2017 IGF Best Practice Forum on Cybersecurity

Dear National and Regional IGF representatives,

The IGF Best Practices Forum on Cybersecurity is calling for input for its 2017 effort. We are very interested in understanding national and regional specifics on the cybersecurity challenges we all face, and are looking for your assistance.

During 2015 and 2016, the Policy Options for Connecting and Enabling the Next Billion(s) (CENB) activity within the Internet Governance Forum identified two major elements:

- Which policy options are effective at creating an enabling environment, including deploying infrastructure, increasing usability, enabling users and ensuring affordability;
- How Connecting and Enabling the Next Billion(s) contributes to reaching the new Sustainable Development Goals (SDGs).

The Best Practice Forum on Cybersecurity realizes that making Internet access more universal, and thus it supporting the SDGs, has significant cybersecurity implications. Well-developed cybersecurity helps contribute to meeting the SDGs. Poor cybersecurity can reduce the effectiveness of these technologies, and thus limit our opportunities to helping achieve the SDGs. In our 2017 effort, we aim to identify policy mitigations that can help ensure the next billion(s) of users can be connected in a safe and reliable manner.

BPF members have already performed some security focused analysis of the CENB Phase I and II documents developed during previous years. You can review these documents here:

Security focused reading of CENB Phase I - https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/687
Security focused analysis of CENB Phase II - https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/688

You can assist in the BPF by sending us answers to any or all of the following questions. They are divided in two sets:

- *General questions* should be relatively easy to answer, and provide a strong contribution to the BPF. Thank you in advance for addressing these.
- *Specific questions* are focused on very specific areas of interest. We do not expect you to respond to all of them, but if you have the opportunity to discuss them in your NRI, we welcome your input.

You are invited to share your responses on the BPF mailing list (*https://www.intgovforum.org/mailman/listinfo/bp_cybersec_2016_intgovforum.org*). For any questions, you can reach out to the Secretaria at igf@unog.ch with in cc lead expert Mr. Maarten van Horenbeeck (maarten@first.org), and the BPF's co-facilitators, Mr. Olusegun Olugbile (solugbile@gmail.com) and Mr. Markus Kummer (kummer.markus@gmail.com).

Thank you,

Markus Kummer
Olusegun Olugbile
IGF BPF on Cybersecurity co-facilitators

Questionnaire

Full Name of the NRI you are responding for:

European Dialogue on Internet Governance (EuroDIG)

Your name and official role at the NRI you are responding for:

- ❏ Coordinator
- ❏ Chair or co chair
- ❏ X Member of the Steering Group/Organizing Committee/MAG of the NRI
  [Tatiana Tropina is Subject Matter Expert (SME) for Cyber Security at EuroDIG. SMEs are responsible for the clustering of submissions into a thematic category they have an expertise in. They define subtopics and identify submissions which fall under this subtopic. The aim is to verify submissions which can be merged in one session. In the

course of the session organising process SMEs will serve as a mentor for the respective category by supporting Focal Points.]

- ❑ Interested participant/observer in an NRI
- ❑ An NRI community member
- ❑ Observer on the NRIs mailing list

Your contact information (e-mail):
Sandra Hoferichter: sandra@eurodig.org
Tatiana Tropina: tatiana.tropina@gmail.com
General questions

- Has your NRI organized a session on cybersecurity? Was it considered a priority session?
  Answer: *in 2017, cybersecurity was considered among the priority sessions at EuroDIG as it received one of the largerst numbers of proposals for discussion during the call for issues (which shapes EuroDIG's agenda in a bottom-up manner). There are were 4 cybersecurity-related sessions: 1 Plenary, 2 workshops on specific issues and one capacity building session.*

- For how many years has your NRI covered cybersecurity as a topic?
  Answer: *Cybersecurity was among the topics covered by EuroDIG since EuroDIG's inception in 2008.* Since 2015 we are focusing on building upon the results of the year before and provide a continuous discussion. The results are published on the EuroDIG wiki and the EuroDIG Messages.

- What did the session address, or was covered in the session agenda? Were any implementation plans or policy proposals presented or discussed at your meetings, or discussed during intersessional work?

  Answer:
  There were 4 cybersecurity sessions at EuroDIG 2017, with two of them focused on discussing and mapping the issues of cybersecurity and multi-stakeholder approaches to it, one capacity building session and one workshop on criminal justice that discussed specific policy proposals from the EU Commission and Europol on the mutual legal assistance. The latter workshop in addition to discussion presented a set of practical proposals.

The plenary session -- “Alice in wonderland – mapping the cybersecurity landscape in Europe and beyond” -- addressed the issue of mapping cybersecurity landscape under three axes:

- *economical (economic rationale for industry),*
- *technical (what do recent cyberattacks teach us), and*
- *regulatory (how much regulation is needed).*

The workshop “Stress testing the multistakeholder model in cybersecurity” discussed multistakeholderism in cybersecurity governance and both the practical and policy tools to serve to that end. Among other issues, it focused on collaborative security model as a different take on the multistakeholder approach.

The capacity building session focused on explanation of some advanced issues related to cybersecurity.

The workshop “Criminal justice on the Internet – identifying common solutions” focused on a current proposals to bridge the differences in legal frameworks in the EU to facilitate mutual legal assistance in digital investigations and on addressing technical problems in crime investigation such as Carrier-Grade NATs. The workshop discussed, in particular, the proposal from European Commission on improving mutual legal assistance and particular steps that are to be taken in this regard. The panel and participants came to a set of conclusion for improvement of the mutual legal assistance in digital investigation in Europe and beyond (for details see the answer to the question below).

- What were the main outcomes, or work initiated out of this session?

Answer: after each session, the rapporteurs submitted the main outcomes in the form of messages, that are available here: https://www.eurodig.org/fileadmin/user_upload/eurodig_Tallinn/Messages_from_Tallinn_EuroDIG_2017.pdf

The workshop “Criminal justice on the Internet – identifying common solutions” was the most actions-oriented. It concluded with the set of recommendations, which included the *need for standardisation of forms, capacity building and training, the establishment of channels for facilitating requests (like online portals). The workshop highlighted the need for respecting safeguards and human rights, transparency, and participation of all stakeholders in the process. Furthermore, it was concluded that capacity building among law enforcement is necessary to answer complex mutual legal assistance requests properly. Lastly the participants concluded that there is a need to engage with electronic service providers to gradually reduce the use of technologies that prevent online criminal attribution such as Carrier Grade NAT / LSNAT.*

The plenary session -- "Alice in wonderland – mapping the cybersecurity landscape in Europe and beyond" provided the set of messages related to the cybersecurity as international security and highlighted the need for international cooperation, for the specific role of the governments in providing cybersecurity, awareness, education, cooperation between stakeholders and human rights protection.
The workshop "Stress testing the multistakeholder model in cybersecurity" discussed multistakeholderism in cybersecurity governance and both the practical and policy tools to serve to that end. Among other issues, it focused on collaborative security model as a different take on the multistakeholder approach.

The workshop "Stress testing the multistakeholder model in cybersecurity" concluded with acknowledging that every stakeholder has different economic interests and insentives and different logic and that only a good multistakeholder process will bridge the differences. While recognising that there are calls for a stronger role of the governments in cybersecurity processes, the workshop recommended strengthening the role of civil society for esuring accountability and transparency.

- Does your NRI maintain any key messages on cybersecurity?
  As it was pointed in the answer to the above question, each session's outcome is summarised in the form of the messages from EuroDIG, and cybersecurity sessions are among them. The messages from Tallin are available at:
  https://www.eurodig.org/fileadmin/user_upload/eurodig_Tallinn/Messages_from_Tallinn_EuroDIG_2017.pdf

Specific questions

- What working definition do you maintain for cybersecurity? What is considered a cybersecurity issue and what is not?

  Answer: *EuroDIG doesn't have specific definition for cybersecurity. As a bottom-up driven process, EuroDIG collects the issues from any interested parties and shapes the program based on the issues. Any submission of the topic can be attributed to a "cyebrsecurity" category by the submitters themselves. However, after the call for issues ends, the cybersecurity subject matter expert assesses the proposals received and checks if the topics submitted under the "cybersecurity" category really falls under this issue or should be attributed to the session on another major topic.*

  There are sometimes issues boadering with overlapping categories EuroDIG has as topics – e.g. privacy or human rights, when the issue could be assigned to both sessions as it includes cybersecurity element but rather focussing on digital rights or privacy. In this case, the submitter is contacted to clarify the focus to make a final assessment.

- How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

  Answer: *The dicsussions at EuroDIG 2017, including the keynote messages delivered by the President of Estonia (host country) highlighted that trust and security are the key factors for achieving sustainable development and the future digital society.*

- How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

- Assessment of the CENB Phase II policy recommendations identified a few clear threats. Which of the following do you consider priorities? Do you see particular policy options or best practices to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:

  General answer: *As EuroDIG is a dialogue, a community-driven process, the priorities in the discussion is shaped by the submission of the call of the issues and the issues are discussed at the sessions. Neither secretariat nor subject matter expert set the priorities in cybersecurity discussion. In the following answers, the policy options and other* *answers are indicated only in case if they were discussed during the cybersecurity plenary and workshops and are outlined in the session messages.*

- ○ Issues that impact the reliability and access to Internet services
  Priority? Yes/No
  Policy options?
    - ▪
    - ▪

    - ○ Security of mobile devices
      Priority? Yes/No
      Policy options?
        - ▪
        - ▪

    - ○ Potential abuse by authorities, including surveillance
      Priority? Yes/No
      Policy options?
        - ▪
        - ▪

    - ○ Confidentiality and availability of sensitive information
      Priority? Yes/No
      Policy options?
        - ▪
        - ▪

    - ○ Online abuse and gender based violence
      Priority? Yes/No
      Policy options?
        - ▪
        - ▪

    - ○ Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Points (IXP)
      Priority? Yes/No
      Policy options?

    -
    -

- Vulnerabilities in the technologies supporting critical industrial processes such as electricity provisioning
  Priority? Yes/No
  Policy options?
    -
    -

- De-anonymization of improperly anonymized citizen data
  Priority? Yes/No
  Policy options?
    -
    -

- The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis
  Priority? Yes/No
  Policy options?
    -
    -

- Internet of Things security.
  Priority? Yes/No
  Policy options?
    -
    -

- Human Factors and security awareness and education
  Priority? Yes/No
  Policy options?
    -
    -

- **Other**: describe a cybersecurity issue critical to developing the SDGs in relevant to your nation or region (100 words or less)

Priority? Yes/No
Policy options?

▪
▪

- Please, enumerate Innovative Practices in the field of cybersecurity that you have seen discussed in your community, and which help promote the safe connection of the next billion(s) of users, or promote the Sustainable Development Goals.

- Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity.

  This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

  Answer: *one of the sessions at EuroDIG 2017 discussed in depth the multi-stakeholder model and its complexity. The conclusions highlighted that the way internet was constituted and works each party needs to take responsibility to ensure resilience and to take a collaborative security approach to foster confidence and protect opportunities. Since every stakeholder has different incentives and different economic interests and different logics (regarding security/privacy/DP), only a good multistakeholder process would bridge these differences. While it was agreed that governments usually try to take the lead in setting policy and regulatory priorities, the role of civil society is important to monitor accountability and transparency.*

- Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

  Answer: *at the EuroDIG 2017, while stressing that the multi-stakeholder collaboration and role of technical community, industry and civil society is very important, more voices were raised with the suggestion that governments should take a leading role in driving national and international cybersecurity agenda and setting regulatory and policy priorities. This, however, should not undermine the collaborative approaches and the role of tech community and industry in identifying risks, providing security of networks and customers, and the role of civil society in safeguarding transparency, accountability, due process and human rights.*

- What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?

- How about bringing an awareness about Cyber Security Intelligence and its potentiality?