|  |  |  |
| --- | --- | --- |
| C:\Users\ponder\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\BDT-25th_anniversary_2017-Logo_411959-3_transparent.png | **Telecommunication Development Advisory Group (TDAG)**  **22nd Meeting, Geneva, 9-12 May 2017** | C:\Users\murphy\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\PQ94T9LJ\bd_E_25Years_Horizontal-411959 (003).jpg |
|  | |  |
|  | | **Document** **TDAG17-22/****63-E** |
|  | | **26 April 2017** |
|  | | **Original:** **English** |
| Ministry of Internal Affairs and Communications, Japan | | |
| Proposal TO ContinuE the Study of Cybersecurity In Question 3/2 | | |
|  | | |
| **Summary:**  This contribution emphasises the importance of continuous discussion on cybersecurity and proposes continuous work on this area for developing countries in ITU-D. In the 2013-2017 Study Period, ITU-D SG2 Question 3: Securing information and communication networks: Best practices for developing a culture of cybersecurity, has played a key role to lead discussions and information sharing regarding cybersecurity topics/issues among ITU-D members involving public sectors, private sectors (industries) and academia. It is worth considering carrying on such efforts into the next study period.  **Action required:**  TDAG is invited to consider this document and take action  **References:**  N/A | | |

# Background: Role of ITU-D SG2 Question 3

As globally noticed, taking actions for cybersecurity is one of the most urgent issues for all organizations. Securing information and communication networks and developing a culture of cybersecurity have become key in today’s world.

ITU-D Study Group2 Question 3; Securing information and communication networks: Best practices for developing a culture of cybersecurity (Q3/2), has lead the cyber security discussions and contributed to members in the 2014-2017 Study period.

Q3/2 covers:

1. developing best practices for evaluating the impact of spam
2. providing information on current security challenges
3. gathering national experiences relating to Cybersecurity
4. analyzing cybersecurity awareness survey
5. providing a compendium of cybersecurity activities
6. Examining specific needs of persons with disabilities
7. examining ways and means to assist developing countries for cybersecurity related challenges
8. gathering national experience and national requirements in the area of Child Online Protection
9. holding workshops for information sharing related cybersecurity topics
10. gathering national experience and requirements on common criteria and security testing

During the current study period, Q3/2 had 6 meetings and received over 50 contributions to discuss above areas. The Q3/2 final report includes above major topics and also proposes recommendations for the next study period including requests from developing countries.

Q3/2 has also actively played a role as a venue for information sharing to all ITU members.   
3 cybersecurity workshops were held and 50-300 participants from public sectors, private sectors (industries) and academia, actively jointed each workshop.

|  |  |  |
| --- | --- | --- |
| 1st WS | September 2015 | Nation Global Cybersecurity Challenges |
| 2nd WS | January 2016 | National Cyberdrills and Effective implementation of a National Cybersecurity Strategy |
| 3rd WS | January 2017 | Cybersecurity and Risk Assessments in Practice |

In particular, the first workshop was jointly held with ITU-T SG17 and it became a successful use case of joint work with cross sectors in terms of the number of participant and sharing common objectives among sectors. Q3/2 also received positive feed-back and requests for continuous holding of workshop and it was well recognized and agreed that ITU events such as workshop/seminar could effectively work as a venue for useful information sharing that could meet participants’ needs and keep updating cybersecurity issues.

2. Proposals

ITU-D SG2 Question 3 has played a key role for cybersecurity discussion and its role will be more important as discussed in the 4th SG2 meeting in April 2017.

It is therefore proposed that the activities by Q3/2 should be continued with the current mandatory. While activities in the 2014-2017 under the current mandatory (ToR) were well covered and reported, Q3/2 also recognized the need of continuation of further actions such as evolving and emerging technical threats beyond spam and malware, additional capacity building and practical implementations of the topics following discussions in the workshops into the new study period. Q3/2 can also maximize the role for information sharing with providing workshop/seminars to discuss topics that will include upcoming/ emerging trends and issues by the latest technologies.

Such contribution by Q3/2 together with related Questions, sectors and liaison organizations will be useful to developing countries.

Considering above, it is also proposed that the title of Q3/2 should clearly indicated discussions for both on-going and new technical threats such as “Best practices for addressing emerging and evolving threats to cybersecurity” as reached consensuses in the 4th SG2 meeting.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_