Cyber Development Training

Cairo – Egypt, 11-15 December 2022

TRAINING OUTLINE

Title	**Cyber Development Training**
Modality	Physical
Dates	Cairo – Egypt, 11-15 Dec. 2022
Duration	5-days
Training fees	Free
Description	The primary objective is to facilitate the access to relevant, useful and actionable resources to the developing countries, especially the least developed countries to enhance their cybercapacity, and ultimately their national capacity and skills.
Registration deadline	8 Dec. 2022

1. SCOPE

The growing reliance on ICTs for the well-functioning of societies demands increased attention on cybersecurity. The confidentiality, integrity, and availability of ICT systems is challenged by rapidly evolving cyber-risks that can impede digitalization's transformational power.

However, improving cybersecurity capacity – also known as cybercapacity - is complex, multidimensional, and resource-consuming, and entails different areas of intervention, including in organizational processes, human skills, and adoption of technologies. Due to these challenges, lower- and middle-income countries may be less able to manage digital risks effectively and efficiently.

Financial costs of cybersecurity are one of these challenges. Securing digital assets can be expensive, and security may be perceived as an expense that does not generate immediate or short-term returns rather than as a long-term investment. Further, governments may prefer to allocate limited financial resources to other compelling areas that may also be more immediate. In addition, the complexity of cybersecurity can cause it to be difficult for policymakers to develop or implement a clear strategy for capacity development.

In addition, the development of the Regulatory landscape needs efforts in different aspect such as legal, technical and financial domains which need huge effort from developing countries especially LDCs to maintain the required human capabilities to achieve sustainable development in this regard.

Finally, there is a critical shortage of regulatory and cybersecurity expertise skills and professionals in the developing world (especially LDCs). Expanding and integrating a skilled workforce is necessary to equip developing countries with the expertise to implement impactful development in such domains. The lack of expertise transversally applies across sectors, from technical profiles to law enforcement and policymakers.

2. LEARNING OBJECTIVES

To allow participants to access to relevant, useful and actionable resources to enhance their cybercapacity, and ultimately their national capacity and skills through a set of cybersecurity/regulatory on Job Training and educational activities that are tailored to their needs as highlighted in the latest iterations of the Global Cybersecurity Index (GCI). These activities are aimed at creating multidisciplinary skills including engineering, technical, organizational, lawful, incident response etc. The goal is to create an heterogenous pool of professionals that governments can tap to design and implement a comprehensive ecosystem.

3. LEARNING OUTCOMES

Upon completion of this training, participants will be able to:

- Apply the theoretical and practical knowledge of IT and cyber security and security methods for computer, network and electronic communication.
- have an overview of the core components of what it takes for a country to become cyber-prepared, highlighting the critical aspects that governments should consider when developing their national strategies and implementation plans.
- Implement the essential elements required when developing a National Cyber Incident Response Plan and the best practices for disaster recovery planning.

- Handle cyber incident response activities, incident resolution approaches and the good practices of information sharing, and effective communication related to incidents of national significance.
- Testing, implementation, and maintenance of the National Cyber Incident Response Plan.
- Apply Forensic investigation scenarios that enable participants to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to carry out a computer forensic investigation successfully.

4. TARGET POPULATION

The target audience for this training are staff (middle to senior levels) of national cybersecurity agencies or CERTs.

5. TUTORS/INSTRUCTORS

Orhan Osmani Marwan Ben Rached Ahmed ElRaghy	Orhan.Osmani@itu.int Marwan.BenRached@itu.int Ahmed.elraghy@itu.int

6. TRAINING CONTENTS

The following topics will be covered in this training:

- Vulnerability Assessment and Penetration Testing
- Cyber incident response
- Cyber forensics
- Malware analysis
- Building national cyber resilience and protecting critical information infrastructure, Role of National CIRT
- Lifecycle, principles and good practices on National Cyber Security Strategy development and implementation

7. TRAINING SCHEDULE (Cairo Time)

Day	Morning Session (9:30 am to 1 pm)	Lunch Break	Afternoon Session (2 pm to 3:30 pm)
Day 1: **11 December**	08:30-09:00 **Registration**	1:00-2:00	**Session3: 2:00-3:30** **Law enforcement cooperation with CSIRTs/National CIRTs**
	09:00-09:25 **Opening Remarks** - NTRA - ITU (Ahmed Elraghy) 09:25-09:40 Coffee Break and Group photo		
	Session1: 09:40-11:00 **CYB Governance & CERT Operation**		
	Session2: 11:30-1:00 **Digital Forensics** **Speaker: Abdelrahman Bakry**		
Day 2: **12 December**	**Session4: 9:30-11:30** **Speaker: Drill Scenario 1**	1:00-2:00	**Session6: 2:00-3:30** **Malware analysis**
	Coffee break 11:30-12:00		
	Session5: 12:00-1:00 **GCI: An overview for cybersecurity enhancement**		

Day 3: **13 December**	**Session 7: 9:30-11:30** **Speaker: Drill 2 Scenario 2**	1:00-2:00	**Session9: 2:00- 3:30** **Incident Response Training**
	Coffee Break 11:30-12:00		
	Session 8: 12:00-1:00 **Cybersecurity and online safety awareness: what steps can countries take to protect the most vulnerable?** Part I: Women as disproportionately affected by cyber threats; gender inclusion to improve cybersecurity Part II: Children and young people: how to empower them to fully take advantage of the opportunities of cyberspace? Part III: Elderly population: the need for better risk awareness Part IV: Inclusion in cybersecurity workforce development as part of the solution		
Day 4: **14 December**	**Session10: 9:30-11:30** **Cyber Crisis Management: Financial Sector – Tabletop Exercise (TTX)**	1:00-2:00	**Session12: 2:00-3:30** - **Vulnerability Assessment and Penetration Testing**
	Coffee break 11:30-12:00		
	Session11: 12:00-1:00 - **Vulnerability Assessment and Penetration Testing**		

Day 5: **15 December**	**Session13: 9:30-11:00** **NCS Guide: NCS Development and Implementation Practices** This session will touch on the NCS Guide, its structure and share some experiences/good practices in NCS Development and Implementation. An online NCS self-paced training: Lifecycle, principles and good practices of national cybersecurity strategy development and implementation is available in English, French, and Spanish	1:00-2:00	**Session15: 2:00-3:30** **Closing Ceremony**
	Coffee Break 11:00-11:30		
	Session14: 11:30-1:00 **Malware analysis**		

8. METHODOLOGY (Didactic approach)

Discussions: Participants are expected to participate actively in discussion on selected topics throughout the training.
Course materials will be published on the website after the completion of the course.

9. EVALUATION AND GRADING

Evaluation will be based on quizzes.

IMPORTANT: a passing mark of 70% is required for obtaining a completion certificate.

10. TRAINING COURSE COORDINATION

Course Coordinator:	ITU Coordinator:
Mrs. Maha Badar Manager of EG-ATRC at NTRA Focal point at NTRA Cairo - Egypt Mobile: +201022933965 Email: Mahab@tra.gov.eg	**Mr. Ahmed El Raghy** Senior Advisor ITU Arab Regional Office Tel: +202 3537 1777 Mobile: +201005281908 Fax: +202 3537 1888 Email: ahmed.elraghy@itu.int

11. REGISTRATION

ITU Academy portal account

Registration should be made online at the ITU Academy portal. To be able to register for the course you **MUST** first create an account in the ITU Academy portal at the following address:
https://academy.itu.int/user/register

Training course registration

When you have an existing account or created a new account, you can register for the course online at the following link: https://academy.itu.int/training-courses/full-catalogue/cyber-development-training-least-developing-countries-ldcs You can also register by finding your desired course in our training catalogue https://academy.itu.int/training-courses/full-catalogue