2017 IGF Best Practice Forum (BPF): Cybersecurity – Virtual Meeting II

Summary Report

21 June 2017

1. The IGF Best Practice Forum (BPF) on Cybersecurity held its second virtual meeting on 21 June 2017. The meeting was facilitated by Markus Kummer. The primary purpose of the call was to review analyses of the IGF's 'Connecting and Enabling the Next Billion(s)' (CENB) outcome documents, which will be used as a basis for the BPF's input-gathering questionnaire. A recording of the meeting is available here: https://intgovforum.webex.com/intgovforum/ldr.php?RCID=a5e69e021ea502257ae4d8c5f73bf825

2. The meeting began with some brief announcements from Markus Kummer. Markus introduced MAG member Segun Olugbile, also on the call, as the co-facilitator of the BPF. The proposed IGF 2017 main session on cybersecurity, which had been discussed at length in the MAG's recently concluded face-to-face meeting, was also mentioned. Markus told participants that the Cybersecurity BPF reporting into this main session represented a good opportunity for collaboration and to make the BPF's work more visible and prominent. This contrasts with last year when all BPFs shared a main session and their messages tended to get diluted.

3. Andrew Cormack, who volunteered to do a close review of the CENB II document for policy recommendations with cybersecurity implications, gave an overview of his work (**ANNEX II**), which had been sent earlier through the BPF's mailing list. Andrew noted several of the Sustainable Development Goals (SDGs) focused on in the document were potentially affected by cybersecurity issues in a number of ways. Maarten van Horenbeeck undertook a similar approach for the CENB I outcome and briefed BPF members on his review (**ANNEX III**), which had also been shared on the mailing list. It was agreed the CENB II review would form the main basis for the questionnaire, although some inputs could also come from the CENB I analysis. Noting the wide range of the work, Markus remarked there would be a lot of natural 'cross-fertilization' with the two other 2017 BPFs on Gender & Access and Local Content. Another participant observed that many of the points in the CENB I analysis were highly relevant to issues currently faced by developing countries and that they would be important to raise in the questionnaire, in particular from a capacity building perspective.

4. Wout de Natris also spoke briefly about his proposal to seek out one pressing and timely cybersecurity challenge from the BPF questionnaire's respondents (**ANNEX IV**). It was agreed this would be an interesting line of inquiry and that it should be integrated into the overall draft questionnaire document. Maarten made the suggestion that in order to make the text more succinct and easily incorporated, it could be boiled down to a single additional question, along the lines of, "If you had to choose one issue that you think threatens the development of the Internet, what would it be?" Andrew further suggested that respondents could be asked whether they would add anything to the list of cybersecurity challenges included in the questionnaire.

5. Next steps for the work ahead were outlined as follows:
   - Step 1. The BPF members will develop a draft questionnaire, largely on the basis of the CENB II analysis and the proposed additional question(s) from Wout.
   - Step 2. The contact list for the questionnaire will be finalized, with the understanding that the questionnaire should be as widely disseminated as possible. This entails sending through general mailing lists but also in targeted fashion to individuals and organizations.
   - Step 3. The group will prepare text/letters to accompany and explain the questionnaire.

   Regarding Step 1, it was agreed Maarten, Andrew and Wout would co-draft a preliminary questionnaire for the rest of the group to edit in a shared document and to discuss on the mailing list. On Step 2, Maarten informed participants there were already 104 organizations and names in an active Google doc that had been shared with the BPF members. Markus mentioned that the Secretariat could assist in finding contacts for some organizations. It was also said the Secretariat could help produce initial drafts for the letters accompanying the questionnaire.

6. Finally, the participants agreed on a 'compressed timetable' to complete the steps above. The **target date for finishing the questionnaire will be end of July**; the **BPF will reconvene between 6 and 10 August** to do a final review of the questionnaire and discuss outstanding issues; and the **questionnaire will be sent out in mid-August.**

Annex I – Participants List

Markus Kummer (Facilitator)

Eleonora Mazzucchi (IGF Secretariat)

Andrew Cormack

Lucimara Desidera

Foncham Denis Doh

Maarten van Horenbeeck

Jean-Robert Hountomey

Louise Marie Hurel

Lawrence Muchilwa

Wout de Natris

Janvier Ngnoulaye

Olusegun Olugbile

Alejandro Pisanty

Delfi Ramirez

David Strudwick

Timea Suto

Annex II – Notes on CENB II (Andrew Cormack)

Notes on how cyber-security can affect the achievement of the Sustainable Development Goals (SDGs). Derived from the IGF Policy Options for Connecting and Enabling the Next Billion(s): Phase II. Many of the cyber-security issues affect several SDGs: the connections selected here are chosen as perhaps the best examples of these dependencies.

SDG1 (No Poverty) depends on individuals being able to access information over the Internet. Thus it can be disrupted by weaknesses in, and attacks on, the availability of information services and the networks that individuals use in connecting to them. Issues such as **denial of service attacks** and **services that can act as amplifiers** for them could therefore affect progress towards this goal. Similar issues arise in SDGs 4 (Quality Education), 10 (Reduced Inequalities), 14 (Life below water) & 15 (Life on Land), and the overall aim of providing "meaningful access".

SDG2 (Zero Hunger) includes farmers seeking information, reporting on local conditions, applying for grants etc. Since such activities may involve implicit or explicit criticism of public authorities, they will be hindered by any perception that those authorities are engaged in **surveillance of internet usage**.

SDG3 (Good Health) includes telemedicine, disease monitoring and the storage of patient data. Developed countries have already experienced setbacks in these areas as a result of incidents affecting the **confidentiality and availability of sensitive information** held by medical and health services.

SDG5 (Gender Equality) is harmed by individuals or organisations using communications technologies to engage in **online abuse** and gender-based violence.

SDG6 (Clean Water) involves using communications technologies for the remote monitoring and control of treatment and pumping equipment. **Vulnerabilities in SCADA (Supervisory Control and Data Acquisition) equipment** that is connected to shared networks are a major concern that can turn such automation from a benefit into a serious pollution and health threat.

SDG7 (Affordable and Clean Energy) depends on the widespread acceptance of smart meters and smart grids. Loss of trust in these systems can easily be caused if monitoring equipment and systems do not keep information confidential, or if **information is used for inappropriate purposes**.

SDG8 (Decent Work and Economic Growth) highlights the importance of mobile payment systems, which are critically dependent on the **security of mobile devices** such as phones and tablets.

SDG9 (Industry, Innovation and Infrastructure) suggests that developing countries may find opportunities to develop disruptive industries in the area of IoT (Internet of Things). However **lack of secure development processes** are already causing concerns for IoT and any industry based on them could be severely damaged by a security failure in its products.

SDG11 (Sustainable Cities and Communities). Many of the technical tools suggested as supporting this aim can also become serious threats to individuals and communities if they are not secure. Criminals, neighbours, governments or even family members with **unauthorised access** to internet-monitored home security, traffic monitoring or CCTV systems can cause serious privacy, material, physical or emotional harm.

SDG16 (Peace and Justice) concerns citizen engagement in government, but also notes that these tools can be used for repression and the spread of prejudice. Either will strongly discourage engagement. Systems used to hold authorities to account must be **protected from abuse by those authorities**.

Annex III – Notes on CENB I (Maarten van Horenbeeck)

The 2017 Best Practices Forum on Cybersecurity is reviewing the cybersecurity implications of policy recommendations made as part of "*Policy Options for Connecting and Enabling the Next Billion(s): Phase II*". The outcome of this work will help inform policy makers of the important cybersecurity implications of implementing or evaluating a specific policy option.

In order to ensure a comprehensive review, these notes describe a review of the cybersecurity implications of policy options identified as part of "Policy Options for Connecting and Enabling the Next Billion(s): Phase I". While that document did not align with the Sustainable Development Goals, and thus will not be our line of inquiry in approaching the Phase II review, this review is intended to ensure our guidance is comprehensive.

In Appendix A, a set of reviewed policy recommendations, extracted from the Phase I CENB document is listed. Reviewing those, I identified a set of high-level criteria which came up, in many cases repeatedly. I noted some brief security implications of each:

1. Promoting improved and extended broadband infrastructure:
    - Increased broadband increases the risk of vulnerable endpoints being leveraged in high-bandwidth **Distributed Denial of Service attacks**. Whereas unmaintained, unpatched or unlicensed devices on low bandwidth networks have mostly localized impact, on high bandwidth networks the impact is likely to have more implications at the global network level.
2. Promoting spectrum increases and promoting increased reliance on wireless modes of operation:
    - Use of spectrum for internet access is subjected to **local jamming as a Denial of Service attack**, which has different recovery scenarios (they must be triangulated and stopped) than cable disruptions (which can physically be fixed).
    - Wireless network access increases the importance of **strong traffic encryption** controls.
3. Promoting increased power grid capacity:
    - Extension of power grid capacity, in particular over greater distances will involve the deployment and reliance on the **security of Supervisory Control and Data Acquisition (SCADA) equipment**.
4. Promoting the development of Internet Exchange Points:
    - Internet Exchange Points have strong physical security needs, and imply the use of specialized software and hardware which must be maintained. Use of components with **good software security and a standard, maintainable and updatable setup** becomes more important as IXPs are more distributed and perhaps run by local teams with less experience.
5. Promoting user awareness education:

- Educating users on the use of the internet requires those users to be **made aware of security risks and safe conduct online**.
- It requires the **development of initial services with human behavior in mind**, so the default behavior of users on the services they use as their first entry online is secure.

6. Deploying government services using an Open Data model:
   - **Making data available requires proper anonymization**, which is not an easy challenge. Data must be available in aggregate to be of use, but should not be released in such way that permits de-anonymization.
   - Data released by the government must have **strong integrity** to enable society to make appropriate decisions based on its analysis.
   - When third parties start building on top of the data set, its **availability** becomes important to permit these third parties to function.
7. Addressing unsolicited e-mail and other forms of spam:
   - Spam and unsolicited messages may make otherwise effective communication channels difficult or unpleasant to use. **Abuse management mechanisms** are needed, which should be carefully introduced so as not to lead to censorship or put in place other boundaries on communication.
8. Promoting the increase of locally relevant content and local language support:
   - Increased local language support, in particular when associated with other character sets may increase the risk of **homoglyph attacks** on the URIs used for such content, or other, international content;
   - Locally relevant content may not be required to be available globally. These reduced performance requirements may incentivize content creators to store it on local network resources. Having only a single copy of the information available in a region increases the risk of a **Denial of Service attack** rendering it unavailable, or a local outage causing it to be destroyed.
9. Promoting national domain name infrastructure:
   - National domain name infrastructure is often less robust than the gTLD's on which large international enterprises are deployed, such as .com, .net and .org. Increasing reliance on it requires investment in **secure domain name and registry infrastructure**.
10. Promoting sharing of passive infrastructure:
    - Shared infrastructure may expose infrastructure owned by one operator to another, requiring the implementation of **strong security controls** restricting access;
    - Shared infrastructure **reduces overall redundancy of networks**. An outage of a single site may affect multiple providers.
11. Addressing minority and gender-based online harassment:
    - Addressing minority or gender-specific harassment requires contextual knowledge of what means "harassment" and proper reporting channels. These reporting channels may not always be available when a service provider is in a different country, or operating under a different legal framework.
12. Strengthen telecommunications infrastructure through public private partnerships:
    - Public-private partnerships may include shared operational capability between government and industry providers, which requires **strong security controls and separation of duties** to ensure the public partners is unable to affect technical implementations for e.g. domestic surveillance.
13. Enabling initiating economic opportunities, such as starting a company, online:
    - Bringing services critical to the economy such as these online requires secure development processes to ensure the **underlying data stores are protected from unauthorized access and modification**;

  - A **Denial of Service attack** against such services may hamper the ability of businesses to do their work, or citizens to become economically active.

14. Make internet devices more affordable
    - Increased price pressure without specific quality requirements may result in vendors saving on costly, but important processes such as **quality control**. This may result in devices being introduced without passing through a software development lifecycle that includes security testing, or a supportable update process.

Annex IV – Proposed Message to Contributors on Cybersecurity Challenges (Wout de Natris)

The Best Practice Forum Cyber Security of the Internet Governance Forum is in its second year. It will pick up on last year's recommendations. Next to this body of work, it contemplates to select one topic in the realm of cyber security, after which stakeholders, needed to work on a solution to the selected challenge, will actively be invited to join the BPF.

The idea is to work together on this topic. This way we'll find out whether it is possible to work on and solve a cybersecurity challenge through a coordinated action, within the context of the IGF, together.

There is one prerequisite to the first question below, your answer has to be generic. E.g. solve botnets and not solve the "Conficker" botnet or solve Ransomware vs. solve "WannaCry". These are just examples. Your answer can touch on any cyber security issue. The BPF leadership will select the most acute topic presenting itself from your answers.

1. What is for you(r organisation) the most critical cyber security issue that needs solving and would benefit most from a multistakeholder approach within this BPF?

2. In what way does this critical issue limit our ability to expand the number of end users or effect the quality of service to current end users?

3. Which stakeholders need to be invited to join the BPF and (help) solve the issue you mention?

Please send your answers to the list before (date TBD.)