participation methods, when available and functioning properly, are not sufficient to overcome the imbalance.

Where direct participation is not possible, there should always be ways for a broader range of stakeholders to provide their views or concerns. Furthermore, there should also be due consideration of the issues and concerns of those "not in the room". In consideration of those not in the room, attention should also be paid to those who are beyond or otherwise not connected to the process, including those:

- who have limited bandwidth or no connection to the Internet;
- who have yet to be connected to the Internet entirely;
- whose native language is not English;
- who are unable to navigate the needed tools to contribute for accessibility reasons; and
- who lack the tools to contribute, are in need of remote participation tools, or do not know how to contribute.

## Examples

Submissions received through the 2015 BPF call for input[46] provide unique examples of multistakeholder mechanisms and processes in practice, as described by organizers of the 2013 IGF in Bali, Indonesia, a representative from the Swiss IGF, an example submitted by a stakeholder from Rwanda, and from the Internet Governance Conference Japan (IGCJ).Other examples noted include the 2014 NETMundial process[47] and the WSIS+10 multistakeholder preparatory process.

[46] See Further Reading list at the end of this summary for full references to the examples.

[47] Marilia Maciel, Nicolo Zingales, and Daniel Fink (2014). *The Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial)*. Available: https://publixphere.net/i/noc/page/IG_Case_Study_NETMundial (Accessed 11 November 2015).

### ‘Consensus’[48] and ‘rough consensus’

Throughout the 2015 BPF process and in developing the BPF’s final outcome paper, many participants commented on the ambiguities and differences of opinion about the term ‘consensus’ and what it means in the context of multistakeholder decision-making processes. The term ‘rough consensus’ is also widely used in the Internet governance field and its definition was also discussed and seen as a term that should be explored and/or defined further to help future multistakeholder decision-making structures. One participant provided input from the viewpoint of consensus-building, where the general view can be described as:

> *… consensus has been reached when everyone agrees they can live with whatever is proposed after every effort has been made to meet the interests of all stake holding parties.*[49]

Another BPF participant provided input from the viewpoint of the International Organization for Standardization (ISO) where consensus is described as:

> *General agreement, characterised by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments. NOTE: consensus need not imply unanimity.*[50]

Another opinion shared was that in some United Nations processes:

> *…there is no formal definition, but the practice is to declare consensus if there is no formal opposition. That is, the Chair says something like 'I propose to approve XYZ', and, if nobody formally objects, then 'XYZ' is approved 'by consensus’.*

In the Internet Engineering Task Force (IETF), RFC2418 (1998) describes a "rough consensus" process:

> *IETF consensus does not require that all participants agree although this is, of course, preferred. In general, the dominant view of the working group shall prevail. (However, it must be noted that "dominance" is not to be determined on the basis of volume or persistence, but rather a more general sense of agreement.) Consensus can be determined by a show of hands, humming, or any other means on which the WG agrees (by rough consensus, of course). Note*

[48] A number of ‘consensus-building’ references are included in the *Practice descriptions and other input received through the 2015 BPF* section at the end of this document

[49] Susskind, Lawrence; McKearnan, Sarah; and Thomas-Larmer, Jennifer. (1999). *The Consensus Building Handbook*. Thousand Oaks, Calif.: Sage Publications.

[50] http://www.iso.org/sites/ConsumersStandards/1_standards.html#section1_5
" ISO/IEC Guide 2:2004 Standardization and related activities – General vocabulary".

> *that 51% of the working group does not qualify as "rough consensus" and 99% is better than rough. It is up to the Chair to determine if rough consensus has been reached.*

However, the concept of "rough consensus" has evolved in the IETF through usage and experience and RFC2418 is currently being updated as "a community sense of strongly-dominant agreement, in the absence of compelling objections, is used to make decisions". RFC7282 has also recently been published to elaborate on the use of consensus (and humming) in decision-making. One of the key concepts here is that objections must be fully addressed even if not accommodated, although objections must provide a fully reasoned argument relevant to the subject. The IETF case must also be understood in the context of development of engineering solutions in technical standards.[51]

### Recommendations

There was agreement during the BPF session at IGF 2015 in João Pessoa, Brazil, that any group or organizations undertaking multistakeholder deliberations should thoroughly discuss their own definitions of 'consensus' or 'rough consensus' prior to moving towards making any decisions, to be sure that the term is clearly defined and understood by all involved.

## 'Mechanisms'

'Mechanisms' as defined by the 2014 BPF are the practices of interaction within a multistakeholder mechanism sometimes relying on rough consensus and that require a degree of trust among stakeholders. However, some participants in the 2015 BPF said the meaning of rough consensus is not clear in the context of a multistakeholder process for policy development (as discussed above).

One participant thought it would be useful to produce a list of different sorts of technologies (as types of mechanisms) available that facilitate multistakeholder work. The following list was developed through the BPF's mailing list:

- For drafting documents or papers, Etherpad is free and open-source and can be self-hosted (http://etherpad.org). Riseup pads (https://pad.riseup.net/) are a

[51] With regards to the term "rough consensus", one participant said it "is a term of art in [the] IETF [Internet Engineering Task Force], and I doubt that the way [the] IETF determines 'rough consensus' would be appropriate for other processes. There has been a recent tendency to use the term 'rough consensus' to refer to any outcome [that] was obviously not a consensus outcome, even though no IETF-like process was used to reach the outcome".

good alternative, but tend to disappear after 30 days of inactivity. Other alternatives include ZohoDocs and OnlyOffice.

- For editing, Wiki was suggested (https://www.mediawiki.org/wiki/MediaWiki).
- For meetings, the free, open-source and self-hostable alternative to paid options is Jitmeet (https://jitsi.org/Projects/JitsiMeet).
- For audio conferences, Mumble was suggested (http://wiki.mumble.info/wiki/Main_Page).
- For meeting plus document collaboration, Team Viewer52 was suggested.
- More mainstream tools like Slack, Evernote, and InVision were also recommended; as was Zoom for video conferencing.

### *Possible criteria for meaningful multistakeholder mechanisms:*

Multistakeholder mechanisms and processes flow from shared trust among stakeholders and common definitions. If either or both of these factors are weak or absent, a multistakeholder process may be less likely to reach an outcome. Where these factors are present, a multistakeholder process has the potential to reach substantive agreements among stakeholders. Some argue that there is no single "best" multistakeholder model.

Many in the 2015 BPF agree that basic elements of a multistakeholder mechanism as outlined in the report should hold. Specifically, there should be involvement and input from multiple stakeholders, a shared understanding of the issues, a desire to collaborate to address the issues, and the existence of trust among stakeholders. However, it was argued that it is not clear if the same approach will have the same results across all countries and for all issues.

A paper titled "*The Criteria of Meaningful Stakeholder Inclusion in Internet Governance*",[53] which was submitted by an active contributor to this BPF, proposes a civil society approach recognising a set of four criteria for meaningful stakeholder inclusion in global Internet governance processes:

1. The body should have access to the perspectives of all those with significant interests in a policy problem or its possible solutions.
2. There must be mechanisms to balance the power of stakeholders to facilitate them reaching a consensus on policies that are in the public interest.
3. Mechanisms of accountability must exist between the body and its stakeholders to demonstrate the legitimacy of their authority and participation respectively.

[52] As a security best practice, one participant cautioned against recommending Team Viewer, as "it exposes a large attack surface for end users/participants that is not required for the purposes of a meeting/document collaboration and can definitely be solved through other venues that do not increase the security risk in such a manner".

[53] See: https://docs.google.com/document/d/1d4jHTahdLhebykMHbaPFpTjlkECZGi5OQgjOTqGn2jg/edit.

4. For each stage involved in governance, the body should either be directly empowered to execute it, or linked to external institutions that have the authority to do so, as appropriate.

Such criteria could simplify the examination and critiquing processes that purportedly allow for public or multistakeholder involvement in public policy development.

Example:

Some interesting insight was provided on the topic of equality among stakeholders and the concept of "equal footing" by the submission of the UK Government to this BPF that describes the UK Government Multistakeholder Advisory Group on Internet Governance (MAGIG). The paper is explains that the MAGIG is "not a multistakeholder model but rather an example of how governments can involve a range of stakeholders in developing policy".

## CONCLUSIONS

Multiple drafts of the BPF's outcome document were released online for public comment leading up to the IGF 2015 meeting in João Pessoa, Brazil, where the IGF community was asked to consider if the paper could be used as an output document that can, in turn, be used as an input by other groups involved in developing, or evolving, their own multstakeholder processes.

Stakeholders who participated in the 2015 physical meeting[54] of the BPF at IGF 2015 supported the initiative to use the report as an output document and to maximise its visibility and usability moving forward. A few suggestions made during the session include:

- the BPF's paper could be shared with the regional and national IGF initiatives.
- the group could compile existing codes of conduct or standards of behaviour that already exist and that could be useful to groups that are already working but might not have such guidelines, or for groups who will be starting multistakeholder work of some kind.
- the paper could evolve into a 'how-to' guide for developing multistakeholder groups or mechanisms, or could evolve into becoming a paper that provides a catalogue of options for groups seeking to use multistakeholder processes.

[54] The transcript of the meeting can be found here: http://www.intgovforum.org/cms/187-igf-2015/transcripts-igf-2015/2316-2015-11-10-bpf-developing-meaningful-multistakeholder-participation-mechanism-workshop-room-5.

- online trainings or webinars could facilitate disseminating the existing work done and could also help the work evolve, pending the renewal of the IGF and decisions taken by the IGF MAG together with the community.

## FURTHER READING:

*The following is a compilation of inputs received from the community in response to a public community-wide call for input[55] at the outset of the 2015 BPF intersessional work cycle. This section also contains some useful and relevant academic articles submitted and collected by members of this BPF for further discussion and use by the IGF community.*

*The following practice descriptions and other input were either collected by the BPF from existing research or submitted for the consideration of the BPF by members of the IGF community. They are included as examples for others to use as an educational resource.*

**Indonesia in IGF 2013 and the way forward:**
https://docs.google.com/document/d/1gG9pdgDsKejrR5ViRI26Lb5m2MQ6GTtSqHqk5I8CUj0/edit

**City TLDs and Best Practices - Submitted by Thomas Lowenhaupt,** the founder and director of Connecting.nyc Inc. and former member of the .NYC Community Advisory Board: https://docs.google.com/document/d/1rU8h2m1-zdIbYIFzaWYzE7IjfVN67VcpWfQNeotX-N4/edit

**Contribution to the IGF Conference: Case of Rwanda in New Information and Communications Technology (NICT):** *The good practice of NICT in Rwanda:* https://onedrive.live.com/view.aspx?resid=50432DE1FDE1CD44!111&app=Word&authkey=!ALmQiH6V65_SIhk.

**Research paper from the Berkman Center for Internet & Society at Harvard University:**
*Multistakeholder as Governance Groups: Observations from Case Studies:*
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549270

**Swiss IGF contribution on meaningful multistakeholder participation mechanisms:**
https://docs.google.com/document/d/1hsHj_G5HBfP0mjP6xUaFKGWEH_MdX0f9WjV6E9dMjI8/edit?usp=sharing

**Paper contributed via the BPF mailing list by Mr. Jeremy Malcolm:**
https://docs.google.com/document/d/1d4jHTahdLhebykMHbaPFpTjIkECZGi5OQgjOTq

[55] See: http://www.intgovforum.org/cms/best-practice-forums/3-developing-meaningful-multistakeholder-participation-mechanisms.

Gn
2jg/edit

**Internet Governance Conference Japan (IGCJ):** http://igcj.jp/

**Input received through the mailing list from Ms. Anriette Esterhuysen:** *Mapping multistakeholderism in Internet Governance: Implications for Africa:* http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Discussion_paper_-_Mapping_Multistakeholderism_in_Internet_Governance_-_Implications_for_Africa.pdf

**Contribution from Mr. Gary Hunt of the government of the UK:**
*UK DCMS Multistakeholder Best Practice Contribution*:
https://drive.google.com/file/d/0B4oPMhWAuvN-eWJPaTBBTWg4SVk/view

**Thoughts on Best Practices for Multistakeholder Participation Mechanisms:**
http://www.apig.ch/best_practices.pdfhttps://drive.google.com/file/d/0B4oPMhWAuvN-eWJPaTBBTWg4SVk/view?usp=sharing_eid

**Reflections on making Internet governance democratic and participative:**
http://www.apig.ch/democratic_and_participative.pdf

**Contribution from Sherly Haristya and Peng Hwa Ang:**
http://bestbits.net/multistakeholderism-and-the-problem-of-democratic-deficit-sherly-haristya-and-ang-peng-hwa/

## ESTABLISHING AND SUPPORTING CSIRTs FOR INTERNET SECURITY

**Lead experts: Maarten Van Horenbeeck, Cristine Hoepers**
**Coordinator: Markus Kummer**
**Rapporteur: Wout de Natris**

**Period of activity:** two terms (2014 & 2015)
**Approximate number of contributors:** 25
**Contributions for the BPF were collected during virtual meetings (7), on the mailing list, by providing case studies, via the public review platform, and during the BPF session at the IGF 2015 meeting.**

**Read the BPF's full report:** http://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/627-bpf-csirt-2015-report-final-v2

## INTRODUCTION

The work of this BPF started in 2014 for IGF 2014 in Istanbul, Turkey. The work in the first term focused primarily on finding best practices for establishing and maintaining a computer security incident response team (CSIRT). The suggested name of the BPF in 2014, namely BPF on Establishing and Supporting Computer Emergency Response Teams (CERTs) for Internet Security, was changed because handling incidents is primarily what CSIRTs do. The CSIRT community also indicated that the term 'CERT' is somewhat confusing for those external to the community.

The 2014 BPF found that various best practices are common, well-defined and well-known within the community. The discussion within the BPF focused primarily on topics that were main concerns for the CSIRTs community itself, namely misunderstandings regarding what a CSIRT is and does; privacy and CSIRTs; schooling and awareness; mistrust among CSIRTs due to the tendency to task a CSIRT with additional functions, e.g. law enforcement, anti-terrorism, and intelligence (often the appointed national CSIRT); or placing the CSIRT within larger organisations with those functions. Another topic looked at was the expressed need for a national point of contact in each country; an appointed or voluntarily acting CSIRT of last resort that responds to a request for assistance in case of emergencies when no one else is responding.

Looking back on the 2014 process, one overarching theme that members decided to make their main theme, could be distilled from the recommendations made in the BPF's first term: *Misconceptions around the role and responsibilities of a CSIRT*. As these misconceptions mostly lie outside of the CSIRT community, this choice led to the decision that the BPF should actively reach out to other stakeholder communities in its second term in 2015. This proved a difficult, and time-consuming task. The BPF's session at the IGF 2015 meeting in João Pessoa, Brazil, however, enabled the BPF to gather more stakeholder input as it enabled new, actively invited stakeholders to come to the session and to share their views, which led to valuable insights and potential ways forward. A new topic that presented itself in 2015 is 'responsible disclosure', which is discussed in more detail below.

This BPF considers itself a success. It found that the 2014 report is seen as a source of inspiration for those having to build a new CSIRT, with one tangible outcome in Serbia, where the report was used as a basis while building a national CSIRT. In 2015 a further indicator for the level of success is the fact that controversial topics within the CSIRT community are addressed in the BPF and translated into actions from and debates within the CSIRT community itself, such as the Forum for Incident Response and Security Teams (FIRST) or successfully brought to other fora such as the Organisation for Economic Co-operation and Development (OECD) and the Global Forum of Cyber Expertise.

The BPF addressed issues that delve to the core of how CSIRTs are used to work and their rationale, which led to the acknowledgement that (perhaps) some changes are called for in the ways in which CSIRTs tend to operate and the realities they face in 2015. An all-telling question, that was not answered (yet), remains: does the current definition of a CSIRT match the reality of work asked and tasked? The challenge for CSIRTs lies in gaining more influence so that the successful aspects of CSIRTs, with maintaining foremost trust-building aspects, remain in place and most unavoidable changes due to the active involvement of CSIRTs in defending national and economic security are adapted in ways that maintain CSIRTs' positive characteristics.

This year's report shows the first signs of both of these changes, where misunderstandings are addressed directly with other stakeholder communities and trust to work together is built. In this way the underpinning value of a CSIRT's existence, namely trust, is maintained between stakeholders and broadened between different stakeholder communities.

## SUMMARY

The BPF's work was built on the presumption and BPF stakeholder consensus that a CSIRT is:

> “a team of experts that responds to computer incidents, coordinates their resolution, notifies its constituents, exchanges information with others and assists constituents with the mitigation of the incident.”

This definition is vital when understanding the context of the main theme of the 2015 BPF, namely misconceptions around the role and responsibilities of a CSIRT. A brief investigation showed that misconceptions are rarely found within the CSIRT community, but arise in its interactions with other stakeholders. Among other things, external stakeholders demand additional tasks from CSIRTs or embed CSIRTs in wider security organizations.

The effects of such demands include a loss of trust – something that is regarded as an essential element in facilitating the voluntary mutual assistance and information exchange between CSIRTs. Teams need each other to mitigate incidents and emergencies. Endowing CSIRTS with extra tasks could cause both intended and unintended consequences to trust; and a loss of trust directly affects the effectiveness of CSIRTs, because the exchange of information and offered assistance could be hindered or stopped altogether. Laws, applicable to these wider tasks or larger entities, may even prohibit information exchange, which also affects the relationship between CSIRTs as in order to be successful, assistance from other CISRTs is often needed. Cooperation is second nature to CSIRTs, which have an international network where insights and solutions are shared, relationships are built and common approaches are tested.

Despite these comments, there is consensus that there is no right or wrong approach when it comes to a CSIRT. As was shared by one of the participants: “The role of CSIRTs is defined by the parent organization and CSIRTs should perform duties as they are given to it.” While some CSIRTS may be “successful” if one considers the role attributed to it by its parent organization, more demands could be made of a CSIRT – the basis of this document.

It is important to understand, and again the importance of cooperation based on trust is stressed here, that CSIRTs are found within very different organizations in both the private and public sector, including within companies, governments, the military, universities, and even to protect a product. Each CSIRT exists with one purpose: to secure its constituents from incidents and to mitigate incidents when they occur. To fulfil this function in an optimal way, CSIRTs (defined by very different backgrounds and purposes) need each other. It is here that the influence of extra tasks to a governmental CSIRT affects trust and cooperation most. Hence the unanswered question: were the decisions for allocating extra tasks taken intentionally or unintentionally? Were the implications on trust fully understood when the decision was made, often by policymakers within government?

In the past two decades the Internet and its underlying nodes and networks have become increasingly critical infrastructure on which the economy and national security have come to depend. This has an inevitable effect on the way external stakeholders regard CSIRTs. This BPF showed that the role and involvement of CSIRTs in national security and/or in guarding economic interests tends to expand. Given the fact that nation states use vulnerabilities in software or defence systems of an attacked party (whether public or private), CSIRTs become automatically involved to some degree.

In recent years, due to frequent incidents, hacks and intrusions in networks, interest from governments and higher management within private organisations in cybersecurity issues has notably risen; creating expectations and different demands. Expected laws within the European Union increase demands in cybersecurity from both a network and information security angle for critical infrastructure, which often resides in private hands, and also from the perspective of (the reporting of) data breaches; thus a privacy point of view.

Reporting incidents is about to become the norm. On the one hand, it is likely a government CSIRT that is reported to, while on the other hand, to mitigate the incidents, cooperation between CSIRTs is necessary. This fundamentally changes the voluntary way cooperation takes place at present, an example how decisions can change the very base of cooperation for CSIRTs.  Experts like Mark Goodman see reporting as fundamental. In his book *Future Crimes*, Goodman writes about the under-reporting of incidents: "This silence is at the very heart [of] our cyber-security problems," with the result that "these incidents cannot be aggregated and studied, common defences are not developed, and perpetrators roam free to attack another day".[56]

These recent developments have led to a valuable insight. In the past, CSIRTs were often absent in policy discussions, but these recent developments have highlighted the need for direct involvement of CSIRTs in policy discussions as the traditional definition of a CSIRT has been put under considerable strain. While the need to cooperate with other involved stakeholders could bring mutual benefits and, arguably, is more necessary than ever, it could also, as a downside, have a negative impact on trust within the CSIRT community itself.

One example is cooperation with law enforcement agencies (LEA). Mutual cooperation and assistance is seen by several participants as an enhancement to other participants' roles, as long as their functions are truly and correctly separated. Each has its own role and, within this role, CSIRTs can assist LEAs with building evidence, e.g. through providing technical expertise or analyses of complex attacks or by sharing information. The moment a CSIRT becomes equated with law enforcement, as is the case in several African countries, the level of trust needed to assist or cooperate

[56] Mark Goodman (2015). *Future Crimes*. New York: Doubleday. pp 374-375.

between this CSIRT and the potential partners from the private sector is damaged or dissipates. Some BPF participants even argue that the only truly successful CSIRTs are private CSIRTs.

There was a general agreement that communication between CSIRTs themselves and with other stakeholders is of vital importance to avoid misconceptions and maintain trust and (or gain) cooperation.

## CSIRTs and privacy

BPF participants feel that they are custodians of privacy. As someone from the CSIRT community described it:

> "How are you going to protect privacy and free speech on the Internet *without* a CSIRT to let you know when a malware strain is ex-filtrating private data, or who will assist when a (D)DoS attack floods your preferred communications server with unwanted traffic? Neither of those can be done by the end user."

A few concerns about privacy remain, however, and could be addressed by making the ways CSIRTs handle and share data more transparent and accountable.

One valuable insight gained was that where CSIRTs are concerned, it is better to use the term 'data protection' than privacy. This term is easily understandable; where privacy may mean something different to individuals and in diverse cultures and jurisdictions. On the other hand, it is also understood that the term privacy is more relevant to the broader public.

One outcome was that the BPF recommended that the CSIRT community discusses whether a document that makes the process of data handling more transparent, but also addresses questions on the necessity of handling and processing of that data, is feasible. This proposed work has to achieve one goal: that all those directly and indirectly involved understand that, as was noted "a well-run CSIRT is an essential part of protecting their privacy and security".

## Policy and CSIRTs

Not long ago, when the European Commission consulted the CSIRT community on policy, a CSIRT representative was noted as saying:

> "Politicians and lawyers should leave CSIRTs alone; they know what they are

doing."

The European Commission, in turn, proposed a Directive with the aim of ensuring "a high common level of network and information security (NIS) across the EU".[57]

Although several BPF participants still have their doubts about involvement in policy debates, others have come to understand that not being present in policy debates is the equivalent of not being heard. In order to preserve what is good, in the context of a fast-paced sector, CSIRTs need to raise awareness of their needs and priorities with policymakers.

Some CSIRTs' actions already show an awareness of the importance of interacting with policymakers. An OECD report on CSIRT metrics,[58] for instance, contains an introductory chapter in the report stating what CSIRTs are and what they do following cooperation and input from various CSIRTs. In a general sense the need for more involvement in relevant policy discussions shows from a 2015 FIRST initiative, where the organizations participating identified "cybersecurity policy advisory" as one of the new roles of a CSIRT.

## (Supply) chain approaches to cybersecurity and the role of CSIRT

There is no single actor that can make the Internet safer for end users. ICT products and services, end users' sanitary measures, awareness programmes, regulatory measures, and other initiatives are hugely interdependent. Another form of influence on cybersecurity that is seen as worthwhile to investigate further includes the effects CSIRTs can have on the security and safety of products and services in the ICT (supply) chain. The BPF investigated the potential role a CSIRT could play in this regard and found a few examples that are not currently common within CSIRTs, but appear to be successful. The case studies provided below merit further study, although some concerns around trust remain.[59]

### Case study: Switzerland's SWITCH[60]

[57] European Commission. Commission News release on 'Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union'. (7 February 2013). Available: http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and (Accessed 18 June 2015).

[58] Organisation for Economic and Co-operation and Development. Guidance for improving the comparability of statistics produced by Computer Security Incident Response Teams (CSIRTs) DSTI/ICCP/REG(2013)9/FINAL. (8 June 2015). Available: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG%282013%299/FINAL&doclanguage=en. (Accessed 18 June 2015).

[59] Note that these case studies have been edited for the sake of consistency in this BPF Handbook.

[60] Case study contribution by Serge Droz; edited for consistency.

SWITCH CERT processes thousands of IPs from hacked personal computers daily. Different sources are aggregated and then distributed to respective network owners for remediation. Since last year, these efforts are supported by the Swiss Internet Security Alliance. Its members, banks, ISPs and hosting companies coordinate the effort of cleaning infected personal computers by providing a common help to end users and sharing intelligence.

Operating the registry for the country code top-level domain names (ccTLDs) .ch and .li, SWITCH closely works with the Swiss regulator to create a legal basis to fight the misuse of domain names. The registry now has the power to shut down a domain name if it is used to steal personal information (phishing) or distribute malware.

SWITCH has a comprehensive programme today; working with hosters and registrars to solve issues before blocking. This means that over 80% of all incidents are solved in less than a day. The close collaboration between all involved stakeholders was crucial to SWITCH's success. Stakeholders regularly meet to discuss how collaboration could be improved. SWITCH also keeps stakeholders informed and provides tools to fix issues.

### Case study: Korea's KrCERT/CC[61]

The Republic of Korea's CERT, KrCERT/CC, operates a distributed denial of service (DDOS) mitigation centre for small- and medium-sized enterprizes (SMEs). The DDoS Shelter Service has been operational since 2010 to minimise the damage caused by DDoS attacks on businesses that are not fully prepared.

There are a lot of small to medium-sized enterprises such as online shopping malls in Korea due to advances in Internet service; many of which are not equipped to respond to security incidents by themselves. Therefore, the Korean government provides the DDoS Shelter Service for small and medium-size enterprises that cannot respond to DDoS attacks in order to not only minimise economic damages of victims and to protect their assets, but to also ensure their customers' continuous use the web services without disconnection.

These examples were presented to the BPF in the form of case studies and show that a CSIRT can have an impact in a broader way. Concerns remain about the effects that allocating additional tasks to a CSIRT may have, however. On the other hand, as illustrated by the cases above (more of which are included in the BPF's outcome document), the topic has potential and future research in the area could be useful. Suggested topics for research include whether there are other successful examples in the world, and whether there are new opportunities for CSIRTs to provide extensive, non-standard services to their constituency that materially improve cybersecurity whilst not damaging trust.

[61] Case study contribution by Eunju Pak; edited for consistency.

## CSIRTs and law enforcement

While many recognise the benefit of enabling cooperation between CSIRTs and law enforcement, there remains a serious problem when the two merge. As a BPF participant noted:

> “Misconception: CERTS will solve the problem of cybercrime. Fact: CERTs play an important role in fighting cybercrime by supporting the authorities doing their job, but not taking it over.”

In other words, CSIRTs traditionally combat the effects of cybercrime; helping customers, i.e. their constituency, to quickly recover and resume normal operation after an incident. CSIRTs do not investigate incidents from an enforcement point of view. This point was underscored by a contribution from the European Commission:

> “In fact, they benefit from not having such a function (LEA) because it lowers the threshold for individuals and organisations to report incidents and ask for help.”

This mixture of functionalities appears to be a major issue that capacity-building programmes around CSIRTs face regularly. It was advised that a strict distinction between a CSIRT and a LEA is built into these programmes from the outset.

## Clash of cultures

The BPF concluded that a clash of cultures is currently taking place in which CSIRTs’ traditional working methodologies are challenged. There is (i) the government, which aims to increase the role of CSIRTs where they take on a crucial response capability for the wider nation; often with some tension to involve (ii) law enforcement and the intelligence function. There is also (iii) the technical community, which wants to ensure its role is limited to response capabilities; enabling it to work effectively with other CSIRTs that have similar roles.

The CSIRTs that were established over the past two decades were built under the current CSIRT (maturity) models. With the growing interest of other governmental agencies in the Internet, and the increasing importance given to the topic in the context of economic security and the national security of nations, the entities and people interested in the work of CSIRTs have significantly changed. The erstwhile libertarian idea of an “Internet free state” - characterised by concepts like permission-less innovation and a lack of government intervention (concepts that usually have strong support within the technical community) - has come under pressure and is increasingly challenged.

On the other hand, this BPF acknowledged that companies with (vital) national interests, often residing in the private sector, have become prime targets, for example with the aim of stealing intellectual property, extortion and sabotage. Such companies are therefore approached more uniquely from a security perspective than before. Their CSIRTs, if they have, are in the front line of defence of national security against the above-mentioned examples and, as a result, have gained interest from higher management levels in the public and private realm as well.

From a clash of cultures to a mash of cultures? There is an increased need for successful collaboration of CSIRTs to be highlighted. Many case studies, including those featured in the BPF's outcome document, show that there are unique but valuable approaches that are worthy of further discussion and dissemination. One example is the OECD report,[62] detailing CSIRTs and appropriate metrics, to which all this BPF's lead experts contributed. This type of report is widely studied and read, and offers a way of organically introducing the CSIRTs' needs to the wider policy community. By adding insights, knowledge and input to policy circles, mutual trust and understanding can be built and achieved. It was noted that the objectives of all parties involve ensuring a safer Internet. This commonality offers a strong basis for starting discussions.

### Responsible disclosure

The BPF recognised that responsible disclosures, a computer security term describing a vulnerability disclosure model[63] by so-called ethical hackers,[64] forms a topic that deserves further consideration, as such hackers play a distinctive role in making the Internet a safer environment. There is currently a genuine interest in addressing the topic of responsible disclosure and to find safer ways for reporting by ethical hackers that will not unfairly expose them to prosecution that is not in the public's interest. The IGF is advised to see if there is a multistakeholder angle of responsible disclosures that merits further study into it.

## KEY FINDINGS

The particular value of the IGF lies in its role as a connector. While there are many different institutions dealing with specific issues related to CSIRTs in depth, the IGF offers

[62] Ibid.

[63] https://en.wikipedia.org/wiki/Responsible_disclosure (Accessed 15 December 2015).

[64] Wikipedia describes an ethical hacker as "a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems". https://en.wikipedia.org/wiki/Ethical_hacker. (Accessed 15 December 2015).

the potential of bringing experts from different stakeholder communities together in the search of common solutions. If the two terms of this BPF have shown anything, it is how influential such a process can be.

The work carried out by this BPF is regarded within the CSIRT community as valuable, as evidenced by the aforementioned use of the 2014 BPF's work to help create a CSIRT in Serbia. This BPF furthermore addressed topics that confronted the CSIRT community with outside pressure on their way of thinking and working as it evolved over the past decades. Discussing these pressures in the context of the BPF has led to valuable insights. CSIRTs realise that their core values have to be made known more universally through active reach-out to other communities, but also that a new way of cooperation and data-sharing may be necessary in a fast-changing world. CSIRTs now not only actively share their views, questions and potential answers in different stakeholders' fora, they also discuss sensitive topics among themselves. Finally they actively reach out to and invite input from, for example, privacy and human rights advocates. The provided answers are a part of the potential workload for 2016.

The pressure from governments and higher management levels due to persistent attacks on networks and systems is will likely increase. It is therefore important that all the parties involved understand what a CSIRT is, does and how it is successful.

During the BPF's process, an important question also emerged: **How do we engage these other stakeholders?** The answer was provided in the months that followed, when CSIRTs engaged others in diverse stakeholder communities and regions to share their message. An insight that was excepted as valuable was that CSIRT have to be present in the (virtual) places where policy debates are held and contribute. There they can share their message. A side effect may be that others will reciprocate that action in the future when issues arise.

Where privacy is concerned, it is advised to use the term 'data protection' rather than privacy. It was established that CSIRTs have support from privacy commissioners and that CSIRTs are 'defenders' of data. But it was also acknowledged that there are concerns about the lack of transparency and accountability concerning the processing and sharing of privacy sensitive data outside of the community that have merit. A study into transparency and accountability for CSIRTs in the face of data handling, processing and sharing, is seen as a potential step forward.

There are several interesting, novel ways in which some CSIRTs protect their constituencies and assume a wider role in cybersecurity too. Successful involvement in botnet mitigation centres, anti-DDoS measures, and pro-active handling of cybersecurity issues within a wider community were noted. Such roles are not common practice, but are regarded as a potential topic for further study.

## PRACTICAL RECOMMENDATIONS

The BPF derived several general recommendations from its work, as well as recommendations for future work within the CSIRT community in general and for individual members in particular (these have been extracted verbatim from the BPF's output document and are listed below). The recommendations mostly relate to the need to understand other parties' rationale better, for transparency, and for accountability where the data protection functions of CSIRTs are concerned.

**Recommendation 1:** There is a need for policymakers to discuss the role of CSIRTs with the CSIRT community to avoid misconceptions around the role of CSIRTs.

**Recommendation 2:** CSIRTs are recommended to be actively involved in relevant policy discussion at both the national and international level. In order to engage with other stakeholders it is important to be where they are. The provided examples show that it brings influence and understanding.

**Recommendation 3:** Every government has the right to create the CSIRT it needs. It is recommended though that governments make an informed decision, taking into consideration the potential consequences of their choice.

**Recommendation 4:** Where CSIRTs are concerned privacy and security have to stand together in order for a CSIRT to be truly successful.

**Recommendation 5:** Data protection is a term that is better understood in a general sense than privacy. Hence it is advised to use this term in a CSIRT context more as it is far more concrete.

**Recommendation 6:** Data protection has to be at the core of the work of a CSIRT.

**Recommendation 7:** It is recommended to involve Data Protection Commissioners more in the work of CSIRTs.

**Recommendation 8:** To ensure transparency and accountability where data protection is concerned, it is advised to make a study whether a standard protocol can assist attaining transparency, as well as more conscious decisions about limits to data sharing, anonymization of data where possible and the handling of data by CSIRTs.

**Recommendation 9:** CSIRTs should minimize data collection and processing, while also focusing on their constituency and anonymizing relevant information.

**Recommendation 10:** A well-run CSIRT is an essential part in the protection of data and security within a society.

**Recommendation 11:** Further study is recommended into the expanding role of CSIRTs. This could e.g. include whether there are sensible limits to tasks given and what role a CSIRT can play in enhancing cooperation in the security chain between other stakeholders, e.g. manufacturers of ICT products and providers of ICT services and does the current definition of a CSIRT match the reality of work asked and tasked.

**Recommendation 12:** Further study is recommended into the ways CSIRTs and law enforcement can enhance their cooperation in meaningful ways, each from within its respective mission.

**Recommendation 13:** Further study is recommended into responsible disclosure and how to create conditions that ethical hackers can contribute to a safer Internet experience for all.

**Recommendation 14:** CSIRTs have a role in handling effects of cybercrimes and providing technical support for investigations, but cybercrime is overall crime and as such should be dealt by law enforcement entities, like the police. Containing too much of this work within a CSIRT, or making a CSIRT part of a law enforcement agency is likely to have significant impact on its ability to work with the private sector.

## RECOMMENDATIONS FOR FUTURE RESEARCH

As this BPF does not consider its work finished, the main recommendation of this BPF is that its work continues in some form or another.

### A third BPF term?

The work in progress, as described above, is seen as so successful and influential that several experts in the BPF have indicated they want this BPF to continue; also because of the need to address many new topics within a multistakeholder environment. These could be, for instance, further work on data protection and transparency; the influence of CSIRTs on other stakeholders in the ICT (supply) chain (e.g. in botnet mitigation); the implementation of Internet standards and best practices; more secure ICT products;

etc. Participants have also identified new challenges for CSIRTs that need to be considered from a multistakeholder angle, including, for example, incidents in clouds.

### Dynamic coalition on cybersecurity, safety, and more

Another potential way forward that is currently under consideration is focusing on the broader aspects of cybersecurity. This could be done by forming a dynamic coalition involving experts who have been working in the BPF on the Regulation and mitigation of unsolicited communications, as there are overlapping issues concerning cybersecurity and network abuse. Preliminary discussions (still ongoing) have focused on the theme "preventing network abuse". Questions that could be addressed include how to reduce abuse; how to implement best practices; and how to improve the overall security of the Internet.

Cybersecurity can only be realised when worked on and dealt with through the entire chain of parties involved in ICT, from soft- and hardware developers to infrastructure providers, and from service providers to CSIRTs. Yet many of those directly involved in cybersecurity are not present in debates such as those taking place at the IGF. This is an issue area that would benefit from the multistakeholder approach and could be taken up by the broader IGF community in different formats, such as a BPF or dynamic coalition, but also at main sessions, workshops, and through coordination with national and regional IGF initiatives. This BPF accordingly recommends investigating these wider aspects of cybersecurity in the future.

### Responsible disclosure

Responsible disclosure was identified as one of the possible issues to be investigated in the future by a new BPF. This issue has gained a lot of attention in different fora and could not only benefit from further discussions in a multistakeholder setting such as the IGF, but also as the topic of a new BPF in 2016.

## FURTHER READING:

**Literature list available online:** http://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/502-literature-list-csirts

# THE REGULATION AND MITIGATION OF UNSOLICITED COMMUNICATIONS

**Experts: Julia Cornwell-McKean (lead), Cristine Hoepers, Neil Schwartzman**
**Coordinator: Markus Kummer**
**Rapporteur: Wout de Natris**

**Period of activity: two terms (2014 & 2015)**
**Approximate number of contributors: 40**
**Contributions for the BPF were collected during virtual meetings (number 7), on the mailing list, via the public review platform, case studies, a survey through IGF Africa, a matchmaking event at the IGF and during the BPF session at the IGF 2015 meeting.**

**Read the BPF's full report: http://www.intgovforum.org/cms/documents/best-practice-forums/regulation-and-mitigation-of-unwanted-communications/633-igf-2015-best-practice-forum-regulation-and-mitigation-of-unsolicited-communications-1**

## INTRODUCTION

The 2015 BPF on the Regulation and Mitigation of Unsolicited Communications continued the work it had started in 2014, and which had focused on best practices in the fight against unsolicited communications. The original name of the 2014 BPF mentioned "unwanted communications", which was changed to "unsolicited" for more clarity. The term "unsolicited communications" stems from legal texts in which such communications is defined.

In its 2014 outcome report[65] the BPF presented Internet standards and best practices; the need for them to be implemented was stressed; examples of anti-spam laws around the world were provided; the need for awareness campaigns was noted; and all of these were translated into recommendations.

For the purposes of the 2015 BPF, the terms "unsolicited communications" and "spam" are analogous; referring to all (written) unsolicited communications (that are carried on the Internet), including, and not limited to, messages that spread malware or have other nefarious purposes. For this reason the addition "(e.g. spam)", which was contained in last year's title, was removed from the title of this year's BPF.

In 2015, the BPF focused on two main, overarching streams:

[65] Report of the BPF on 'Regulation and mitigation of unsolicited communications (e.g. 'spam') (2014). Available: http://www.intgovforum.org/cms/documents/best-practice-forums/regulation-and-mitigation-of-unwanted-communications/411-bpf-2014-outcome-document-regulation-and-mitigation-of-unsolicited-communications-spam/file. [Accessed 15 December 2015].

- statistical and numerical data scaling the problem, and current examples of multi-stakeholder cooperation that attempt to resolve the problem; and
- the future of unsolicited communications in relation to the next billion Internet users coming online: challenges for the developing world.

The 2015 BPF also presents established practices; providing examples of where they have been successful so that others are encouraged to consider what may work in their own environments.

## SUMMARY

The BPF found that despite unsolicited communications being an issue of global concern, accurate quantification is a significant hurdle. No single dataset can measure the scope and scale of the problem; nor can it determine the cost implication involved for industries and governments. Statistics reflecting the impact of cybercrime are also difficult to source. In spite of these difficulties, this report presents the most reliable statistical information available, which indicates that there has been a recent downward trend in spam volumes. It is not yet known what the reasons for this decrease are and whether the trend will continue. The sources behind these statistics are as varied as the information. The BPF concluded that more research is needed in order to compile a more single-sourced data set that allows a true impact assessment of unsolicited communications on an economy.

The statistical graphs are not presented in this summary, but can be found in the BPF's outcome document. They provide valuable insight into volumes, countries of origin, the (financial) impact of phishing on industry sectors, countries hosting infected computers, volumes of command and control servers within countries, the impact of crime following the roll-out of broadband connections in specifically Kenya, etc. As someone noted in a conversation around this process:

> *"The abuse department of an ISP notices when a country comes newly online within minutes. The spam volumes from that country rise instantly."*

While connectivity will inevitably bring a wealth of information and accessibility, it will also bring risks. This BPF has therefore considered the likely challenges for the next billion Internet users to come online; drawing on the experience and expertise of those who are already online and, in some cases, have learned some difficult lessons, while balancing this with the opinions of those coming online. The BPF has the view that the problems that are likely to be encountered by the next billion Internet users are most likely very similar to those that have been addressed before. Spam, infections, malware and cybercrime will invariably be prevalent for future users, perhaps more so in developing nations, as measures that have been developed over time to address such issues may not be implemented prior to the broader deployment of broadband connectivity in such regions. However, the BPF also acknowledges that the next billion Internet users may require some alternate solutions directly applicable to their specific circumstances. For example, it is likely that connectivity by end users will occur predominantly through mobile devices and will be IPv6-based; thus making the implementation of traditional approaches more difficult (for example, many anti-spam blocklists have only recently started developing IPv6 blocking capabilities).

To learn more, the BPF worked closely with IGF Africa on a survey conducted under its members. The results are presented below.

## Method

The BPF received several case studies, including opinion pieces, academic research, successful practices, and examples of public-private and private-private partnerships. These case studies can be learned from and, where appropriate, replicated or adapted. Examples include a botnet mitigation initiative, different stakeholders from the ICT community cooperating to mitigate distributed denial of service (DDoS) attacks on the member companies and institutions; measures initiated by the national CSIRT to reduce spam figures in Brazil; capacity-building programmes; experience with creating an anti-spam law and unit with an enforcement capability; and academic studies into botnet mitigation and territoriality. Several initiatives that contribute to a safer Internet environment from around the world were also highlighted, as were organizations in which different stakeholders from within and beyond the ICT sectors find ways to cooperate on cybersecurity. The case studies demonstrate that a shared idea, need or vision can lead to cooperation and solutions that make the Internet safer. They are contained in the annexes to the BPF’s full outcome report.

## KEY FINDINGS

The work of the BPF brought together useful statistics and case studies, and also builds on the 2014 recommendations. The best practices to fight spam and other forms of online abuse from different angles have not changed in 2015. In fact, in many cases they still await much-needed implementation. In the 2015 process, several things stood out or came forward that deserve serious review as many of the examples provided can be a source of inspiration to others around the globe when faced with these specific problems.

### Case study: Operation safety net

'Operation safety net' is a document in which different stakeholders come together and present best practices and recommendations for governments, industries and end users. This document is:

> *…the second edition of a public-private initiative between members of the Messaging, Mobile, Malware Anti-Abuse Working Group (M3AAWG) and members of the London Action Plan (LAP), the global spam enforcement community. The report provides best practice recommendations for various stakeholders to address both online and mobile threats, including recommendations for consumers to be more proactive in securing their own devices; for service providers to implement certain security technologies and practices; for governments to ensure modern regulatory and legislative environments are established and enforced, and to work with international organizations to champion relevant collaborative efforts.*
>
> *These recommendations provide a set of tools to manage online, mobile and voice threats, although the threats described in this report provide only a snapshot of the threat environment today. As online activities change, the use of mobile computing grows, and Internet users and businesses change their responses and defences to existing threats, these threats will shift and adapt to exploit new vulnerabilities and pursue new targets. Putting these recommendations into practice will take a concerted multilateral approach. To that end, the authors of this report strongly encourage the OECD and other international organizations to join with M3AAWG and the LAP and engage with the organizations that govern and administer Internet infrastructures. In addition, in order to stay in front of the changing threat environment, all organizations concerned are encouraged to proactively collaborate in monitoring threats*

*and implementing new measures as needed to address them.*[66]

In a general sense the BPF found that it was extremely difficult to stick to the topic of unsolicited communications. This is only one aspect of cybersecurity and often interacts with other aspects. The need to look at cybersecurity and safety in general is one outcome of this year's work. This does not mean that unsolicited communications is a topic to discard. This BPF advises all stakeholders to mitigate this problem in order to have end users and society as a whole experience a safer Internet. Again, and this cannot be stressed enough, the Internet standards and best practices are already in existence, but need implementation.

A few topics, highlighted in the next section, stand out as having proven to make a difference or show great promise to do so.

## Botnet mitigation centres

Central to the spam problem is the issue of malware that permits the spread of unsolicited communication via botnets.[67] In the past few years, several countries have started anti-botnet centres in which infected machines are reported and registered, the corresponding end user is contacted, either directly or through his ISP, and often advice is given on how to disinfect an infected device. The first studies into this topic seem to show that there is a correlation between these centres and dropping infection figures.

### Examples from the Netherlands and Finland

AbuseHub is the botnet mitigation centre of the Netherlands. Its contribution showed the multistakeholder approach of the founders, who come from several communities. The latest addition for example is the hosting providers association joining AbuseHub. The first effects study showed that there is a shift of infections from members of the AbuseHUB to non-members.[68] The wording is guarded as further study is still needed, but the findings are nevertheless encouraging. In Finland, botnet mitigation for ISPs is a part of legislation. As a result Finland traditionally has the lowest infection rates in the world.

[66] Operation Safety-Net. Best Practices to Address Online, Mobile, and Telephony Threats. MAAWG/LAP (2015) see: http://londonactionplan.org/wp-content/uploads/2012/12/Operation-Safety-Net-web-version.pdf (Accessed 15 December 2015).

[67] "Botnets are networks of compromised machines remotely controlled by so-called botmasters", as defined in a contribution from BPF participant Karine e Silva, see annex 6 of the full report.

[68] Giovane C. M. Moura, Qasim Lone, Hadi Asghari, and Michel J.G. van Eeten (2015). *Evaluating the impact of AbuseHub on botnet mitigation. Interim deliverable 1.0*. Available: https://www.rijksoverheid.nl/...impact-of-abusehub-on-botnet-mitigation/evaluatie-the-impact-of-abusehub-on-botnet-mitigation.pdf (Accessed 15 December 2015).

More generally, it can also be concluded that in order to be successful in mitigating unsolicited communications, cooperation between different stakeholders is needed and often across national borders.

## Training for Africa

The BPF prioritised learning more about the needs and wants of those users coming newly online and thus solicited input from developing nations; working closely with, specifically, the regional African IGF initiative. A survey was sent by the African IGF Secretariat to its members; leading to a response from 15 persons. The results[69] were discussed during the African IGF's annual meeting in September and it was reported that the participants "found the results reflecting the real situation in Africa".

Capacity-building and training were flagged as a particular need by survey respondents. To therefore focus more on this issue, the BPF organized a "matchmaking" session on "Day Zero" of the IGF 2015 meeting in João Pessoa, Brazil; an experiment that contributed to the work in a significant way. The session discussed many of the issues that were highlighted in the BPF report and detected a willingness from many participants to collaborate in moving these issues forward. Some felt strongly that it is important for trainers to travel to the people who are in need of training. In the future, the organization and funding of such capacity-building initiatives could be discussed to put the concept of training into practice.

This BPF is close to consensus on the need for training at the network level in Africa and concludes that this BPF's survey results from the African IGF provide an indication of some of the realities in African contexts where unsolicited communications are concerned. The focus should primarily lie with basic cybersecurity capacity-building within an expanded remit that encompasses broader cybersecurity and cyber safety issues for network and anti-abuse administrators within telecommunication companies, ISPs and hosting providers in Africa (and, by implication, also other developing nations). This body of work should focus on the implementation of basic security measures and measures that are fairly easy to implement and come without debilitating costs. The BPF found that there is a strong need to make the African Internet and ICT experience safer and a related desire from ISPs in developed nations for Africa to be safer so that less abuse is received globally.

The need for training is confirmed by data from Kenya. A graph from a research report showed that cyber abuse using broadband connections rises faster than the number of

[69] The results can be found in the full report, pp 18 – 22.

broadband connections itself in the country.[70]

The BPF noted that there is a willingness to provide this training, and some participants with experience in training exercises stressed the importance of on-the-ground, hands-on training. To facilitate such opportunities for capacity-building, it will be necessary to coordinate and connect relevant individuals and organizations that are able to coordinate and potentially fund such initiatives. The BPF asks the IGF to look into the facilitation of further matchmaking sessions between relevant stakeholders.

### A single data set

As already noted, it proved impossible to present a single data set that showed in which way countries, economies or companies are all impacted by unsolicited communications. The BPF thus recommends that more research should be done to measure the scope and to scale the problem and its cost on economies – both for industries and governments.

There could be a connection in this regard with the fact that it is not typical to report cyber incidents and cybercrime to the authorities, who in return often do not distinguish between offline and online crime in their statistics. Despite the fact that this BPF acknowledges that, for example, fraud is fraud no matter how it is committed, many experts agree that there is a need to start making a distinction and to create the infrastructure to report online crime differently. As one expert wrote: "What gets measured, gets done."

### Cross-border cooperation

International cooperation is a prerequisite when mitigating or successfully investigating unsolicited communications. One contribution from academia noted:

> *"Contrary to law enforcement powers, online activities are characterised by the fluidity and thinning of geographical borders. In cyberspace, communication is ubiquitous and malicious users take advantage of this flexibility to target victims in various parts of the world, while subjecting themselves to minimum risk."*[71]

Another stated:

> *"The issue of jurisdiction over online activities has been controversial since the earliest days of large scale Internet usage… the time has come to*

[70] Kenya cyber-security report 2014. Rethinking cyber-security – "An Integrated Approach: Processes, Intelligence and Monitoring." See www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf (Accessed 15 December 2015).
[71] Contribution by Karine e Silva of the University of Tilburg. See annex 6 of the full report.

> *abandon territoriality as the core principle of jurisdiction.*"[72]

On the basis of the input provided to this BPF in the past two terms, from academic researchers as well as in the above-mentioned recommendations made by some African participants, it is the consensus view of this BPF that cross-border cooperation must evolve.

### Examples of mitigation

This BPF has found multiple examples of how different stakeholders cooperate, support each other and work together to mitigate different forms of unsolicited communication and presents them as examples to learn from. In many nations there is no law against unsolicited communications. The countries that have a law and an entity that can enforce have found that a law is one of the pillars of mitigation.

## PRACTICAL RECOMMENDATIONS

This year's work led to several general recommendations, presented below, that cover a diversity of topics including, but not limited to, training, education, the value of botnet mitigation centres, cybercrime reporting, the desirability of further region-specific surveys, and the benefits of multistakeholder arrangements (both public-private and private-private).

The BPF also presented and individually discussed the draft recommendations during its session at the IGF 2015 meeting in João Pessoa, Brazil, through so-called idea rating sheets. The recommendations were, generally speaking, received well and many have been nuanced in response to the productive and candid discussions that resulted. This process proved to be successful, productive and very interactive. It led to the following (general) recommendations for the consideration of those actively involved in unsolicited communications and cybersecurity at large (the recommendations have been extracted verbatim from the BPF's output document and are listed below).

**Recommendation 1:** That newly connected economies consider multistakeholder anti-botnet efforts (botnet mitigation centers) as they have a role in reducing the number of infections on end users' devices.

[72] Professor Dan Jerker B. Svantesson Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). See annex 7 of the full report.

**Recommendation 2:** That effort be taken by law enforcement to categorise crimes undertaken using the Internet.

**Recommendation 3:** That governments and law enforcement take proactive steps to encourage the reporting of cybercrime by all users: citizens and industry.

**Recommendation 4:** That further attention ought to be given to surveying the needs of African nations (and other developing nations), not only in dealing with the problem of spam, but the broader issues of cybersecurity and cyber safety.

**Recommendation 5:** That there is a need for basic cybersecurity training, including in relation to the mitigation of unsolicited communications, in the African region and perhaps other regions of the globe. Active participation from other regions is recommended. An example could be to organise workshops at the African Internet Summit.

**Recommendation 6:** That there is a need for education of citizens, including children, on matters relating to cybersecurity in economies coming newly online.

**Recommendation 7:** That industries affected by spam, phishing, etcetera must continue to evolve in order to protect their own reputations and to ensure that their own customers do not become victims; including the provision of funding for education programs.

**Recommendation 8:** That further consideration ought to be given to producing simple lists of low or no cost initiatives that can assist newly-connected economies to protect their infrastructure.

**Recommendation 9:** That consideration ought to be given by newly connected economies to a wide variety of multi-stakeholder arrangements, including public-private and private-private initiatives in combating unsolicited communications.

## LESSONS FROM CASE STUDIES

Many of the recommendations listed above are bolstered by the case studies this BPF received, which are presented in the annexes of this year’s outcome report. Importantly, these case studies all indicate that there can be various different solutions to related problems.

A few insights are also evident from these examples, including that every solution begins with a vision that can originate from within the government, a private company, a branch organization, a CSIRT, an individual, etc. From there (multi)stakeholder cooperation is sought to tackle a specific cybersecurity challenge. There simply is no one-size-fits-all solution.

The other overarching conclusion that presented itself was that it is impossible to achieve cybersecurity alone. In all of the examples encountered by the BPF, forms of cooperation are evident in which different stakeholders contribute, participate and share to become safer together. In discussions it seems common to look to a government to provide solutions, but many case studies submitted to the BPF showed that some solutions were built without any government involvement at all. In some instances, the government facilitated and/or actively supported a mostly private process, while in others government was a leading or instigating factor.

The examples presented in the case studies offer valuable experiences that others could learn from and adapt to their own circumstances.

## RECOMMENDATIONS FOR FUTURE RESEARCH

This BPF considers its work and mandate completed and advises to stop work on "unsolicited communications". In general, this work was found to be valuable and it was acknowledged that, in order to facilitate the implementation of the recommendations, there is a need for a regular 'check-in' or review. The IGF is asked to assist in organizing this process in the coming years.

The suggestions for future work relate to the IGF and include considerations for the immediate follow-up to this BPF as well as possible themes for the future work for the IGF.

The BPF identified the need for future work in the broader cybersecurity and cyber safety areas as unsolicited communications are only one aspect of the many issues relating to the protection of infrastructure and citizens online. One way forward to continue work in a meaningful way could be to form a dynamic coalition. As there are overlapping issues concerning cybersecurity and network abuse with the work carried out by the BPF on CSIRTs,[73] one option could be to involve experts who worked in both of these BPFs.

[73] See the full report of the BPF Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security, page 26. http://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/627-bpf-csirt-2015-report-final-v2/file.

To avoid a duplication of efforts, any future work the IGF undertakes needs to take into consideration ongoing work in other organizations and fora, such as FIRST, M$^3$AAWG, and the International Telecommunications Union (ITU). The IGF can add value by connecting stakeholder communities and fostering discussion and cooperation with a view to implementing outcomes. The themes proposed for future work could be taken up as workshops, main sessions, new BPFs, dynamic coalitions or other new initiatives.

The following themes are offered to the broader IGF community for consideration:

### *The implementation of Internet standards and best practices*

Cybersecurity is achieved through a combination of factors, namely the implementation of standards and (maintenance of) best practices; end users' use of cyber sanitation measures; governmental interventions (like awareness programmes); safer ICT products (throughout the whole production chain); etc. No single actor can influence a safer Internet environment on its own as there is a strong interdependency. By focusing work on the need for implementing standards and best practices, different stakeholder groups can be brought together and can discuss the hurdles that prevent the implementation of Internet standards and best practices.

This topic touches on establishing and fixing the root causes of unsolicited communications, for example vulnerabilities in soft- and hardware, unclear responsibilities in production, maintenance and service chains, weak enforcement, the voluntary patching of security flaws, national jurisdiction versus the Internet, etc. The root causes were also not dealt with in-depth in this report, although they were sometimes alluded to. To have delved into root causes would have meant widening the scope of this BPF beyond manageable proportions.

Other related issues that were not addressed by the BPF but could be addressed in the future include root causes of cyber insecurity and challenges related to the IoT.

### *Developing reliable metrics*

There is a need for further work to be done to pin down a set of reliable metrics that relate not only to spam, but also to broader cybersecurity issues.

### *Cybercrime and cybersecurity incidents: reporting and statistics*

The BPF has shown that it is not common for citizens to report cybercrimes or cybersecurity incidents. In addition, when cybercrimes are reported they may not be categorised as such, making reporting and developing strategies for dealing with systemic issues difficult. Experts consider that it is important that reporting becomes the norm in order to classify, measure and start preventive as well as investigative actions. A next step could be to bring the involved stakeholders together and discuss potential ways forward so that priorities can be set and scaled.

### *Basic cybersecurity training in developing countries*

There was consensus on the need for basic cybersecurity capacity-building within an expanded remit that encompasses broader cybersecurity and cyber safety issues for network and anti-abuse administrators in developing countries. This report lists the first steps in this regard, including identifying willing actors that could aid such capacity-building efforts. The IGF could assist by bringing the right people together and thus facilitate meetings where the organisation and funding of cybersecurity workshops in developing countries can be discussed.

There are also other regions and topics to consider besides Africa and this aspect of cybersecurity and safety. There is merit in broadening and professionalising this BPF's basic survey to find out what the challenges in the different regions are.

## CONCLUSION

In conclusion, this BPF has taken significant steps to outline the scale and scope of the unsolicited communication problem, taking into account the limitations of such an exercise.  The BPF has engaged directly with some of those stakeholders who are newly online in parts of Africa and has formed a view that although cybersecurity is constantly evolving, the assistance that is sought by those directly affected generally matches with the expectations of those who can assist.

The BPF has outlined in some detail the experience of others through case studies, and hopes that these experiences also provide a guide for those who are still coming online. It remains, however, for those with funds and in positions of power, including governments, to consider their roles in protecting the connectivity of their respective jurisdictions and educating citizens on safe online practices.

## FURTHER READING:

**Literature list available online:** http://www.intgovforum.org/cms/documents/best-practice-forums/regulation-and-mitigation-of-unwanted-communications/501-literature-list