



Telecommunication
Development Bureau (BDT)



Ref.: BDT/DNS/CYB

Geneva, 10 August 2021

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

Subject: Invitation to participate in the 2021 Global CyberDrill

Dear Sir/Madam,

It is my pleasure to invite you to participate in the 2021 International Telecommunication Union (ITU) Global CyberDrill, taking place from September to November. Mirroring the 2020 Global CyberDrill, the ITU Regional CyberDrills events will be replaced by a single virtual drill.

With specific focus on the role of national Computer Incident and Response Teams (CIRTs) and Computer Security Incident Response Teams (CSIRTs) in building cyber resilience and protecting critical information infrastructure, the 2021 CyberDrill sessions are tailored around four thematic concepts: *reflect, share, learn and practice*.

This virtual cyberdrill will serve as a capacity building platform to enhance the existing communication mechanisms and strengthen innovative cooperation approaches for national CIRT/CSIRTs. It consists of inter-regional meetings, webinars, technical trainings, cybersecurity exercises, and provides a common platform to connect cybersecurity teams across the ITU Member States, Sector Members including academia, regional and international organizations, telecommunication operators, regulators, along with other relevant stakeholders.

It is recommended that participating organizations consist of a team with a minimum of two (2) technical staff, and one (1) representative at the management level. For more information, please refer to the attached Terms of Reference (Annex 1) or visit the event page: <https://itu.int/go/GCD2021>.

For further queries concerning this year's ITU Global CyberDrill, please contact your regional ITU Cybersecurity focal point as detailed in the Annex.

I look forward to your attendance at the virtual cyberdrill.

Yours faithfully,

[Original Signed]

Doreen Bogdan-Martin
Director



ITU/BDT Cyber Security Programme

2021 Global CyberDrill

Terms of Reference

July 2021

Terms of Reference

1. INTRODUCTION

The International Telecommunication Union (ITU) aims to improve the cybersecurity readiness, protection, and incident response capabilities of Member States by conducting CyberDrills at the national, regional and global level. These annual events where cyber-attacks, information security incidents, and other disruptions are simulated, help to test an organization's cyber capabilities. Over the past ten years, ITU has held over thirty CyberDrills partnering with more than 100 countries committed to improving cybersecurity at both national and global levels.

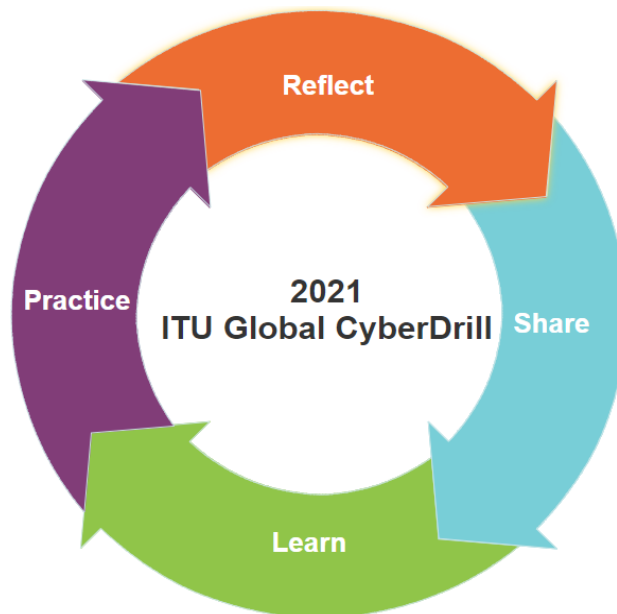
While ITU CyberDrills are generally held at the regional level, the 2020 and 2021 events bring together the cybersecurity community and specifically ITU Member States on a global level in order to meet the challenges posed by the COVID-19 pandemic.

Building upon the discussions and outcomes from last year's event, the 2021 Global CyberDrill will emphasize the role of national Computer Incident and Response Teams (CIRTs) and Computer Security Incident Response Teams (CSIRTs) in building cyber resilience and protecting critical information infrastructure.

2. OBJECTIVES

The 2021 Global CyberDrill will tailor event sessions around four thematic concepts: *Reflect, Share, Learn* and *Practice*.

- **Reflect:** Bring cybersecurity major regional and consider on the five pillars of Cybersecurity Global Cybersecurity
- **Share:** Promote beneficial networks, and stream resources.
- **Learn:** Build capacity communities within critical information protection (CIIP).
- **Practice:** Test key concepts across CSIRT/CIRT/CERT community.



together the global community to review cybersecurity trends improvements based ITU Global Agenda (GCA) and The Index (GCI). knowledge sharing of communication exchange funding for the CSIRT incident response and infrastructure operational resiliency

3. FORESEEN ACTIVITIES

All activities will be delivered virtually over the course of three months. The ITU experts, in cooperation with partners in the field aim to conduct and/or host:

- **Three (3) Interregional Meetings (Reflect):** Featured speakers will include cybersecurity leaders from the government and regional organizations etc. sharing best practices and lessons learned around critical information infrastructure protection (CIIP).
 - Interregional Meeting I: Asia and the Pacific and CIS regions
 - Interregional Meeting II: Africa and Europe regions
 - Interregional Meeting III: Americas and Arab regions

- **Two (2) Webinars (*Share*):**
 - **Webinar I:** Unlocking the Potential of Cybersecurity Cooperation: Opportunities, Challenges, and the Way Forward. Speakers will emphasize the vast quantity of resources available to the CSIRT community, specifically, funding mechanisms within international organizations.
 - **Webinar II:** Women in Cyber: A year later
ITU launched in 2021 the Women in Cyber Mentorship Programme (in collaboration with FIRST and EQUALS). The programme is an outcome of the CyberDrill 2020 Empowering Women in Cybersecurity webinar, where the need for role models and mentorship was identified as pivotal for increasing the number of women leaders in cybersecurity. Building upon ongoing efforts of ITU to close the digital gender divide by mainstreaming gender-focused activities, the programme engages role models and leaders in the field, and connects them with talented women worldwide.
The first edition of the programme was successfully implemented, and the session will bring together mentors, mentees and trainers to discuss the impact of the programme including sharing testimonials and best practices, in a collective effort to devise the future of the programme and of the community for 2022 and beyond.
- **Six (6) Training Sessions (*Learn*):** ITU experts in collaboration with partner organizations will conduct training sessions over the second half of the CyberDrill. Training sessions will be grouped over three weeks. Subjects include:
 - How to Identify and Classify Critical Information Infrastructure Assets and Services
 - Strengthening Legal, Policy and Compliance Frameworks for CIIP
 - Threat Monitoring and Incident Response for CNI using open source tools
 - DDoS Mitigation Fundamentals
 - Conducting Exercises to improve Incident Response
 - Measure and Improve the National CIRT Maturity
- **Six (6) Scenario-Based Exercises (*Practice*):** Exercises are one of the highlights of the ITU CyberDrills, and are open to National/Government CIRTs/CSIRTs. Participating countries are represented by teams of two to four people and will take place over two weeks.

The three interregional meetings will only be open to Member States from those particular regions. 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 including other interested stakeholders of the ITU Member States, and sector members

5. REGISTRATION AND LOGISTICS

We recommend that all participants attending the CyberDrill have a computer/laptop with a stable Internet connection.

For more information on the 2021 Global CyberDrill, please visit the event website: <https://itu.int/go/GCD2021>.

Registration details including meeting links and additional meeting information will be sent to participants registered email address. Registration for trainings and exercises will close on 10th September 2021 or when sessions are at capacity.

6. 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, Mr. Ahmed ElRaghy (ahmed.elraghy@itu.int)
- Regional Office for Asia and the Pacific, Mr. Calvin Chan (calvin.chan@itu.int)
- Regional Office for CIS, Mr. Farid Nakhli (farid.nakhli@itu.int)
- Regional Office for Europe, Mr. Jaroslaw Ponder (jaroslaw.ponder@itu.int)

7. EVENT CALENDAR

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://itu.int/go/GCD2021>.

