Telecommunication
Development Bureau (BDT)

Ref.: Circular/BDT/DNS/CYB/051 Geneva, 24 July 2020

- ITU Member States
- ITU-D Sector Members
- Academia
- Regional/International Organisations
- Critical National Sectors/National CERTS
- ITU Cybersecurity Focal Points

Subject: Invitation to participate in the 2020 ITU Global CyberDrill

Dear Sir/Madam,

I have the pleasure to invite you to participate in the 2020 International Telecommunication Union (ITU) Global CyberDrill, which will be held from September to November 2020. The ITU CyberDrill will be hosted virtually due to the ongoing COVID-19 pandemic and associated risks and restrictions related to travel and gatherings.

The COVID-19 pandemic has increased worldwide the reliance on information and communication technologies (ICTs). ICTs have allowed people to be productive and engaged even while social distancing. Such increased reliance on ICTs has also posed significant challenges to cybersecurity with increased cyber threats.

The planned 2020 ITU Regional CyberDrill events will be replaced by one single virtual Global CyberDrill. Within the Global CyberDrill, we will organize a series of regional dialogues, international webinars, training sessions, and scenario-based exercises over three (3) months to help build capacity within countries to manage cyber threats better. Further details are available in the event handout attached to this letter (Annex 1).

The Global CyberDrill is a capacity building event which aims to enhance the communication and incident response capabilities of participating teams and promote collective efforts by national Computer Incident Response Teams (CIRTs) and Computer Security Incident Response Teams (CSIRTs).

The CyberDrill is open to teams from national CIRTs/CSIRTs, ministries, regulators, telecommunication operators, universities and educational institutions, telecommunication equipment manufacturers, research and design institutes, software developers, and other interested stakeholders of the ITU Member States, Sector Members, and Academia. It is recommended that the participating team consist of minimum two (2) technical staff and one (1) management level staff.

To get more information and to register for Global CyberDrill events, please visit the following link: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx

The ITU Regional Thematic Priority Leads in Cybersecurity are available for any queries you have concerning the 2020 ITU Global CyberDrill events.

- Regional Office for Africa, Mr. Serge Valery Zongo (serge.zongo@itu.int)
- Regional Office for Americas, Mr. Pablo Palacios (Pablo.Palacios@itu.int)
- Regional Office for Arab States, Ms. Rouda Al Amir Ali (Rouda.AlamirAli@itu.int)
- Regional Office for Asia and the Pacific, Mr. Sameer Sharma, (sameer.sharma@itu.int)
- Regional Office for CIS, Mr. Farid Nakhli (farid.nakhli@itu.int)
- Regional Office for Europe, Mr. Jaroslaw Ponder (jaroslaw.ponder@itu.int)

Yours faithfully,

[Original signed]

Doreen Bogdan-Martin
Director

ANNEX 1

2020 ITU Global CyberDrill

1. INTRODUCTION

The International Telecommunication Union (ITU) improves a States' cybersecurity readiness, protection, and incident response capabilities by conducting CyberDrills at the regional and international levels. A CyberDrill is an annual event during which cyber-attacks, information security incidents, or other types of disruptions are simulated in order to test an organization's cyber capabilities, from being able to detect a security incident to the ability to respond appropriately and minimize any related impact. Through a CyberDrill, participants are able to validate policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations. To date, the ITU has organized more than 29 CyberDrill events around the world to enhance cybersecurity capacity and capabilities through regional collaboration and cooperation.

2. OBJECTIVES

The main objectives of this CyberDrill are to:

- Provide situational awareness to key public and private sector participants who lead their firms, organizations, or jurisdictions during a cyber disruption;
- Bring the CERT/CIRT/CSIRT community together in a unified exercise to build global response and recovery capabilities;
- Test operational resiliency key concepts across CSIRT/CIRT/CERT community;
- Identify, exercise, and foster the improvement of processes, procedures, interactions and information sharing mechanisms that exist or should exist among CERTs/CSIRTs, SOCs, agencies, public bodies, and across regional organizations responsible for crisis management and regulatory bodies;
- Exercise coordination mechanisms, information sharing efforts, the development of shared situation awareness, and decision-making procedures of the cybersecurity community during cyber events; and,
- Raise awareness of other cyber exercise initiatives.

3. FORESEEN ACTIVITIES

Due to the travel restrictions and other important measures in response to the COVID-19 pandemic, the CyberDrill events will be carried out online over the course of three (3) months, starting from September to November 2020. The ITU experts, in cooperation with partners in the field, aim to conduct and/or host:

- **Six (6) regional dialogues on lessons learned from the COVID-19 pandemic**:
    a. The COVID-19 pandemic has increased pressure on national ICT systems, at times making them more vulnerable to cyber-attacks on critical infrastructure. The regional dialogues will provide the opportunity for representatives of CSIRT/CIRT/CERT of all Member States

to share their experiences in dealing with cybersecurity issues during the COVID-19 pandemic.

- **Three (3) webinar sessions**:
  a. **Empowering Women in Cybersecurity:** This webinar will feature panelists who will discuss women's role in the field of cybersecurity across all sectors. This series of events will be open to all participants.
  b. **Cyber Crisis Management:** Having a dedicated cyber crisis management strategy is the foundation for building national Cyber Resilience. This panel will feature experts in the field of cyber crisis management. This series of events will be open to all participants.
  c. **Measuring and Improving CIRTs maturity:** This panel discussion will focus on measuring and enhancing maturity as essential aspects of continuously advancing and strengthening CSIRT capabilities. This webinar will feature experts who have extensive experience working with CIRTs. This series of events will be open to all participants.

- **Six (6) training sessions**:
  a. ITU experts in collaboration with partner organizations will conduct each training session, which will take place on different days at pre-defined time. The training sessions will consist of discussions on building effective Cyber Threat Intelligence (CTI) Capabilities, incident response, communication in crisis management, industrial cybersecurity and incident response, fake news identification and practical cyber threat intelligence. These training sessions will be open to all participants.

- **Six (6) scenario-based exercises**:
  a. Conducting scenario-based exercises is one of the highlights of the ITU CyberDrills. This year, ITU plans to conduct six scenario-based exercises on different days at a fixed time. The exercises are open only to National/Government CIRTs/CSIRTs, and each participating country will be represented by a team consisting of a minimum of two (2) and a maximum of four (4) participants.

The Regional Webinars on "CIRTs and Lessons Learned from COVID-19" will only be open to Member States from that particular region. The remaining webinars, training sessions, and scenarios-based exercises will be open to all participants, irrespective of region.

4. TARGET AUDIENCE

The regional dialogues, webinars, and trainings are open to national CIRTs/CSIRTs, Ministries, regulators, telecommunication operators, academia and educational institutions, telecommunication equipment manufacturers, research and design institutes, software developers and other interested stakeholders of the ITU Member States, and Sector Members.

The exercises are open only for National/Governmental CIRTs/CSIRTs and each registered country will be represented by one team consisting of two (2) participants.

5. LOGISTICS

We recommend that all participants have a computer or laptop with a stable and suitable internet connection when participating in a CyberDrill events.

6. REGISTRATION

For more information and to register for the events, please visit the event website: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx

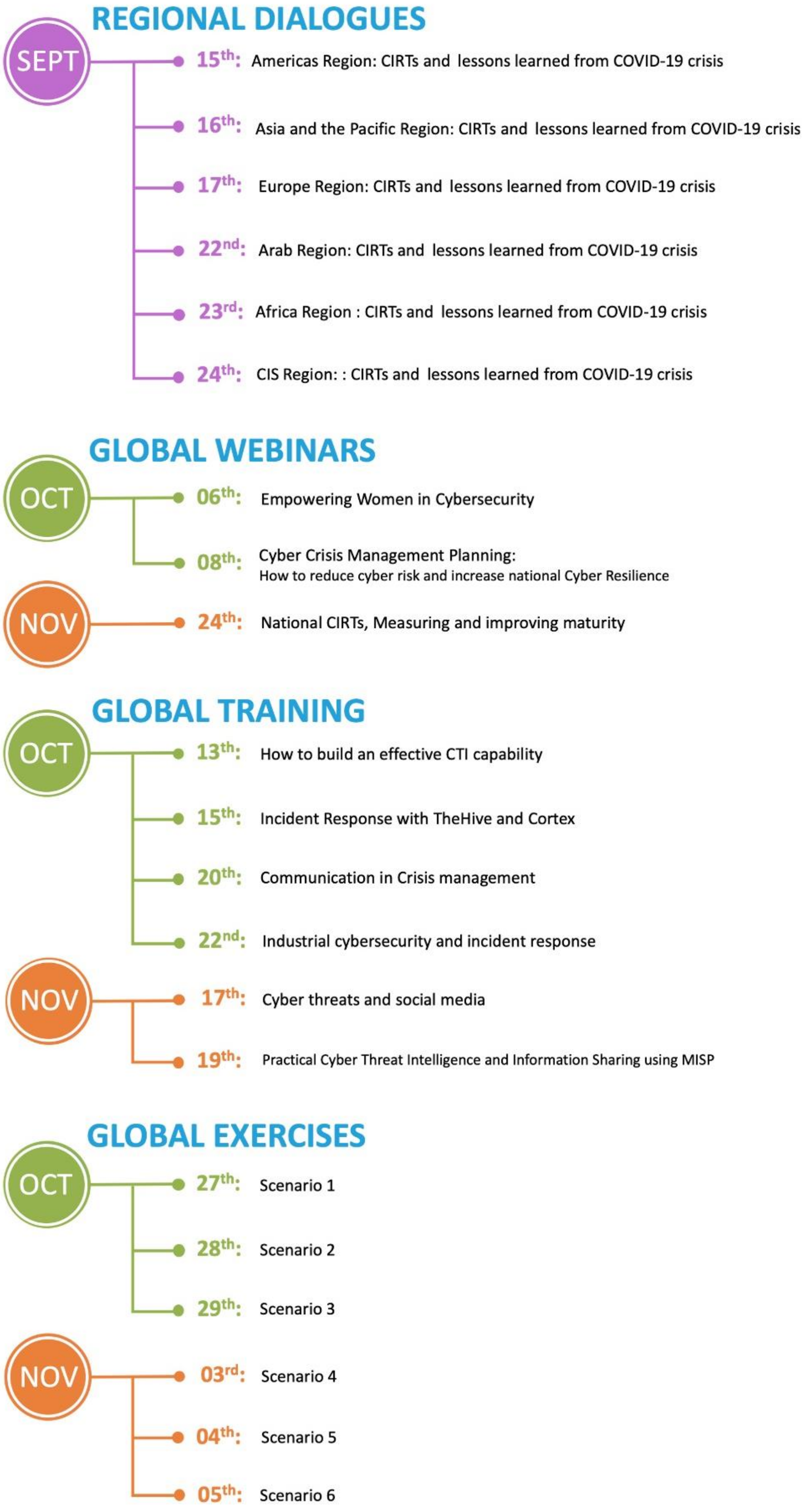
Registration details, including meeting links and other information, shall be sent to the participants' registered email addresses. Registration for trainings and exercises will close on Wednesday 30 September 2020, or when sessions are fully booked.

7. CONTACT DETAILS

If you have any questions, please feel free to contact your regional ITU Cybersecurity focal point:

- Regional Office for Africa, Mr. Serge Valery Zongo (serge.zongo@itu.int)
- Regional Office for Americas, Mr. Pablo Palacios (Pablo.Palacios@itu.int)
- Regional Office for Arab States, Ms. Rouda Al Amir Ali (Rouda.AlamirAli@itu.int)
- Regional Office for Asia and the Pacific, Mr. Sameer Sharma, (sameer.sharma@itu.int)
- Regional Office for CIS, Mr. Farid Nakhli (farid.nakhli@itu.int)
- Regional Office for Europe, Mr. Jaroslaw Ponder (jaroslaw.ponder@itu.int)

8. EVENT CALENDAR



REGIONAL DIALOGUES

SEPT

- 15th: Americas Region: CIRTs and lessons learned from COVID-19 crisis
- 16th: Asia and the Pacific Region: CIRTs and lessons learned from COVID-19 crisis
- 17th: Europe Region: CIRTs and lessons learned from COVID-19 crisis
- 22nd: Arab Region: CIRTs and lessons learned from COVID-19 crisis
- 23rd: Africa Region : CIRTs and lessons learned from COVID-19 crisis
- 24th: CIS Region: : CIRTs and lessons learned from COVID-19 crisis

GLOBAL WEBINARS

OCT

- 06th: Empowering Women in Cybersecurity
- 08th: Cyber Crisis Management Planning: How to reduce cyber risk and increase national Cyber Resilience

NOV

- 24th: National CIRTs, Measuring and improving maturity

GLOBAL TRAINING

OCT

- 13th: How to build an effective CTI capability
- 15th: Incident Response with TheHive and Cortex
- 20th: Communication in Crisis management
- 22nd: Industrial cybersecurity and incident response

NOV

- 17th: Cyber threats and social media
- 19th: Practical Cyber Threat Intelligence and Information Sharing using MISP

GLOBAL EXERCISES

OCT

- 27th: Scenario 1
- 28th: Scenario 2
- 29th: Scenario 3

NOV

- 03rd: Scenario 4
- 04th: Scenario 5
- 05th: Scenario 6

Regular updates of the agenda will be posted to the CyberDrill webpage, please check the online calendar for detailed and up-to-date information : https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybedrills-2020.aspx